



FEDERAL REGISTER

Vol. 88

Wednesday,

No. 65

April 5, 2023

Pages 20059–20382

OFFICE OF THE FEDERAL REGISTER



The **FEDERAL REGISTER** (ISSN 0097-6326) is published daily, Monday through Friday, except official holidays, by the Office of the Federal Register, National Archives and Records Administration, under the Federal Register Act (44 U.S.C. Ch. 15) and the regulations of the Administrative Committee of the Federal Register (1 CFR Ch. I). The Superintendent of Documents, U.S. Government Publishing Office, is the exclusive distributor of the official edition. Periodicals postage is paid at Washington, DC.

The **FEDERAL REGISTER** provides a uniform system for making available to the public regulations and legal notices issued by Federal agencies. These include Presidential proclamations and Executive Orders, Federal agency documents having general applicability and legal effect, documents required to be published by act of Congress, and other Federal agency documents of public interest.

Documents are on file for public inspection in the Office of the Federal Register the day before they are published, unless the issuing agency requests earlier filing. For a list of documents currently on file for public inspection, see www.federalregister.gov.

The seal of the National Archives and Records Administration authenticates the **Federal Register** as the official serial publication established under the Federal Register Act. Under 44 U.S.C. 1507, the contents of the **Federal Register** shall be judicially noticed.

The **Federal Register** is published in paper and on 24x microfiche. It is also available online at no charge at www.govinfo.gov, a service of the U.S. Government Publishing Office.

The online edition of the **Federal Register** is issued under the authority of the Administrative Committee of the Federal Register as the official legal equivalent of the paper and microfiche editions (44 U.S.C. 4101 and 1 CFR 5.10). It is updated by 6:00 a.m. each day the **Federal Register** is published and includes both text and graphics from Volume 1, 1 (March 14, 1936) forward. For more information, contact the GPO Customer Contact Center, U.S. Government Publishing Office. Phone 202-512-1800 or 866-512-1800 (toll free). E-mail, gpocusthelp.com.

The annual subscription price for the **Federal Register** paper edition is \$860 plus postage, or \$929, for a combined **Federal Register**, **Federal Register** Index and List of CFR Sections Affected (LSA) subscription; the microfiche edition of the **Federal Register** including the **Federal Register** Index and LSA is \$330, plus postage. Six month subscriptions are available for one-half the annual rate. The prevailing postal rates will be applied to orders according to the delivery method requested. The price of a single copy of the daily **Federal Register**, including postage, is based on the number of pages: \$11 for an issue containing less than 200 pages; \$22 for an issue containing 200 to 400 pages; and \$33 for an issue containing more than 400 pages. Single issues of the microfiche edition may be purchased for \$3 per copy, including postage. Remit check or money order, made payable to the Superintendent of Documents, or charge to your GPO Deposit Account, VISA, MasterCard, American Express, or Discover. Mail to: U.S. Government Publishing Office—New Orders, P.O. Box 979050, St. Louis, MO 63197-9000; or call toll free 1-866-512-1800, DC area 202-512-1800; or go to the U.S. Government Online Bookstore site, see bookstore.gpo.gov.

There are no restrictions on the republication of material appearing in the **Federal Register**.

How To Cite This Publication: Use the volume number and the page number. Example: 88 FR 12345.

Postmaster: Send address changes to the Superintendent of Documents, Federal Register, U.S. Government Publishing Office, Washington, DC 20402, along with the entire mailing label from the last issue received.

SUBSCRIPTIONS AND COPIES

PUBLIC

Subscriptions:

Paper or fiche	202-512-1800
Assistance with public subscriptions	202-512-1806

General online information 202-512-1530; 1-888-293-6498

Single copies/back copies:

Paper or fiche	202-512-1800
Assistance with public single copies	1-866-512-1800 (Toll-Free)

FEDERAL AGENCIES

Subscriptions:

Assistance with Federal agency subscriptions:

Email	FRSubscriptions@nara.gov
Phone	202-741-6000

The Federal Register Printing Savings Act of 2017 (Pub. L. 115-120) placed restrictions on distribution of official printed copies of the daily **Federal Register** to members of Congress and Federal offices. Under this Act, the Director of the Government Publishing Office may not provide printed copies of the daily **Federal Register** unless a Member or other Federal office requests a specific issue or a subscription to the print edition. For more information on how to subscribe use the following website link: <https://www.gpo.gov/frsubs>.



Contents

Federal Register

Vol. 88, No. 65

Wednesday, April 5, 2023

Agency for International Development

NOTICES

Performance Review Board Members, 20118

Agriculture Department

See Forest Service

Centers for Disease Control and Prevention

NOTICES

Laboratory Recommendations:

Syphilis Testing in the United States, 20169–20170

Coast Guard

PROPOSED RULES

Drawbridge Operations:

Cheboygan River at Cheboygan, MI, 20082–20084

Safety Zones:

Delaware Bay, Lower Township, NJ, 20084–20086

Commerce Department

See Foreign-Trade Zones Board

See Industry and Security Bureau

See International Trade Administration

See National Oceanic and Atmospheric Administration

See Patent and Trademark Office

Commodity Futures Trading Commission

NOTICES

Privacy Act; System of Records, 20141–20149

Education Department

NOTICES

Agency Information Collection Activities; Proposals, Submissions, and Approvals:

Request for Title IV Reimbursement or Heightened Cash Monitoring 2, 20149–20150

Applications for New Awards:

Disability Innovation Fund, Pathways to Partnerships Innovative Model Demonstration Project, 20150–20159

Employment and Training Administration

NOTICES

Meetings:

Native American Employment and Training Council, 20189–20190

Energy Department

See Federal Energy Regulatory Commission

See Southwestern Power Administration

Environmental Protection Agency

PROPOSED RULES

Air Quality State Implementation Plans; Approvals and Promulgations:

California; Sacramento Metropolitan Air Quality Management District, 20086–20092

National Primary Drinking Water Regulations:

Consumer Confidence Report Rule Revisions, 20092–20115

NOTICES

Agency Information Collection Activities; Proposals, Submissions, and Approvals:

Clean Water Act Water Quality Certification, 20165–20166

Proposed Consent Decree:

Clean Air Act Citizen Suit, 20166–20167

Federal Aviation Administration

RULES

Airworthiness Directives:

CFM International, S.A. Turbofan Engines, 20059–20062

Dassault Aviation Airplanes, 20062–20065

General Electric Company Turbofan Engines, 20067–20070

The Boeing Company Airplanes, 20065–20067, 20070–20073

Standard Instrument Approach Procedures, and Takeoff Minimums and Obstacle Departure Procedures; Miscellaneous Amendments, 20073–20076

NOTICES

Agency Information Collection Activities; Proposals, Submissions, and Approvals:

Application for Employment with the Federal Aviation Administration, 20203–20204

Airport Property:

Tulsa International Airport, Tulsa, OK, 20205

Petition for Exemption:

AMAC Aerospace Switzerland AG; Summary of Petition Received, 20204–20205

The Boeing Co.; Summary of Petition Received, 20205–20206

Federal Bureau of Investigation

NOTICES

Agency Information Collection Activities; Proposals, Submissions, and Approvals:

Credit Card Payment Form, 20188–20189

Identity History Summary Request Form, 20187–20188

Federal Communications Commission

RULES

Authorizing Permissive Use of the Next Generation Broadcast Television Standard, 20076–20077

NOTICES

Privacy Act; Matching Program, 20167–20168

Federal Energy Regulatory Commission

NOTICES

Combined Filings, 20159–20160, 20162–20163

Guidance:

Revised Final Engineering Guidelines for the Evaluation of Hydropower Projects, 20160–20162

Initial Market-Based Rate Filings Including Requests for Blanket Section 204 Authorizations:

Partin Solar, LLC, 20163

Westlake Natrium, LLC, 20162

Surrender of Preliminary Permit:

SV Hydro, LLC, 20159

Federal Highway Administration**NOTICES**

Environmental Impact Statements; Availability, etc.:
Interstate Bridge Replacement Program, 20206–20207

Federal Maritime Commission**NOTICES**

Agreements Filed, 20168–20169

Federal Transit Administration**NOTICES**

Environmental Impact Statements; Availability, etc.:
Interstate Bridge Replacement Program, 20206–20207

Food and Drug Administration**NOTICES**

Guidance:

Human User Safety in New and Abbreviated New Animal
Drug Applications, 20170–20171

Foreign-Trade Zones Board**NOTICES**

Authorization of Production Activity:
Barco Stamping Co. Inc., Foreign-Trade Zone 219, Yuma,
AZ; Correction, 20119

Forest Service**NOTICES**

Final Permanent Seasonal Hunting Order:
Douglas Ranger District of the Thunder Basin National
Grassland, 20119

Proposed Permanent Recreational Shooting Order:
Laramie Ranger District of the Medicine Bow-Routt
National Forests, 20118–20119

General Services Administration**RULES**

Federal Acquisition Regulations:
Federal Supply Schedule Clause Corrections, 20077–
20079

Health and Human Services Department

See Centers for Disease Control and Prevention
See Food and Drug Administration
See Health Resources and Services Administration
See National Institutes of Health
See Substance Abuse and Mental Health Services
Administration

NOTICES

Medicare Program:
Administrative Law Judge Hearing Program for Medicare
Claim and Entitlement Appeals; Quarterly Listing of
Program Issuances—October through December 2022,
20172–20173

Requests for Nominations:
Advisory Committee on Blood and Tissue Safety and
Availability, 20173–20174
Advisory Council on Alzheimer's Research, Care, and
Services, 20173

Health Resources and Services Administration**NOTICES**

Agency Information Collection Activities; Proposals,
Submissions, and Approvals:
The National Health Service Corps and Nurse Corps
Interest Capture Form, 20171–20172

Homeland Security Department

See Coast Guard

See U.S. Citizenship and Immigration Services

NOTICES

Agency Information Collection Activities; Proposals,
Submissions, and Approvals:
Sector Outreach and Programs Online Meeting
Registration Tool, 20176–20177
Charter Amendments, Establishments, Renewals and
Terminations:
Homeland Security Academic Partnership Council,
20175–20176

Housing and Urban Development Department**NOTICES**

Agency Information Collection Activities; Proposals,
Submissions, and Approvals:
Continuum of Care Homeless Assistance—Technical
Submission, 20179–20180
Disaster Recovery Grant Reporting System, 20178–20179

Industry and Security Bureau**NOTICES**

Agency Information Collection Activities; Proposals,
Submissions, and Approvals:
Five-Year Records Retention Requirement for Export
Transactions and Boycott Actions, 20119–20120

Interior Department

See Land Management Bureau

See National Indian Gaming Commission

See National Park Service

International Trade Administration**NOTICES**

Antidumping or Countervailing Duty Investigations, Orders,
or Reviews:
Acetone from the Republic of Korea, 20122–20124
Ammonium Sulfate from the People's Republic of China,
20124–20125
Biodiesel from Argentina and Indonesia, 20130–20131
Carbon and Alloy Steel Wire Rod from the Republic of
Turkey, 20127
Certain Cold-Rolled Steel Flat Products from the Republic
of Korea, 20128–20130
Certain Hardwood Plywood Products from the People's
Republic of China, 20121–20122
Certain New Pneumatic Off-the-Road Tires from India,
20125–20127
Multilayered Wood Flooring from the People's Republic
of China, 20120–20121

International Trade Commission**NOTICES**

Investigations; Determinations, Modifications, and Rulings,
etc.:
Certain Preserved Mushrooms from the Netherlands,
Poland, and Spain, 20187
Fresh Garlic from China, 20186–20187

Justice Department

See Federal Bureau of Investigation

NOTICES

Agency Information Collection Activities; Proposals,
Submissions, and Approvals:
2023 National Census of Victim Service Providers, 20189

Labor Department

See Employment and Training Administration

See Occupational Safety and Health Administration

Land Management Bureau**NOTICES**

Agency Information Collection Activities; Proposals, Submissions, and Approvals:
Measurement of Oil, 20180–20181

Meetings:

Western Montana Resource Advisory Council, 20181–20182

National Highway Traffic Safety Administration**NOTICES**

Request for Comments:

Crash Investigation Sampling System Expansion, 20207–20208

National Indian Gaming Commission**NOTICES**

Agency Information Collection Activities; Proposals, Submissions, and Approvals, 20182–20185

National Institutes of Health**NOTICES**

Meetings:

National Institute of Environmental Health Sciences, 20175

National Oceanic and Atmospheric Administration**RULES**

Fisheries of the Caribbean, Gulf of Mexico, and South Atlantic:

Re-opening of the Commercial Longline Fishery for Golden Tilefish in the South Atlantic, 20079–20080

Fisheries of the Exclusive Economic Zone Off Alaska:

Pacific Cod by Catcher Vessels Using Trawl Gear in the Bering Sea and Aleutian Islands Management Area, 20080–20081

PROPOSED RULES

Fisheries of the Northeastern United States:

Improvement and Modernization of Atlantic Surfclam and Ocean Quahog Vessel Reporting Regulations, 20115–20117

NOTICES

Agency Information Collection Activities; Proposals, Submissions, and Approvals:

Space-Based Data Collection System Agreements, 20132–20133

Environmental Impact Statements; Availability, etc.:

Proposed Atchafalaya National Estuarine Research Reserve, 20131–20132

Takes of Marine Mammals Incidental to Specified Activities:

Replacement of Pier 3 at Naval Station Norfolk; Norfolk, VA, 20133–20138

National Park Service**NOTICES**

National Register of Historic Places:

Pending Nominations and Related Actions, 20185–20186

National Science Foundation**NOTICES**

Agency Information Collection Activities; Proposals, Submissions, and Approvals:

Grantee Reporting Requirements for the Small Business Innovation Research and the Small Business Technology Transfer Programs, 20192

Nuclear Regulatory Commission**NOTICES**

Licenses; Exemptions, Applications, Amendments etc.:

Susquehanna Steam Electric Station, Units 1 and 2 and the Associated Independent Spent Fuel Storage Installation, Susquehanna Nuclear, LLC, 20193–20194

Occupational Safety and Health Administration**NOTICES**

Agency Information Collection Activities; Proposals, Submissions, and Approvals:

The Standard on 4,4'-Methylenedianiline for General Industry, 20190–20191

Patent and Trademark Office**NOTICES**

Patent Center Electronic Office Action Program, 20138–20141

Pipeline and Hazardous Materials Safety Administration**NOTICES**

Meetings:

Lithium Battery Air Safety Advisory Committee, 20209–20210

Safety of Underground Natural Gas Storage, 20208–20209

Presidential Documents**PROCLAMATIONS**

Special Observances:

Arab American Heritage Month (Proc. 10539), 20355–20358

Care Workers Recognition Month (Proc. 10540), 20359–20360

Education and Sharing Day, USA (Proc. 10548), 20379–20380

Month of the Military Child (Proc. 10541), 20361–20362

National Cancer Control Month (Proc. 10542), 20363–20365

National Child Abuse Prevention Month (Proc. 10543), 20367–20368

National Donate Life Month (Proc. 10544), 20369–20370

National Public Health Week (Proc. 10547), 20375–20377

National Sexual Assault Awareness and Prevention Month (Proc. 10545), 20371–20372

Second Chance Month (Proc. 10546), 20373–20374

World Autism Awareness Day (Proc. 10549), 20381–20382

Science and Technology Policy Office**NOTICES**

Request for Information:

National Nanotechnology Initiative Environmental, Health, and Safety Research Strategy, 20194–20195

Securities and Exchange Commission**PROPOSED RULES**

Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, et al., 20212–20354

NOTICES

Self-Regulatory Organizations; Proposed Rule Changes:

ICE Clear Europe, Ltd., 20200–20202

The Options Clearing Corp., 20195–20200

Southwestern Power Administration**NOTICES**

Integrated System Power Rates, 20163–20165

State Department**NOTICES**

Meetings:

Modernizing the Columbia River Treaty Regime;
Listening Session, 20202

Temporary Waiver and Modification of Certain Regulatory
Requirements:

Exchange Visitor Program, 20202–20203

Substance Abuse and Mental Health Services**Administration****NOTICES**

Meetings:

Center for Substance Abuse Prevention National Advisory
Council, 20175

Transportation Department

See Federal Aviation Administration

See Federal Highway Administration

See Federal Transit Administration

See National Highway Traffic Safety Administration

See Pipeline and Hazardous Materials Safety
Administration

U.S. Citizenship and Immigration Services**NOTICES**

Agency Information Collection Activities; Proposals,
Submissions, and Approvals:

Petition by Investor to Remove Conditions on Permanent
Resident Status, 20177–20178

Separate Parts In This Issue**Part II**

Securities and Exchange Commission, 20212–20354

Part III

Presidential Documents, 20355–20365, 20367–20377,
20379–20382

Reader Aids

Consult the Reader Aids section at the end of this issue for
phone numbers, online resources, finding aids, and notice
of recently enacted public laws.

To subscribe to the Federal Register Table of Contents
electronic mailing list, go to [https://public.govdelivery.com/
accounts/USGPOOFR/subscriber/new](https://public.govdelivery.com/accounts/USGPOOFR/subscriber/new), enter your e-mail
address, then follow the instructions to join, leave, or
manage your subscription.

CFR PARTS AFFECTED IN THIS ISSUE

A cumulative list of the parts affected this month can be found in the Reader Aids section at the end of this issue.

3 CFR

Proclamations:

10539.....	20357
10540.....	20359
10541.....	20361
10542.....	20363
10543.....	20367
10544.....	20369
10545.....	20371
10546.....	20373
10547.....	20375
10548.....	20379
10549.....	20381

14 CFR

39 (5 documents)	20059,
20062, 20065, 20067, 20070	
97 (2 documents)	20073,
20074	

17 CFR

Proposed Rules:

232.....	20212
240.....	20212
242.....	20212
249.....	20212

33 CFR

Proposed Rules:

117.....	20082
165.....	20084

40 CFR

Proposed Rules:

52.....	20086
141.....	20092
142.....	20092

47 CFR

73.....	20076
---------	-------

48 CFR

538.....	20077
552.....	20077

50 CFR

622.....	20079
679.....	20080

Proposed Rules:

648.....	20015
----------	-------

Rules and Regulations

Federal Register

Vol. 88, No. 65

Wednesday, April 5, 2023

This section of the FEDERAL REGISTER contains regulatory documents having general applicability and legal effect, most of which are keyed to and codified in the Code of Federal Regulations, which is published under 50 titles pursuant to 44 U.S.C. 1510.

The Code of Federal Regulations is sold by the Superintendent of Documents.

DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

14 CFR Part 39

[Docket No. FAA-2022-1405; Project Identifier AD-2022-01070-E; Amendment 39-22374; AD 2023-05-05]

RIN 2120-AA64

Airworthiness Directives; CFM International, S.A. Turbofan Engines

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Final rule.

SUMMARY: The FAA is superseding Airworthiness Directive (AD) 2021-10-09 for certain CFM International, S.A. (CFM) CFM56-5B and CFM56-7B model turbofan engines with a certain high-pressure turbine (HPT) inner stationary seal installed. AD 2021-10-09 required removal, inspection, and replacement of the affected HPT inner stationary seal and, depending on the findings, replacement of the rotating air HPT front seal, HPT rotor blades, and No. 3 ball bearing. This AD was prompted by cracks found in the rotating air HPT front seal. After the FAA issued AD 2021-10-09, the manufacturer notified the FAA that the service information incorrectly lists the year of certain honeycomb repairs and that affected HPT inner stationary seals could potentially be installed on CFM CFM56-5C model turbofan engines. This AD requires removal, inspection, and replacement of the affected HPT inner stationary seal and, depending on the findings, replacement of the rotating air HPT front seal, HPT rotor blades, and No. 3 ball bearing. This AD also revises the applicability to add CFM CFM56-5C model turbofan engines. The FAA is issuing this AD to address the unsafe condition on these products.

DATES: This AD is effective May 10, 2023.

The Director of the Federal Register approved the incorporation by reference

of certain publications listed in this AD as of May 10, 2023.

ADDRESSES:

AD Docket: You may examine the AD docket at *regulations.gov* by searching for and locating Docket No. FAA-2022-1405; or in person at Docket Operations between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. The AD docket contains this final rule, any comments received, and other information. The address for Docket Operations is U.S. Department of Transportation, Docket Operations, M-30, West Building Ground Floor, Room W12-140, 1200 New Jersey Avenue SE, Washington, DC 20590.

Material Incorporated by Reference:

- For CFM service information identified in this final rule, contact CFM International Inc., Aviation Operations Center, 1 Neumann Way, M/D Room 285, Cincinnati, OH 45125; phone: (877) 432-3272; email: *aviation.fleetsupport@ge.com*.

- You may view this service information at the FAA, Airworthiness Products Section, Operational Safety Branch, 1200 District Avenue, Burlington, MA 01803. For information on the availability of this material at the FAA, call (817) 222-5110. It is also available at *regulations.gov* by searching for and locating Docket No. FAA-2022-1405.

FOR FURTHER INFORMATION CONTACT:

Kevin Clark, Aviation Safety Engineer, ECO Branch, FAA, 1200 District Avenue, Burlington, MA 01803; phone: (781) 238-7088; email: *kevin.m.clark@faa.gov*.

SUPPLEMENTARY INFORMATION:

Background

The FAA issued a notice of proposed rulemaking (NPRM) to amend 14 CFR part 39 to supersede AD 2021-10-09, Amendment 39-21542 (86 FR 27264, May 20, 2021) (AD 2021-10-09). AD 2021-10-09 applied to certain CFM CFM56-5B and CFM56-7B model turbofan engines with an HPT inner stationary seal, part number 1808M56G01, installed. The NPRM published in the **Federal Register** on December 1, 2022 (87 FR 73683). The NPRM was prompted by cracks found in the rotating air HPT front seal. After the FAA issued AD 2021-10-09, the manufacturer notified the FAA that the service information referenced in AD 2021-10-09 incorrectly listed the year

of certain honeycomb repairs. Additionally, the manufacturer notified the FAA that affected HPT inner stationary seals could potentially be installed on CFM CFM56-5C model turbofan engines. In the NPRM, the FAA proposed to require removal, inspection, and replacement of the affected HPT inner stationary seal and, depending on the findings, replacement of the rotating air HPT front seal, HPT rotor blades, and No. 3 ball bearing. In the NPRM, the FAA also proposed to revise the applicability to add CFM CFM56-5C model turbofan engines.

Discussion of Final Airworthiness Directive

Comments

The FAA received comments from three commenters. The commenters were Air Line Pilots Association, International (ALPA), American Airlines (AA), and The Boeing Company (Boeing). The following presents the comments received on the NPRM and the FAA's response to each comment.

Support for the AD

ALPA and Boeing supported the NPRM without change.

Request To Specify Service Bulletins and Revision Numbers

AA requested that the FAA specify service bulletins and their respective revision numbers throughout this AD. AA stated that paragraph (c), Applicability, references the service bulletins as follows, CFM Service Bulletin (SB) CFM56-5B S/B 72-0952, Revision 02, dated August 10, 2022 (CFM SB CFM56-5B S/B 72-0952); CFM SB CFM56-5C S/B 72-0796, Revision 02, dated August 10, 2022 (CFM SB CFM56-5C S/B 72-0796); CFM SB CFM56-7B S/B 72-1054, Revision 02, dated August 10, 2022 (CFM SB CFM56-7B S/B 72-1054). AA noted that the SB format within the parentheses abridges the complete description of the service bulletins and is used in proposed paragraphs (g)(2), (h)(2)(i), and (2)(ii). AA reasoned that this SB format could be interpreted as the original (basic) service bulletin, which provides outdated accomplishment instructions and could contribute to errors during the accomplishment of this AD.

The FAA established a shorthand notation in paragraph (c), Applicability,

of the NPRM for each service bulletin, which contained the full citation, including the manufacturer name, SB number, revision number, and date, followed by the shorthand notation. The FAA then used the established shorthand notation to reference the service bulletins in paragraphs (g)(2), (h)(2)(i), and (2)(ii), as applicable, of the NPRM. Avoiding the use of the shorthand notation and including the revision numbers and dates for each SB reference is unnecessary, as the referenced service information is defined in both the preamble and the AD body. The FAA did not change this AD as a result of this comment.

Request To Revise Paragraph (c) of This AD

AA requested that the FAA revise paragraph (c), Applicability, of this AD to include the following, “This AD does not apply to affected CFM56–5B and CFM56–7B model turbofan engines with the affected HPT inner stationary seal installed if the seal has been repaired as specified in CFM56 Engine Shop Manual (ESM), 72–41–03, REPAIR 003 after December 31, 2012 and prior to the effective date, June 24, 2021, of FAA AD 2021–10–09.” AA reasoned that this language was part of AD 2021–10–09,

paragraph (c), Applicability. The exclusion of this text from the final rule would make the population of HPT inner stationary seals, within the previously identified time frame, applicable to the proposed AD.

In response to this comment, the FAA has revised paragraph (c), Applicability, of this AD to include: “This AD does not apply to affected CFM CFM56–5B, CFM56–5C, and CFM56–7B model turbofan engines with the affected HPT inner stationary seal installed if the seal has been repaired as specified in CFM56–5B ESM, 72–41–03, REPAIR 003; CFM56–5C ESM, 72–41–03, REPAIR 003; or CFM56–7B ESM, 72–41–03, REPAIR 003, after December 31, 2012.”

Conclusion

The FAA reviewed the relevant data, considered any comments received, and determined that air safety requires adopting the AD as proposed. Accordingly, the FAA is issuing this AD to address the unsafe condition on these products. Except for minor editorial changes, and any other changes described previously, this AD is adopted as proposed in the NPRM. None of the changes will increase the economic burden on any operator.

Related Service Information Under 1 CFR Part 51

The FAA reviewed the following service information:

- CFM SB CFM56–5C S/B 72–0796, Revision 02, dated August 10, 2022.
- CFM SB CFM56–5B S/B 72–0952, Revision 02, dated August 10, 2022.
- CFM SB CFM56–7B S/B 72–1054, Revision 02, dated August 10, 2022.

This service information, differentiated by engine model, specifies procedures for inspecting the HPT inner stationary seal honeycomb. This service information is reasonably available because the interested parties have access to it through their normal course of business or by the means identified in the ADDRESSES section.

Costs of Compliance

The FAA estimates that this AD affects 210 engines installed on airplanes of U.S. registry. Operators have the option to replace or repair the affected HPT inner stationary seal. The parts cost includes the estimated costs for replacement with a repaired HPT inner stationary seal.

The FAA estimates the following costs to comply with this AD:

ESTIMATED COSTS

Action	Labor cost	Parts cost	Cost per product	Cost on U.S. operators
Replace HPT inner stationary seal	1 work-hour × \$85 per hour = \$85	\$7,910	\$7,995	\$1,678,950
Inspect HPT inner stationary seal	1 work-hour × \$85 per hour = \$85	0	85	17,850

The FAA estimates the following costs to do any necessary replacements that would be required based on the

results of the inspection. The agency has no way of determining the number of

engines that might need these replacements:

ON-CONDITION COSTS

Action	Labor cost	Parts cost	Cost per product
Replace rotating air HPT front seal	1 work-hour × \$85 per hour = \$85	\$344,600	\$344,685
Replace HPT rotor blades (pair)	1 work-hour × \$85 per hour = \$85	31,000	31,085
Replace No. 3 ball bearing	1 work-hour × \$85 per hour = \$85	30,000	30,085

Authority for This Rulemaking

Title 49 of the United States Code specifies the FAA’s authority to issue rules on aviation safety. Subtitle I, Section 106, describes the authority of the FAA Administrator. Subtitle VII, Aviation Programs, describes in more detail the scope of the Agency’s authority.

The FAA is issuing this rulemaking under the authority described in Subtitle VII, Part A, Subpart III, Section

44701, General requirements. Under that section, Congress charges the FAA with promoting safe flight of civil aircraft in air commerce by prescribing regulations for practices, methods, and procedures the Administrator finds necessary for safety in air commerce. This regulation is within the scope of that authority because it addresses an unsafe condition that is likely to exist or develop on products identified in this rulemaking action.

Regulatory Findings

The FAA has determined that this AD will not have federalism implications under Executive Order 13132. This AD will not have a substantial direct effect on the States, on the relationship between the national government and the States, or on the distribution of power and responsibilities among the various levels of government.

For the reasons discussed above, I certify that this AD:

- (1) Is not a “significant regulatory action” under Executive Order 12866,
- (2) Will not affect intrastate aviation in Alaska, and
- (3) Will not have a significant economic impact, positive or negative, on a substantial number of small entities under the criteria of the Regulatory Flexibility Act.

List of Subjects in 14 CFR Part 39

Air transportation, Aircraft, Aviation safety, Incorporation by reference, Safety.

The Amendment

Accordingly, under the authority delegated to me by the Administrator, the FAA amends 14 CFR part 39 as follows:

PART 39—AIRWORTHINESS DIRECTIVES

■ 1. The authority citation for part 39 continues to read as follows:

Authority: 49 U.S.C. 106(g), 40113, 44701.

§ 39.13 [Amended]

- 2. The FAA amends § 39.13 by:
 - a. Removing Airworthiness Directive 2021–10–09, Amendment 39–21542 (86 FR 27264, May 20, 2021); and
 - b. Adding the following new airworthiness directive:

2023–05–05 CFM International, S.A.:
Amendment 39–22374; Docket No. FAA–2022–1405; Project Identifier AD–2022–01070–E.

(a) Effective Date

This airworthiness directive (AD) is effective May 10, 2023.

(b) Affected ADs

This AD replaces AD 2021–10–09, Amendment 39–21542 (86 FR 27264, May 20, 2021) (AD 2021–10–09).

(c) Applicability

This AD applies to CFM International, S.A. (CFM) model turbofan engines identified in Table 1 to paragraph (c) of this AD with an

installed high-pressure turbine (HPT) inner stationary seal, part number (P/N) 1808M56G01, that has a serial number (S/N) listed in Table 1 of CFM Service Bulletin (SB) CFM56–5B S/B 72–0952, Revision 02, dated August 10, 2022 (CFM SB CFM56–5B S/B 72–0952); Table 1 of CFM SB CFM56–5C S/B 72–0796, Revision 02, dated August 10, 2022 (CFM SB CFM56–5C S/B 72–0796); or Table 1 of CFM SB CFM56–7B S/B 72–1054, Revision 02, dated August 10, 2022 (CFM SB CFM56–7B S/B 72–1054). This AD does not apply to affected CFM CFM56–5B, CFM56–5C, and CFM56–7B model turbofan engines with the affected HPT inner stationary seal installed if the seal has been repaired as specified in CFM56–5B Engine Shop Manual (ESM), 72–41–03, REPAIR 003; CFM56–5C ESM, 72–41–03, REPAIR 003; or CFM56–7B ESM, 72–41–03, REPAIR 003, after December 31, 2012.

TABLE 1 TO PARAGRAPH (c)—CFM MODEL TURBOFAN ENGINES

Make	Model
CFM	CFM56–5B1, CFM56–5B1/2P, CFM56–5B1/3, CFM56–5B1/P, CFM56–5B2, CFM56–5B2/2P, CFM56–5B2/3, CFM56–5B2/P, CFM56–5B3/2P, CFM56–5B3/2P1, CFM56–5B3/3, CFM56–5B3/3B1, CFM56–5B3/P, CFM56–5B3/P1, CFM56–5B4, CFM56–5B4/2P, CFM56–5B4/2P1, CFM56–5B4/3, CFM56–5B4/3B1, CFM56–5B4/P, CFM56–5B4/P1, CFM56–5B5, CFM56–5B5/3, CFM56–5B5/P, CFM56–5B6, CFM56–5B6/2P, CFM56–5B6/3, CFM56–5B6/P, CFM56–5B7, CFM56–5B7/3, CFM56–5B7/P, CFM56–5B8/3, CFM56–5B8/P, CFM56–5B9/2P, CFM56–5B9/3, CFM56–5B9/P.
CFM	CFM56–5C2, CFM56–5C2/4, CFM56–5C2/F, CFM56–5C2/F4, CFM56–5C2/G, CFM56–5C2/G4, CFM56–5C2/P, CFM56–5C3/F, CFM56–5C3/F4, CFM56–5C3/G, CFM56–5C3/G4, CFM56–5C3/P, CFM56–5C4, CFM56–5C4/1, CFM56–5C4/1P, CFM56–5C4/P.
CFM	CFM56–7B20, CFM56–7B20/2, CFM56–7B20/3, CFM56–7B20E, CFM56–7B22, CFM56–7B22/2, CFM56–7B22/3, CFM56–7B22/3B1, CFM56–7B22/B1, CFM56–7B22E, CFM56–7B22E/B1, CFM56–7B24, CFM56–7B24/2, CFM56–7B24/3, CFM56–7B24/3B1, CFM56–7B24/B1, CFM56–7B24E, CFM56–7B24E/B1, CFM56–7B26, CFM56–7B26/2, CFM56–7B26/3, CFM56–7B26/3B1, CFM56–7B26/3B2, CFM56–7B26/3B2F, CFM56–7B26/3F, CFM56–7B26/B1, CFM56–7B26/B2, CFM56–7B26E, CFM56–7B26E/B1, CFM56–7B26E/B2, CFM56–7B26E/B2F, CFM56–7B26E/F, CFM56–7B27, CFM56–7B27/2, CFM56–7B27/3, CFM56–7B27/3B1, CFM56–7B27/3B1F, CFM56–7B27/3B3, CFM56–7B27/3F, CFM56–7B27/B1, CFM56–B27/B3, CFM56–7B27A, CFM56–7B27A/3, CFM56–7B27AE, CFM56–7B27E, CFM56–7B27E/B1, CFM56–7B27E/B1F, CFM56–7B27E/B3, CFM56–7B27E/F.

(d) Subject

Joint Aircraft System Component (JASC) Code 7230, Turbine Engine Compressor Section.

(e) Unsafe Condition

This AD was prompted by cracks found in the rotating air HPT front seal. The FAA is issuing this AD to prevent failure of the HPT inner stationary seal and the rotating air HPT front seal. The unsafe condition, if not addressed, could result in uncontained release of the rotating air HPT front seal, damage to the engine, and damage to the airplane.

(f) Compliance

Comply with this AD within the compliance times specified, unless already done.

(g) Required Actions

(1) At the next engine shop visit after the effective date of this AD, remove the affected HPT inner stationary seal and replace with an HPT inner stationary seal that is eligible for installation.

(2) After removing the affected HPT inner stationary seal required by paragraph (g)(1) of this AD, inspect the removed HPT inner stationary seal for honeycomb separation in accordance with the Accomplishment Instructions, paragraph 3.C.(1), of CFM SB CFM56–5B S/B 72–0952; CFM SB CFM56–5C S/B 72–0796; or CFM SB CFM56–7B S/B 72–1054, as applicable by engine model.

(3) If honeycomb separation is found during the inspection required by paragraph (g)(2) of this AD, before further flight:

(i) Remove the rotating air HPT front seal from service and replace with a rotating air HPT front seal that is eligible for installation.

(ii) Remove the HPT rotor blades and replace with HPT rotor blades eligible for installation.

(iii) Remove the No. 3 ball bearing from service and replace with a No. 3 ball bearing eligible for installation.

(h) Definitions

(1) For the purpose of this AD, an “engine shop visit” is the induction of an engine into the shop for maintenance involving the separation of pairs of major mating engine case flanges, except for the following situations, which do not constitute an engine shop visit.

(i) Separation of engine flanges solely for the purpose of transportation of the engine without subsequent maintenance.

(ii) Separation of engine flanges solely for the purpose of replacing the fan or propulsor without subsequent maintenance.

(2) For the purpose of this AD, an “HPT inner stationary seal that is eligible for installation” is an HPT inner stationary seal:

(i) That is not listed in Table 1 of CFM SB CFM56-5B S/B 72-0952; Table 1 of CFM SB CFM56-5C S/B 72-0796; or Table 1 of CFM SB CFM56-7B S/B 72-1054; or

(ii) With a P/N 1808M56G01 and an S/N listed in Table 1 of CFM SB CFM56-5B S/B 72-0952; Table 1 of CFM SB CFM56-5C S/B 72-0796; or Table 1 of CFM SB CFM56-7B S/B 72-1054, that has been repaired as specified in CFM56-5B ESM, 72-41-03, REPAIR 003; CFM56-5C ESM, 72-41-03, REPAIR 003; or CFM56-7B ESM, 72-41-03, REPAIR 003, as applicable by engine model, after December 31, 2012.

(3) For the purpose of this AD, a “rotating air HPT front seal that is eligible for installation” is any rotating air HPT front seal that was not removed from service as a result of the inspection of the HPT inner stationary seal required by paragraph (g)(2) of this AD in which there was a finding of honeycomb separation.

(4) For the purpose of this AD, “HPT rotor blades eligible for installation” are new HPT rotor blades with zero flight hours since new or HPT rotor blades that have been inspected and returned to a serviceable condition using FAA-approved maintenance procedures.

(5) For the purpose of this AD, a “No. 3 ball bearing eligible for installation” is any No. 3 ball bearing that was not removed from service as a result of the inspection of the HPT inner stationary seal required by paragraph (g)(2) of this AD in which there was a finding of honeycomb separation.

(i) Credit for Previous Actions

You may take credit for the actions specified in paragraphs (g)(1) through (3) of this AD, if you performed those actions before the effective date of this AD using CFM SB CFM56-5B S/B 72-0952, Revision 01, dated January 15, 2020, CFM SB CFM56-7B S/B 72-1054, Revision 01, dated January 15, 2020, or CFM SB CFM56-5C S/B 72-0796, Revision 01, dated January 15, 2020.

(j) Alternative Methods of Compliance (AMOCs)

(1) The Manager, ECO Branch, FAA, has the authority to approve AMOCs for this AD, if requested using the procedures found in 14 CFR 39.19. In accordance with 14 CFR 39.19, send your request to your principal inspector or local Flight Standards District Office, as appropriate. If sending information directly to the manager of the certification office, send it to the attention of the person identified in paragraph (k) of this AD and email to: ANE-AD-AMOC@faa.gov.

(2) Before using any approved AMOC, notify your appropriate principal inspector, or lacking a principal inspector, the manager of the local flight standards district office/certificate holding district office.

(3) AMOCs approved for AD 2021-10-09 (86 FR 27264, May 20, 2021) are approved as AMOCs for the corresponding provisions of this AD.

(k) Related Information

For more information about this AD, contact Kevin Clark, Aviation Safety Engineer, ECO Branch, FAA, 1200 District

Avenue, Burlington, MA 01803; phone: (781) 238-7088; email: kevin.m.clark@faa.gov.

(l) Material Incorporated by Reference

(1) The Director of the Federal Register approved the incorporation by reference of the service information listed in this paragraph under 5 U.S.C. 552(a) and 1 CFR part 51.

(2) You must use this service information as applicable to do the actions required by this AD, unless the AD specifies otherwise.

(i) CFM Service Bulletin CFM56-5C S/B 72-0796, Revision 02, dated August 10, 2022.

(ii) CFM Service Bulletin CFM56-5B S/B 72-0952, Revision 02, dated August 10, 2022.

(iii) CFM Service Bulletin CFM56-7B S/B 72-1054, Revision 02, dated August 10, 2022.

(3) For CFM service information identified in this AD, contact CFM International Inc., Aviation Operations Center, 1 Neumann Way, M/D Room 285, Cincinnati, OH 45125; phone: (877) 432-3272; email: aviation.fleetsupport@ge.com.

(4) You may view this service information at the FAA, Airworthiness Products Section, Operational Safety Branch, 1200 District Avenue, Burlington, MA 01803. For information on the availability of this material at the FAA, call (817) 222-5110.

(5) You may view this service information that is incorporated by reference at the National Archives and Records Administration (NARA). For information on the availability of this material at NARA, email: fr.inspection@nara.gov, or go to: www.archives.gov/federal-register/cfr/ibr-locations.html.

Issued on March 5, 2023.

Christina Underwood,

Acting Director, Compliance & Airworthiness Division, Aircraft Certification Service.

[FR Doc. 2023-07003 Filed 4-4-23; 8:45 am]

BILLING CODE 4910-13-P

DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

14 CFR Part 39

[Docket No. FAA-2022-1579; Project Identifier MCAI-2022-00903-T; Amendment 39-22362; AD 2023-04-15]

RIN 2120-AA64

Airworthiness Directives; Dassault Aviation Airplanes

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Final rule.

SUMMARY: The FAA is superseding Airworthiness Directive (AD) 2021-09-12, which applied to certain Dassault Aviation Model FALCON 7X airplanes. AD 2021-09-12 required revising the existing maintenance or inspection program, as applicable, to incorporate new or more restrictive airworthiness limitations. This AD was prompted by

a determination that new or more restrictive airworthiness limitations are necessary. This AD continues to require the actions in AD 2021-09-12 and requires revising the existing maintenance or inspection program, as applicable, to incorporate additional new or more restrictive airworthiness limitations, as specified in a European Union Aviation Safety Agency (EASA) AD, which is incorporated by reference. The FAA is issuing this AD to address the unsafe condition on these products.

DATES: This AD is effective May 10, 2023.

The Director of the Federal Register approved the incorporation by reference of a certain publication listed in this AD as of May 10, 2023.

The Director of the Federal Register approved the incorporation by reference of a certain other publication listed in this AD as of June 8, 2021 (86 FR 23593, May 4, 2021).

ADDRESSES:

AD Docket: You may examine the AD docket at regulations.gov under Docket No. FAA-2022-1579; or in person at Docket Operations between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. The AD docket contains this final rule, the mandatory continuing airworthiness information (MCAI), any comments received, and other information. The address for Docket Operations is U.S. Department of Transportation, Docket Operations, M-30, West Building Ground Floor, Room W12-140, 1200 New Jersey Avenue SE, Washington, DC 20590.

Material Incorporated by Reference:

- For material incorporated by reference in this AD, contact EASA, Konrad-Adenauer-Ufer 3, 50668 Cologne, Germany; telephone +49 221 8999 000; email ADs@easa.europa.eu; website easa.europa.eu. You may find this material on the EASA website at ad.easa.europa.eu.

- You may view this material at the FAA, Airworthiness Products Section, Operational Safety Branch, 2200 South 216th St., Des Moines, WA. For information on the availability of this material at the FAA, call 206-231-3195. It is also available in the AD docket at regulations.gov under Docket No. FAA-2022-1579.

FOR FURTHER INFORMATION CONTACT: Tom Rodriguez, Aerospace Engineer, Large Aircraft Section, International Validation Branch, FAA, 2200 South 216th St., Des Moines, WA 98198; telephone and fax 206-231-3226; email tom.rodriguez@faa.gov.

SUPPLEMENTARY INFORMATION:

Background

The FAA issued a notice of proposed rulemaking (NPRM) to amend 14 CFR part 39 to supersede AD 2021–09–12, Amendment 39–21526 (86 FR 23593, May 4, 2021) (AD 2021–09–12). AD 2021–09–12 applied to certain Dassault Aviation Model FALCON 7X airplanes. AD 2021–09–12 required revising the existing maintenance or inspection program, as applicable, to incorporate new or more restrictive airworthiness limitations. The FAA issued AD 2021–09–12 to address reduced structural integrity and reduced control of airplanes due to the failure of system components. AD 2021–09–12 specified that accomplishing the revision required by that AD terminates certain requirements of AD 2014–16–23, Amendment 39–17947 (79 FR 52545, September 4, 2014) (AD 2014–16–23).

The NPRM published in the **Federal Register** on December 13, 2022 (87 FR 76151). The NPRM was prompted by AD 2022–0142, dated July 7, 2022, issued by EASA (EASA AD 2022–0142) (also referred to as the MCAI). The MCAI states that new or more restrictive airworthiness limitations have been issued.

You may examine the MCAI in the AD docket at regulations.gov under Docket No. FAA–2022–1579.

In the NPRM, the FAA proposed to continue to require the actions in AD 2021–09–12, and to require revising the existing maintenance or inspection program, as applicable, to incorporate new or more restrictive airworthiness limitations, as specified in EASA AD 2022–0142. The FAA is issuing this AD to address reduced structural integrity and reduced control of airplanes due to the failure of system components.

Discussion of Final Airworthiness Directive

Comments

The FAA received no comments on the NPRM or on the determination of the cost to the public.

Conclusion

This product has been approved by the aviation authority of another country and is approved for operation in the United States. Pursuant to the FAA's bilateral agreement with this State of Design Authority, it has notified the FAA of the unsafe condition described in the MCAI referenced above. The FAA reviewed the relevant data and determined that air safety requires adopting this AD as proposed. Accordingly, the FAA is issuing this AD to address the unsafe condition on this product. Except for minor editorial

changes, this AD is adopted as proposed in the NPRM. None of the changes will increase the economic burden on any operator.

Related Service Information Under 1 CFR Part 51

The FAA reviewed EASA AD 2022–0142. This service information specifies new or more restrictive airworthiness limitations for airplane structures and safe life limits.

This AD also requires EASA AD 2020–0214, dated October 6, 2020, which the Director of the Federal Register approved for incorporation by reference as of June 8, 2021 (86 FR 23593, May 4, 2021).

This material is reasonably available because the interested parties have access to it through their normal course of business or by the means identified in the **ADDRESSES** section.

Costs of Compliance

The FAA estimates that this AD affects 122 airplanes of U.S. registry. The FAA estimates the following costs to comply with this AD:

The FAA estimates the total cost per operator for the retained actions from AD 2021–09–12 to be \$7,650 (90 work-hours × \$85 per work-hour).

The FAA has determined that revising the existing maintenance or inspection program takes an average of 90 work-hours per operator, although the agency recognizes that this number may vary from operator to operator. Since operators incorporate maintenance or inspection program changes for their affected fleet(s), the FAA has determined that a per-operator estimate is more accurate than a per-airplane estimate. The FAA estimates the total cost per operator for the new actions to be \$7,650 (90 work-hours × \$85 per work-hour).

Authority for This Rulemaking

Title 49 of the United States Code specifies the FAA's authority to issue rules on aviation safety. Subtitle I, section 106, describes the authority of the FAA Administrator. Subtitle VII: Aviation Programs, describes in more detail the scope of the Agency's authority.

The FAA is issuing this rulemaking under the authority described in Subtitle VII, Part A, Subpart III, Section 44701: General requirements. Under that section, Congress charges the FAA with promoting safe flight of civil aircraft in air commerce by prescribing regulations for practices, methods, and procedures the Administrator finds necessary for safety in air commerce. This regulation is within the scope of

that authority because it addresses an unsafe condition that is likely to exist or develop on products identified in this rulemaking action.

Regulatory Findings

This AD will not have federalism implications under Executive Order 13132. This AD will not have a substantial direct effect on the States, on the relationship between the national government and the States, or on the distribution of power and responsibilities among the various levels of government.

For the reasons discussed above, I certify that this AD:

- (1) Is not a “significant regulatory action” under Executive Order 12866,
- (2) Will not affect intrastate aviation in Alaska, and
- (3) Will not have a significant economic impact, positive or negative, on a substantial number of small entities under the criteria of the Regulatory Flexibility Act.

List of Subjects in 14 CFR Part 39

Air transportation, Aircraft, Aviation safety, Incorporation by reference, Safety.

The Amendment

Accordingly, under the authority delegated to me by the Administrator, the FAA amends 14 CFR part 39 as follows:

PART 39—AIRWORTHINESS DIRECTIVES

- 1. The authority citation for part 39 continues to read as follows:

Authority: 49 U.S.C. 106(g), 40113, 44701.

§ 39.13 [Amended]

- 2. The FAA amends § 39.13 by:
 - a. Removing Airworthiness Directive (AD) 2021–09–12, Amendment 39–21526 (86 FR 23593, May 4, 2021); and
 - b. Adding the following new AD:

2023–04–15 Dassault Aviation:

Amendment 39–22362; Docket No. FAA–2022–1579; Project Identifier MCAI–2022–00903–T.

(a) Effective Date

This airworthiness directive (AD) is effective May 10, 2023.

(b) Affected ADs

(1) This AD replaces AD 2021–09–12, Amendment 39–21526 (86 FR 23593, May 4, 2021) (AD 2021–09–12).

(2) This AD affects AD 2014–16–23, Amendment 39–17947 (79 FR 52545, September 4, 2014) (AD 2014–16–23).

(c) Applicability

This AD applies to Dassault Aviation Model FALCON 7X airplanes, certificated in

any category, with an original airworthiness certificate or original export certificate of airworthiness issued on or before June 7, 2021.

Note 1 to paragraph (c): Model FALCON 7X airplanes with modification M1000 incorporated are commonly referred to as “Model FALCON 8X” airplanes as a marketing designation.

(d) Subject

Air Transport Association (ATA) of America Code 05, Time Limits/Maintenance Checks.

(e) Unsafe Condition

This AD was prompted by a determination that new or more restrictive airworthiness limitations are necessary. The FAA is issuing this AD to address reduced structural integrity and reduced control of airplanes due to the failure of system components.

(f) Compliance

Comply with this AD within the compliance times specified, unless already done.

(g) Retained Revision of the Existing Maintenance or Inspection Program, With No Changes

This paragraph restates the requirements of paragraph (j) of AD 2021–09–12, with no changes. For airplanes with an original airworthiness certificate or original export certificate of airworthiness issued on or before June 1, 2020, except as specified in paragraph (h) of this AD: Comply with all required actions and compliance times specified in, and in accordance with, European Union Aviation Safety Agency (EASA) AD 2020–0214, dated October 6, 2020 (EASA AD 2020–0214). Accomplishing the revision of the existing maintenance or inspection program required by paragraph (j) of this AD terminates the requirements of this paragraph.

(h) Retained Exceptions to EASA AD 2020–0214, With No Changes

This paragraph restates the exceptions specified in paragraph (k) of AD 2021–09–12, with no changes.

(1) The requirements specified in paragraphs (1) and (2) of EASA AD 2020–0214 do not apply to this AD.

(2) Paragraph (3) of EASA AD 2020–0214 specifies revising “the approved AMP” within 12 months after its effective date, but this AD requires revising the existing maintenance or inspection program, as applicable, to incorporate the “limitations, tasks and associated thresholds and intervals” specified in paragraph (3) of EASA AD 2020–0214 within 90 days after June 8, 2021 (the effective date of AD 2021–09–12).

(3) The initial compliance time for doing the tasks specified in paragraph (3) of EASA AD 2020–0214 is at the applicable “associated thresholds” specified in paragraph (3) of EASA AD 2020–0214, or within 90 days after June 8, 2021 (the effective date of AD 2021–09–12), whichever occurs later.

(4) The provisions specified in paragraphs (4) and (5) of EASA AD 2019–0257 do not apply to this AD.

(5) The “Remarks” section of EASA AD 2020–0214 does not apply to this AD.

(i) Retained Restrictions on Alternative Actions, Intervals, and Critical Design Configuration Control Limitations (CDCCLs), With a New Exception

This paragraph restates the requirements of paragraph (l) of AD 2021–09–12, with a new exception. Except as required by paragraph (j) of this AD, after the maintenance or inspection program has been revised as required by paragraph (g) of this AD, no alternative actions (e.g., inspections), intervals, or CDCCLs are allowed unless they are approved as specified in the provisions of the “Ref. Publications” section of EASA AD 2020–0214.

(j) New Revision of the Existing Maintenance or Inspection Program

Except as specified in paragraph (k) of this AD: Comply with all required actions and compliance times specified in, and in accordance with, EASA AD 2022–0142, dated July 7, 2022 (EASA AD 2022–0142). Accomplishing the revision of the existing maintenance or inspection program required by this paragraph terminates the requirements of paragraph (g) of this AD.

(k) Exceptions to EASA AD 2022–0142

(1) The requirements specified in paragraphs (1) and (2) of EASA AD 2022–0142 do not apply to this AD.

(2) Paragraph (3) of EASA AD 2022–0142 specifies revising “the approved AMP” within 12 months after its effective date, but this AD requires revising the existing maintenance or inspection program, as applicable, within 90 days after the effective date of this AD.

(3) The initial compliance time for doing the tasks specified in paragraph (3) of EASA AD 2022–0142 is at the applicable “limitations” and “associated thresholds” as incorporated by the requirements of paragraph (3) of EASA AD 2022–0142, or within 90 days after the effective date of this AD, whichever occurs later.

(4) The provisions specified in paragraphs (4) and (5) of EASA AD 2022–0142 do not apply to this AD.

(5) The “Remarks” section of EASA AD 2022–0142 does not apply to this AD.

(l) New Provisions for Alternative Actions, Intervals, and CDCCLs

After the existing maintenance or inspection program has been revised as required by paragraph (j) of this AD, no alternative actions (e.g., inspections), intervals, and CDCCLs are allowed unless they are approved as specified in the provisions of the “Ref. Publications” section of EASA AD 2022–0142.

(m) Terminating Action for Certain Requirements in AD 2014–16–23

Accomplishing the actions required by paragraphs (g) or (j) of this AD terminates the requirements of paragraph (q) of AD 2014–16–23.

(n) Additional AD Provisions

The following provisions also apply to this AD:

(1) *Alternative Methods of Compliance (AMOCs):* The Manager, International Validation Branch, FAA, has the authority to approve AMOCs for this AD, if requested using the procedures found in 14 CFR 39.19. In accordance with 14 CFR 39.19, send your request to your principal inspector or responsible Flight Standards Office, as appropriate. If sending information directly to the International Validation Branch, send it to the attention of the person identified in paragraph (o) of this AD. Information may be emailed to: 9-AVS-AIR-730-AMOC@faa.gov. Before using any approved AMOC, notify your appropriate principal inspector, or lacking a principal inspector, the manager of the responsible Flight Standards Office.

(2) *Contacting the Manufacturer:* For any requirement in this AD to obtain instructions from a manufacturer, the instructions must be accomplished using a method approved by the Manager, International Validation Branch, FAA; or EASA; or Dassault Aviation’s EASA Design Organization Approval (DOA). If approved by the DOA, the approval must include the DOA-authorized signature.

(o) Additional Information

For more information about this AD, contact Tom Rodriguez, Aerospace Engineer, Large Aircraft Section, International Validation Branch, FAA, 2200 South 216th St., Des Moines, WA 98198; telephone and fax 206–231–3226; email tom.rodriguez@faa.gov.

(p) Material Incorporated by Reference

(1) The Director of the Federal Register approved the incorporation by reference (IBR) of the service information listed in this paragraph under 5 U.S.C. 552(a) and 1 CFR part 51.

(2) You must use this service information as applicable to do the actions required by this AD, unless this AD specifies otherwise.

(3) The following service information was approved for IBR on May 10, 2023.

(i) European Union Aviation Safety Agency (EASA) AD 2022–0142, dated July 7, 2022.

(ii) [Reserved]

(4) The following service information was approved for IBR on June 8, 2021.

(i) European Union Aviation Safety Agency (EASA) AD 2020–0214, dated October 6, 2020.

(ii) [Reserved]

(5) For EASA ADs 2022–0142 and 2020–0214, contact EASA, Konrad-Adenauer-Ufer 3, 50668 Cologne, Germany; telephone +49 221 8999 000; email ADs@easa.europa.eu; website easa.europa.eu. You may find these EASA ADs on the EASA website at ad.easa.europa.eu.

(6) You may view this material at the FAA, Airworthiness Products Section, Operational Safety Branch, 2200 South 216th St., Des Moines, WA. For information on the availability of this material at the FAA, call 206–231–3195.

(7) You may view this material that is incorporated by reference at the National Archives and Records Administration (NARA). For information on the availability of this material at NARA, email fr.inspection@nara.gov, or go to:

www.archives.gov/federal-register/cfr/ibr-locations.html.

Issued on February 17, 2023.

Christina Underwood,

Acting Director, Compliance & Airworthiness Division, Aircraft Certification Service.

[FR Doc. 2023-07027 Filed 4-4-23; 8:45 am]

BILLING CODE 4910-13-P

DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

14 CFR Part 39

[Docket No. FAA-2023-0433; Project Identifier AD-2022-00619-T; Amendment 39-22381; AD 2023-05-12]

RIN 2120-AA64

Airworthiness Directives; The Boeing Company Airplanes

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Final rule; request for comments.

SUMMARY: The FAA is adopting a new airworthiness directive (AD) for all The Boeing Company Model 767-2C series airplanes. This AD was prompted by arcing on an electrical terminal lug in a certain electrical power panel that caused heat and smoke damage, as a result of a loose power feeder terminal lug connection. This AD requires inspection of each terminal lug on certain electrical power panels for evidence of arcing and/or loose connection and applicable on-condition actions. The FAA is issuing this AD to address the unsafe condition on these products.

DATES: This AD is effective April 20, 2023.

The FAA must receive comments on this AD by May 22, 2023.

ADDRESSES: You may send comments, using the procedures found in 14 CFR 11.43 and 11.45, by any of the following methods:

- *Federal eRulemaking Portal:* Go to regulations.gov. Follow the instructions for submitting comments.

- *Fax:* 202-493-2251.

- *Mail:* U.S. Department of Transportation, Docket Operations, M-30, West Building Ground Floor, Room W12-140, 1200 New Jersey Avenue SE, Washington, DC 20590.

- *Hand Delivery:* Deliver to Mail address above between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays.

AD Docket: You may examine the AD docket at regulations.gov by searching for and locating Docket No. FAA-2023-

0433; or in person at Docket Operations between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. The AD docket contains this final rule, any comments received, and other information. The street address for Docket Operations is listed above.

FOR FURTHER INFORMATION CONTACT:

Hien T. Nguyen, Aerospace Engineer, Systems and Equipment Section, FAA, Seattle ACO Branch, 2200 South 216th St., Des Moines, WA 98198; phone: 405-954-5298; email: Hien.T.Nguyen@faa.gov.

SUPPLEMENTARY INFORMATION:

Background

The FAA received a report of an arcing event on an electrical terminal lug in the P34 panel that caused heat and smoke damage within the panel. It was determined that the arcing was a result of a loose power feeder terminal lug connection. An investigation into the root cause determined that the terminal lug was not torqued to the required specifications resulting in a loose connection. The under-torqued terminal lug was determined to be a workmanship issue. Additional inspections to other electrical power panels resulted in multiple findings of under-torqued terminal lugs. Under-torqued terminal lugs, if not addressed, could result in arcing that may lead to loss of critical function and loss of continued safe flight and landing. The FAA is issuing this AD to address the unsafe condition on these products.

FAA's Determination

The FAA is issuing this AD because the agency has determined the unsafe condition described previously is likely to exist or develop in other products of the same type design.

AD Requirements

This AD requires a general visual inspection of electrical terminal lugs, wires, and attached components in certain electrical power panels for electrical arcing damage, and repair or replacement of any damaged part; and a detailed inspection of each terminal lug for loose lugs in certain power panels, and retorquing each loose terminal lug.

Justification for Immediate Adoption and Determination of the Effective Date

Section 553(b)(3)(B) of the Administrative Procedure Act (APA) (5 U.S.C. 551 *et seq.*) authorizes agencies to dispense with notice and comment procedures for rules when the agency, for "good cause," finds that those procedures are "impracticable, unnecessary, or contrary to the public

interest." Under this section, an agency, upon finding good cause, may issue a final rule without providing notice and seeking comment prior to issuance. Further, section 553(d) of the APA authorizes agencies to make rules effective in less than thirty days, upon a finding of good cause.

There are currently no affected airplanes on the U.S. Register. Accordingly, notice and opportunity for prior public comment are unnecessary, pursuant to 5 U.S.C. 553(b)(3). In addition, for the foregoing reason(s), the FAA finds that good cause exists pursuant to 5 U.S.C. 553(d) for making this amendment effective in less than 30 days.

Comments Invited

The FAA invites you to send any written data, views, or arguments about this final rule. Send your comments to an address listed under **ADDRESSES**. Include Docket No. FAA-2023-0433 and Project Identifier AD-2022-00619-T at the beginning of your comments. The most helpful comments reference a specific portion of the final rule, explain the reason for any recommended change, and include supporting data. The FAA will consider all comments received by the closing date and may amend this final rule because of those comments.

Except for Confidential Business Information (CBI) as described in the following paragraph, and other information as described in 14 CFR 11.35, the FAA will post all comments received, without change, to regulations.gov, including any personal information you provide. The agency will also post a report summarizing each substantive verbal contact received about this final rule.

Confidential Business Information

CBI is commercial or financial information that is both customarily and actually treated as private by its owner. Under the Freedom of Information Act (FOIA) (5 U.S.C. 552), CBI is exempt from public disclosure. If your comments responsive to this AD contain commercial or financial information that is customarily treated as private, that you actually treat as private, and that is relevant or responsive to this AD, it is important that you clearly designate the submitted comments as CBI. Please mark each page of your submission containing CBI as "PROPIN." The FAA will treat such marked submissions as confidential under the FOIA, and they will not be placed in the public docket of this AD. Submissions containing CBI should be sent to Hien T. Nguyen, Aerospace Engineer, Systems and

Equipment Section, FAA, Seattle ACO Branch, 2200 South 216th St., Des Moines, WA 98198; phone: 405-954-5298; email: *Hien.T.Nguyen@faa.gov*. Any commentary that the FAA receives that is not specifically designated as CBI will be placed in the public docket for this rulemaking.

Regulatory Flexibility Act

The requirements of the Regulatory Flexibility Act (RFA) do not apply when an agency finds good cause pursuant to 5 U.S.C. 553 to adopt a rule without prior notice and comment. Because the FAA has determined that it has good cause to adopt this rule without notice

and comment, RFA analysis is not required.

Costs of Compliance

Currently, there are no affected U.S.-registered airplanes. For any affected airplane that is imported and placed on the U.S. Register in the future, the FAA provides the following cost estimates to comply with this AD:

ESTIMATED COSTS

Action	Labor cost	Parts cost	Cost per product
Inspections	43 work-hours × \$85 per hour = \$3,655 per inspection cycle ..	\$0	\$3,655 per inspection cycle.

The FAA estimates the following costs to do any necessary on-condition actions that would be required based on

the results of the inspections. The FAA has no way of determining the number

of aircraft that might need these on-condition actions:

ON-CONDITION COSTS

Action	Labor cost	Parts cost	Cost per product
Remove and Replace	1 work-hour × \$85 per hour = \$85	\$0	\$85
Apply Torque	1 work-hour × \$85 per hour = \$85	0	85

The FAA has received no definitive data on which to base the cost estimates for the replacement parts or repairs specified in this AD.

Authority for This Rulemaking

Title 49 of the United States Code specifies the FAA’s authority to issue rules on aviation safety. Subtitle I, section 106, describes the authority of the FAA Administrator. Subtitle VII: Aviation Programs describes in more detail the scope of the Agency’s authority.

The FAA is issuing this rulemaking under the authority described in Subtitle VII, Part A, Subpart III, Section 44701: General requirements. Under that section, Congress charges the FAA with promoting safe flight of civil aircraft in air commerce by prescribing regulations for practices, methods, and procedures the Administrator finds necessary for safety in air commerce. This regulation is within the scope of that authority because it addresses an unsafe condition that is likely to exist or develop on products identified in this rulemaking action.

Regulatory Findings

This AD will not have federalism implications under Executive Order 13132. This AD will not have a substantial direct effect on the States, on the relationship between the national government and the States, or on the distribution of power and

responsibilities among the various levels of government.

For the reasons discussed above, I certify that this AD:

- (1) Is not a “significant regulatory action” under Executive Order 12866, and
- (2) Will not affect intrastate aviation in Alaska.

List of Subjects in 14 CFR Part 39

Air transportation, Aircraft, Aviation safety, Incorporation by reference, Safety.

The Amendment

Accordingly, under the authority delegated to me by the Administrator, the FAA amends 14 CFR part 39 as follows:

PART 39—AIRWORTHINESS DIRECTIVES

- 1. The authority citation for part 39 continues to read as follows:

Authority: 49 U.S.C. 106(g), 40113, 44701.

§ 39.13 [Amended]

- 2. The FAA amends § 39.13 by adding the following new airworthiness directive:

2023-05-12 The Boeing Company:
Amendment 39-22381; Docket No. FAA-2023-0433; Project Identifier AD-2022-00619-T.

(a) Effective Date

This airworthiness directive (AD) is effective April 20, 2023.

(b) Affected ADs

None.

(c) Applicability

This AD applies to all The Boeing Company Model 767-2C series airplanes, certificated in any category.

(d) Subject

Air Transport Association (ATA) of America Code 24, Electrical Power.

(e) Unsafe Condition

This AD was prompted by a report of an arcing event on an electrical terminal lug that caused heat and smoke damage within the power panel. The FAA is issuing this AD to address under-torqued power feeder terminal lugs and possible loose connections. The unsafe condition, if not addressed, could lead to loss of critical function and loss of continued safe flight and landing.

(f) Compliance

Comply with this AD within the compliance times specified, unless already done.

(g) Required Actions

Within 10 months after the effective date of this AD, do the actions specified in paragraphs (g)(1) and (2) of this AD, in accordance with a method approved by the Manager, Seattle ACO Branch, FAA.

- (1) Do a general visual inspection (GVI) for electrical arcing damage of electrical terminal lugs, wires, and attached components in certain power panels, and before further flight, repair any damage found.

(2) Do a detailed inspection of each terminal lug for loose lugs in power panels, and, before further flight, apply torque to each loose terminal lug.

(h) Alternative Methods of Compliance (AMOCs)

(1) The Manager, Seattle ACO Branch, FAA, has the authority to approve AMOCs for this AD, if requested using the procedures found in 14 CFR 39.19. In accordance with 14 CFR 39.19, send your request to your principal inspector or responsible Flight Standards Office, as appropriate. If sending information directly to the manager of the certification office, send it to the attention of the person identified in paragraph (i) of this AD. Information may be emailed to: 9-ANM-Seattle-ACO-AMOC-Requests@faa.gov.

(2) Before using any approved AMOC, notify your appropriate principal inspector, or lacking a principal inspector, the manager of the responsible Flight Standards Office.

(3) An AMOC that provides an acceptable level of safety may be used for any repair, modification, or alteration required by this AD if it is approved by The Boeing Company Organization Designation Authorization (ODA) that has been authorized by the Manager, Seattle ACO Branch, FAA, to make those findings. To be approved, the repair method, modification deviation, or alteration deviation must meet the certification basis of the airplane, and the approval must specifically refer to this AD.

(i) Related Information

For more information about this AD, contact Hien T. Nguyen, Aerospace Engineer, Systems and Equipment Section, FAA, Seattle ACO Branch, 2200 South 216th St., Des Moines, WA 98198; phone: 405-954-5298; email: Hien.T.Nguyen@faa.gov.

(j) Material Incorporated by Reference

None.

Issued on March 9, 2023.

Christina Underwood,

Acting Director, Compliance & Airworthiness Division, Aircraft Certification Service.

[FR Doc. 2023-07037 Filed 4-4-23; 8:45 am]

BILLING CODE 4910-13-P

DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

14 CFR Part 39

[Docket No. FAA-2022-1240; Project Identifier AD-2022-00683-E; Amendment 39-22386; AD 2023-05-17]

RIN 2120-AA64

Airworthiness Directives; General Electric Company Turbofan Engines

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Final rule.

SUMMARY: The FAA is adopting a new airworthiness directive (AD) for certain

General Electric Company (GE) GE90-76B, GE90-85B, GE90-90B, and GE90-94B model turbofan engines. This AD was prompted by a commanded in-flight shutdown (IFSD) due to cracking and rockback of the high-pressure turbine (HPT) stage 2 nozzles resulting in blade liberation, severe rotor imbalance, and liberation of the exhaust centerbody. This AD requires initial and repetitive borescope inspections (BSIs) of the forward platforms of the HPT stage 2 blades or the leading edges of the HPT stage 2 nozzles and, depending on the results of the inspections, removal and replacement of the HPT stage 2 nozzles with parts eligible for installation. As a mandatory terminating action to the repetitive BSIs of the forward platforms of the HPT stage 2 blades or the leading edges of the HPT stage 2 nozzles, this AD requires replacing the HPT stage 2 nozzles. The FAA is issuing this AD to address the unsafe condition on these products.

DATES: This AD is effective May 10, 2023.

The Director of the Federal Register approved the incorporation by reference of a certain publication listed in this AD as of May 10, 2023.

ADDRESSES:

AD Docket: You may examine the AD docket at [regulations.gov](https://www.regulations.gov) by searching for and locating Docket No. FAA-2022-1240; or in person at Docket Operations between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. The AD docket contains this final rule, any comments received, and other information. The address for Docket Operations is U.S. Department of Transportation, Docket Operations, M-30, West Building Ground Floor, Room W12-140, 1200 New Jersey Avenue SE, Washington, DC 20590.

Material Incorporated by Reference:

- For service information identified in this final rule, contact General Electric Company, GE Aerospace, Room 285, 1 Neumann Way, Cincinnati, OH 45215; phone: (513) 552-3272; email: aviation.fleetsupport@ge.com.

- You may view this service information at the FAA, Airworthiness Products Section, Operational Safety Branch, 1200 District Avenue, Burlington, MA 01803. For information on the availability of this material at the FAA, call (817) 222-5110. It is also available at [regulations.gov](https://www.regulations.gov) by searching for and locating Docket No. FAA-2022-1240.

FOR FURTHER INFORMATION CONTACT:

Stephen Elwin, Aviation Safety Engineer, ECO Branch, FAA, 1200 District Avenue, Burlington, MA 01803;

phone: (781) 238-7236; email: Stephen.L.Elwin@faa.gov.

SUPPLEMENTARY INFORMATION:

Background

The FAA issued a notice of proposed rulemaking (NPRM) to amend 14 CFR part 39 by adding an AD that would apply to certain GE GE90-76B, GE90-85B, GE90-90B, and GE90-94B model turbofan engines. The NPRM published in the **Federal Register** on November 14, 2022 (87 FR 68113). The NPRM was prompted by a report of a commanded IFSD of a GE90-85B model turbofan engine installed on a Boeing Model 777-200ER airplane that occurred on July 12, 2018. Subsequent investigation by the manufacturer found that cracking and rockback of the HPT stage 2 nozzles, due to thermal distress in the fillet radius of the leading edge, resulted in rotor-stator contact with the HPT stage 2 blade platform. This condition caused liberation of an HPT stage 2 blade and severe rotor imbalance, leading to liberation of the exhaust centerbody from the engine. In the NPRM, the FAA proposed to require initial and repetitive borescope inspections of the forward platforms of the HPT stage 2 blades or the leading edges of the HPT stage 2 nozzles and, depending on the results of the inspections, removal and replacement of the HPT stage 2 nozzles with parts eligible for installation. As a mandatory terminating action to the repetitive BSIs of the forward platforms of the HPT stage 2 blades or the leading edges of the HPT stage 2 nozzles, the FAA proposed to require replacement of the HPT stage 2 nozzles. The FAA is issuing this AD to address the unsafe condition on these products.

Discussion of Final Airworthiness Directive

Comments

The FAA received comments from 3 commenters. The commenters were Air France, The Boeing Company (Boeing), and United Airlines. Boeing supported the proposed AD without change. Air France requested changes to the proposed AD, and United Airlines requested confirmation on a calculation process. The following presents the comments received on the NPRM and the FAA's response to each comment.

Request To Revise Compliance Time

Air France noted that affected engines with HPT stage 2 nozzles must be inspected whether or not they have reached the 22,000 hour threshold. The commenter requested that paragraphs (g)(1)(i) and (ii) be revised to both

require compliance before accumulating 250 flight cycles (FC) for all affected engines.

The FAA disagrees with the request. Paragraph (g)(1)(ii) of this AD requires the operator to perform a borescope inspection before accumulating 22,000 flight hours (FH) since new or since last overhaul, or within 250 FCs after the effective date of this AD, whichever occurs later. This requirement provides the operator with an appropriate drawdown threshold for parts that are approaching 22,000 FHs since new or since last overhaul. The FAA did not change this AD as a result of this comment.

Request To Make Terminating Action Optional

Air France requested that the Mandatory Terminating Action in paragraph (h) of this AD be revised to allow for the option to choose to replace the HPT Stage 2 nozzles when the engine is not in a performance restoration workscope shop visit or instead continue with the inspections required by this AD.

The FAA disagrees with the request. The compliance time required by the mandatory terminating action is necessary to address the unsafe condition. The FAA did not change this AD as a result of this comment.

Request To Add GE Service Bulletin as a Difference Between This AD and the Service Information

Air France noted that GE GE90 SB 72–1216, Initial Issue, dated August 22, 2022 (GE90 SB 72–1216) could have been referenced in the “Differences Between this Proposed AD and the Service Information” paragraph of the NPRM because that service bulletin recommends to inspect affected engines when the HPT stage 2 nozzles have reached 22,000 hours since new or overhaul.

The FAA disagrees with the request. For affected engines with less than 22,000 FHs since new or overhaul, GE90 SB 72–1216 recommends performing

the initial inspection before the engine accumulates 22,000 FHs, whereas this AD requires performing the initial inspection before the engine accumulates 22,000 FHs or 250 FCs, whichever occurs later, to minimize unnecessary grounding of airplanes. This compliance time is not considered a major difference, and therefore, is not included within the “Differences Between this AD and the Service Information” section of the NPRM. The FAA did not change this AD as a result of this comment.

Request To Clarify Accepted FH Calculation

United Airlines requested confirmation that calculation of FHs on HPT stage 2 nozzles based on shop records is acceptable for compliance with this AD. United Airlines noted that HPT stage 2 nozzles are not currently a tracked part and, therefore, the determination of accumulated FHs since new or since last overhaul would be based on shop records entered when the HPT stage 2 nozzles were either replaced or overhauled.

The FAA agrees to clarify. The method of calculation presented by United Airlines, including the use of shop records when determining FHs on HPT stage 2 nozzles since new or since last overhaul, is acceptable for compliance with this AD. The FAA did not change this AD as a result of this comment.

Revision of Estimated Costs

In this Final Rule, the FAA has moved the estimated costs associated with paragraphs (g)(3) and (h) from the on-condition costs section to the estimated costs section, since the replacement is required on-condition for a failed inspection and also as a mandatory terminating action. This revision does not increase the economic burden on operators.

Conclusion

The FAA reviewed the relevant data and determined that air safety requires

adopting this AD as proposed. Accordingly, the FAA is issuing this AD to address the unsafe condition on these products. Except for minor editorial changes, this AD is adopted as proposed in the NPRM.

Related Service Information Under 1 CFR Part 51

The FAA reviewed GE GE90 Service Bulletin (SB) 72–1166, Revision 3, dated February 14, 2019. This service information specifies procedures for BSIs of the HPT stage 2 blade forward platforms for rub marks or evidence of contact (circumferential grooves on the HPT stage 2 blade platforms) with the HPT stage 2 nozzle angel wings. This service information also specifies procedures for performing a 360-degree BSI of the HPT stage 2 nozzles leading edges and specifies procedures for removal and replacement of HPT stage 2 nozzles. This service information is reasonably available because the interested parties have access to it through their normal course of business or by the means identified in the ADDRESSES section.

Other Related Service Information

The FAA reviewed GE GE90 SB 72–1071, Revision 1, dated January 16, 2015. This service information specifies procedures for removal and replacement of HPT stage 2 nozzles with HPT stage 2 nozzles that incorporate a design change.

The FAA also reviewed GE GE90 SB 72–1216, Initial Issue, dated August 22, 2022. This service information specifies inspection procedures for affected HPT stage 2 nozzles.

Costs of Compliance

The FAA estimates that this AD affects 8 engines installed on airplanes of U.S. registry.

The FAA estimates the following costs to comply with this AD:

ESTIMATED COSTS

Action	Labor cost	Parts cost	Cost per product	Cost on U.S. operators
BSI of HPT stage 2 nozzles or HPT stage 2 blade interface.	4 work-hours × \$85 per hour = \$340	\$0	\$340	\$2,720
Replace full set of HPT stage 2 nozzles	8 work-hours × \$85 per hour = \$680	918,650	919,330	7,354,640

Authority for This Rulemaking

Title 49 of the United States Code specifies the FAA’s authority to issue rules on aviation safety. Subtitle I,

section 106, describes the authority of the FAA Administrator. Subtitle VII: Aviation Programs, describes in more

detail the scope of the Agency’s authority.

The FAA is issuing this rulemaking under the authority described in Subtitle VII, Part A, Subpart III, Section

44701: General requirements. Under that section, Congress charges the FAA with promoting safe flight of civil aircraft in air commerce by prescribing regulations for practices, methods, and procedures the Administrator finds necessary for safety in air commerce. This regulation is within the scope of that authority because it addresses an unsafe condition that is likely to exist or develop on products identified in this rulemaking action.

Regulatory Findings

This AD will not have federalism implications under Executive Order 13132. This AD will not have a substantial direct effect on the States, on the relationship between the national government and the States, or on the distribution of power and responsibilities among the various levels of government.

For the reasons discussed above, I certify that this AD:

(1) Is not a “significant regulatory action” under Executive Order 12866,

(2) Will not affect intrastate aviation in Alaska, and

(3) Will not have a significant economic impact, positive or negative, on a substantial number of small entities under the criteria of the Regulatory Flexibility Act.

List of Subjects in 14 CFR Part 39

Air transportation, Aircraft, Aviation safety, Incorporation by reference, Safety.

The Amendment

Accordingly, under the authority delegated to me by the Administrator, the FAA amends 14 CFR part 39 as follows:

PART 39—AIRWORTHINESS DIRECTIVES

■ 1. The authority citation for part 39 continues to read as follows:

Authority: 49 U.S.C. 106(g), 40113, 44701.

§ 39.13 [Amended]

■ 2. The FAA amends § 39.13 by adding the following new airworthiness directive:

2023–05–17 General Electric Company:
Amendment 39–22386; Docket No. FAA–2022–1240; Project Identifier AD–2022–00683–E.

(a) Effective Date

This airworthiness directive (AD) is effective May 10, 2023.

(b) Affected ADs

None.

(c) Applicability

This AD applies to General Electric Company (GE) GE90–76B, GE90–85B, GE90–90B, and GE90–94B model turbofan engines, excluding those engines with an installed full set of high-pressure turbine (HPT) stage 2 nozzles with part numbers 1847M47G23 and 1847M47G24.

(d) Subject

Joint Aircraft System Component (JASC) Code 7250, Turbine Section.

(e) Unsafe Condition

This AD was prompted by a commanded in-flight shutdown (IFSD) due to cracking and rockback of the HPT stage 2 nozzles resulting in blade liberation, severe rotor imbalance, and liberation of the exhaust centerbody. The FAA is issuing this AD to prevent failure of the HPT stage 2 nozzles, HPT stage 2 blades, and exhaust centerbody. The unsafe condition, if not addressed, could result in IFSD, failure of the engine and exhaust centerbody, and loss of the airplane.

(f) Compliance

Comply with this AD within the compliance times specified, unless already done.

(g) Required Actions

(1) Within the compliance times specified in paragraphs (g)(1)(i) and (ii) of this AD, perform an initial borescope inspection (BSI) of the forward platforms of the HPT stage 2 blades, or perform a 360 degree BSI of the leading edges of the HPT stage 2 nozzles (optional procedure) in accordance with the Accomplishment Instructions, paragraph 3.A.(3)(a) of GE GE90 SB 72–1166, Revision 3, dated February 14, 2019 (the SB):

(i) For engines with HPT stage 2 nozzles that have accumulated 22,000 or more flight hours since new or since last overhaul as of the effective date of this AD, perform the initial BSI before accumulating 250 flight cycles (FCs) after the effective date of this AD.

(ii) For engines with HPT stage 2 nozzles that have accumulated less than 22,000 flight hours since new or since last overhaul as of the effective date of this AD, perform the initial BSI before accumulating 22,000 flight hours since new or since last overhaul, or within 250 FCs after the effective date of this AD, whichever occurs later.

(2) Thereafter, at intervals not to exceed 100 FCs from performance of the last BSI of the forward platforms of the HPT stage 2 blades, or at intervals not to exceed 500 FCs from the last BSI of the leading edges of the HPT stage 2 nozzles, as applicable, perform a repetitive BSI of the forward platforms of the HPT stage 2 blades or the leading edges of the HPT stage 2 nozzles in accordance with the Accomplishment Instructions, paragraph 3.A.(3)(a) of the SB.

(3) If, during any inspection required by paragraphs (g)(1) or (g)(2) of this AD, rub marks, evidence of contact on the HPT stage 2 blade forward platform on three or more HPT stage 2 blades, or an unserviceable HPT stage 2 nozzle is found, before further flight, remove and replace the HPT stage 2 nozzles with parts eligible for installation.

Note 1 to paragraph (g)(3): Serviceability criteria can be found in the GE90 Boeing 777 Aircraft Maintenance Manual, 72–00–00, INSPECTION/CHECK, Subtask 72–00–00–220–074–G00.

(h) Mandatory Terminating Action

As a mandatory terminating action to the repetitive inspections required by paragraph (g)(2) of this AD, at the next engine shop visit after reaching 22,000 flight hours since new or since last overhaul, replace the HPT stage 2 nozzles with parts eligible for installation.

(i) Definitions

(1) For the purpose of this AD, “parts eligible for installation” is a full set of HPT stage 2 nozzles with part numbers 1847M47G23 and 1847M47G24.

(2) For the purpose of this AD, an “overhaul” is the complete refurbishment of the HPT stage 2 nozzle segments.

(3) For the purpose of this AD, an “engine shop visit” is the induction of an engine into the shop for maintenance involving separation of pairs of major mating engine case flanges, except for the following situations, which do not constitute an engine shop visit:

(i) Separation of engine flanges solely for the purposes of transportation of the engine without subsequent maintenance; or

(ii) Separation of engine flanges solely for the purpose of replacing the fan or propulsor without subsequent maintenance.

(j) Credit for Previous Actions

You may take credit for the initial inspection required by paragraph (g)(1) of this AD if you performed the inspection before the effective date of this AD using GE GE90 SB 72–1166, Revision 2, dated October 13, 2017, or earlier revisions.

(k) Alternative Methods of Compliance (AMOCs)

(1) The Manager, ECO Branch, FAA, has the authority to approve AMOCs for this AD, if requested using the procedures found in 14 CFR 39.19. In accordance with 14 CFR 39.19, send your request to your principal inspector or local Flight Standards District Office, as appropriate. If sending information directly to the manager of the certification office, send it to the attention of the person identified in paragraph (l) of this AD. Information may be emailed to: ANE-AD-AMOC@faa.gov.

(2) Before using any approved AMOC, notify your appropriate principal inspector, or lacking a principal inspector, the manager of the local flight standards district office/certificate holding district office.

(l) Related Information

For more information about this AD, contact Stephen Elwin, Aviation Safety Engineer, ECO Branch, FAA, 1200 District Avenue, Burlington, MA 01803; phone: (781) 238–7236; email: Stephen.L.Elwin@faa.gov.

(m) Material Incorporated by Reference

(1) The Director of the Federal Register approved the incorporation by reference (IBR) of the service information listed in this paragraph under 5 U.S.C. 552(a) and 1 CFR part 51.

(2) You must use this service information as applicable to do the actions required by this AD, unless the AD specifies otherwise.

(i) GE GE90 Service Bulletin (SB) 72-1166, Revision 3, dated February 14, 2019.

(ii) [Reserved]

(3) For GE service information identified in this AD, contact General Electric Company, GE Aerospace, Room 285, 1 Neumann Way, Cincinnati, OH 45215; phone: (513) 552-3272; email: aviation.fleetsupport@ge.com.

(4) You may view this service information at FAA, Airworthiness Products Section, Operational Safety Branch, 1200 District Avenue, Burlington, MA 01803. For information on the availability of this material at the FAA, call (817) 222-5110.

(5) You may view this service information that is incorporated by reference at the National Archives and Records Administration (NARA). For information on the availability of this material at NARA, email: fr.inspection@nara.gov, or go to: www.archives.gov/federal-register/cfr/ibr-locations.html.

Issued on March 9, 2023.

Christina Underwood,

Acting Director, Compliance & Airworthiness Division, Aircraft Certification Service.

[FR Doc. 2023-07005 Filed 4-4-23; 8:45 am]

BILLING CODE 4910-13-P

DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

14 CFR Part 39

[Docket No. FAA-2022-1063; Project Identifier AD-2021-01339-T; Amendment 39-22375; AD 2023-05-06]

RIN 2120-AA64

Airworthiness Directives; The Boeing Company Airplanes

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Final rule.

SUMMARY: The FAA is adopting a new airworthiness directive (AD) for certain The Boeing Company Model 737-8, 737-9, and 737-8200 airplanes. This AD was prompted by a determination that new airworthiness limitations are necessary to require periodic replacement; or testing, and replacement if necessary; of the oxygen sensor of the nitrogen generation system (NGS). This AD requires revising the existing maintenance or inspection program, as applicable, to incorporate the new airworthiness limitations. The FAA is issuing this AD to address the unsafe condition on these products.

DATES: This AD is effective May 10, 2023.

The Director of the Federal Register approved the incorporation by reference

of certain publications listed in this AD as of May 10, 2023.

ADDRESSES:

AD Docket: You may examine the AD docket at regulations.gov under Docket No. FAA-2022-1063; or in person at Docket Operations between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. The AD docket contains this final rule, any comments received, and other information. The address for Docket Operations is U.S. Department of Transportation, Docket Operations, M-30, West Building Ground Floor, Room W12-140, 1200 New Jersey Avenue SE, Washington, DC 20590.

Material Incorporated by Reference:

- For service information identified in this final rule, contact Boeing Commercial Airplanes, Attention: Contractual & Data Services (C&DS), 2600 Westminister Blvd., MC 110-SK57, Seal Beach, CA 90740-5600; telephone 562-797-1717; website myboeingfleet.com.

- You may view this service information at the FAA, Airworthiness Products Section, Operational Safety Branch, 2200 South 216th St., Des Moines, WA. For information on the availability of this material at the FAA, call 206-231-3195. It is also available at regulations.gov under Docket No. FAA-2022-1063.

FOR FURTHER INFORMATION CONTACT: Sam Dorsey, Aerospace Engineer, Propulsion Section, FAA, Seattle ACO Branch, 2200 South 216th St., Des Moines, WA 98198; phone and fax: 206-231-3415; email: samuel.j.dorsey@faa.gov.

SUPPLEMENTARY INFORMATION:

Background

The FAA issued a notice of proposed rulemaking (NPRM) to amend 14 CFR part 39 by adding an AD that would apply to certain The Boeing Company Model 737-8, 737-9, and 737-8200 airplanes. The NPRM published in the **Federal Register** on November 28, 2022 (87 FR 72902). The NPRM was prompted by a determination that a new airworthiness limitation is necessary to require periodic replacement of the oxygen sensor of the NGS. In the NPRM, the FAA proposed to require revising the existing maintenance or inspection program, as applicable, to incorporate the new airworthiness limitation. The FAA is issuing this AD to prevent increasing the flammability exposure of the center fuel tank, which together with an ignition source in the fuel tank, could lead to a fuel tank explosion and consequent loss of the airplane.

Discussion of Final Airworthiness Directive

Comments

The FAA received comments from the Air Line Pilots Association, International (ALPA) and an individual who supported the NPRM without change.

The FAA received additional comments from four commenters, including Boeing, American Airlines, SIA Engineering Company, and United Airlines (United). The following presents the comments received on the NPRM and the FAA's response to each comment.

Request To Refer to Latest Service Information

Boeing and United requested that the proposed AD be revised to specify compliance with Boeing 737-7/8/8200/9/10 Special Compliance Items/Airworthiness Limitations, D626A011-9-04, dated May 2022, instead of Boeing 737-7/8/8200/9/10 Special Compliance Items/Airworthiness Limitations, D626A011-9-04, dated January 2019. Boeing noted that Boeing 737-7/8/8200/9/10 Special Compliance Items/Airworthiness Limitations, D626A011-9-04, dated May 2022 includes a revision to 47-AWL-09 and the addition of new airworthiness limitation 47-AWL-10 (which is a Critical Design Configuration Control Limitation (CDCCL) that specifies procedures for oxygen sensor repairs). Boeing added that the revision to 47-AWL-09 provides additional options for operators beyond replacing the oxygen sensor with a new oxygen sensor. Those options include testing the installed NGS oxygen sensor using a functional check described in the Airplane Maintenance Manual (AMM) (and replacing if necessary), and replacing the oxygen sensor with an NGS oxygen sensor repaired as specified in 47-AWL-10. United noted that these changes provide operators with benefits necessary for the efficient accomplishment of task 47-AWL-09.

The FAA partially agrees with the commenters' requests. Boeing 737-7/8/8200/9/10 Special Compliance Items/Airworthiness Limitations, D626A011-9-04, dated May 2022, provides options that are relieving, but also includes a new CDCCL requirement that was not included in the proposed AD. The FAA has therefore revised this AD to require incorporating the information specified in AWL No. 47-AWL-09, "Nitrogen Generation System—Oxygen Sensor," of Boeing 737-7/8/8200/9/10 Special Compliance Items/Airworthiness Limitations, D626A011-9-04, dated

January 2019; or the information specified in 47–AWL–09 and 47–AWL–10 of Boeing 737–7/8/8200/9/10 Special Compliance Items/Airworthiness Limitations, D626A011–9–04, dated May 2022.

Request To Refer to Latest Service Information

American Airlines requested that the FAA add a provision to accomplish the oxygen sensor replacement with a repaired or overhauled sensor instead of a brand new sensor. The commenter noted that this provision would ease the burden on operators by not requiring them to scrap used sensors and buy new ones. American Airlines added that the 737NG fleet has a similar AWL requirement, with a provision that a repaired sensor may be installed.

The FAA agrees with the commenter's request. As noted previously, this AD has been revised to allow incorporating the information in Boeing 737–7/8/8200/9/10 Special Compliance Items/Airworthiness Limitations, D626A011–9–04, dated May 2022, which includes provisions for replacing the oxygen sensor with a repaired oxygen sensor or testing the oxygen sensor, and replacing if necessary.

Request To Clarify Applicability

SIA Engineering Company asked that the FAA confirm the commenter's understanding of paragraph (c) of the proposed AD. SIA Engineering Company requested confirmation that the proposed AD does not affect The Boeing Company Model 737–8, 737–9, and 737–8200 airplanes having original airworthiness certificate or original export certificate of airworthiness issued on or before April 1, 2021, and with a line number not identified in paragraph (c)(2) of the proposed AD.

The FAA agrees to clarify. This AD applies to The Boeing Company Model 737–8, 737–9, and 737–8200 airplanes having original airworthiness certificate or original export certificate of airworthiness issued on or before April 1, 2021, and it also applies to The Boeing Company Model 737–8, 737–9, and 737–8200 airplanes with a line number specified in paragraph (c)(2) of this AD. This AD does not apply to any airplanes not specified in paragraph (c)(1) or (2) of this AD.

Request To Revise a Sentence in the Background

Boeing requested that the FAA revise a sentence in the Background section. In the NPRM the sentence reads “Degraded performance by the sensor could result in the [air separation module] ASM failing to produce nitrogen-enriched air,

and the fuel tank becoming more flammable due to excessive oxygen-enriched air.” Boeing stated that this sentence is inaccurate because it implies a causality between a failing oxygen sensor and a degrading ASM, when there is none. Boeing added that the sentence further implies that the oxygen enriched air (OEA) is redirected to the fuel tanks if the ASMs start going bad. Boeing stated that the sentence should state: “Degraded oxygen sensor performance could result in the system failing to detect when the ASM performance degrades below the acceptable threshold for nitrogen-enriched air, and the fuel tank becoming more flammable due to receiving poor-quality nitrogen-enriched air.”

The FAA agrees that there is no causality between the degraded performance of the oxygen sensor and failure of ASM. Degradation of the oxygen sensor performance does not directly result in the ASM failing to produce nitrogen-enriched air, but rather it would result in a failure to detect the condition of the ASM not performing at a required level. However, the sentence in question from the Background section of the NPRM will not be carried over to this final rule. Therefore, the FAA has not changed this AD regarding this issue.

Request To Include Cost for Replacement Sensor

United requested that the NPRM be revised to include the cost of a replacement NGS oxygen sensor and its availability.

The FAA disagrees with the commenter's request. This AD does not require compliance with the maintenance actions specified in the AWL items. Instead, this AD requires operators to revise their existing maintenance or inspection program, as applicable, to incorporate the new airworthiness limitations. Compliance with any airworthiness limitation is required by 14 CFR 91.403(c). Therefore, compliance with the AWLs is not a requirement of this AD, and including the cost of a replacement part would be inappropriate. The FAA has not changed this AD regarding this issue.

Conclusion

The FAA reviewed the relevant data, considered any comments received, and determined that air safety requires adopting this AD as proposed. Accordingly, the FAA is issuing this AD to address the unsafe condition on these products. Except for minor editorial changes, and any other changes described previously, this AD is adopted as proposed in the NPRM.

None of the changes will increase the economic burden on any operator.

Related Service Information Under 1 CFR Part 51

The FAA reviewed Boeing 737–7/8/8200/9/10 Special Compliance Items/Airworthiness Limitations, D626A011–9–04, dated January 2019. This service information describes, among other airworthiness limitations (AWLs), airworthiness limitation instruction (ALI) AWL No. 47–AWL–09, “Nitrogen Generation System—Oxygen Sensor,” for replacing oxygen sensors.

The FAA also reviewed Boeing 737–7/8/8200/9/10 Special Compliance Items/Airworthiness Limitations, D626A011–9–04, dated May 2022. This service information describes, among other AWLs, ALI AWL No. 47–AWL–09, “Nitrogen Generation System (NGS)—Oxygen Sensor,” for replacement; or testing, and replacement if necessary; of the oxygen sensor of the nitrogen generation system (NGS), and AWL No. 47–AWL–10, “Nitrogen Generation System (NGS)—Oxygen Sensor Repair,” for repairing oxygen sensors.

This service information is reasonably available because the interested parties have access to it through their normal course of business or by the means identified in **ADDRESSES**.

Costs of Compliance

The FAA estimates that this AD affects 62 airplanes of U.S. registry. The FAA estimates the following costs to comply with this AD:

The FAA has determined that revising the existing maintenance or inspection program takes an average of 90 work-hours per operator, although the agency recognizes that this number may vary from operator to operator. Since operators incorporate maintenance or inspection program changes for their affected fleet(s), the FAA has determined that a per-operator estimate is more accurate than a per-airplane estimate. Therefore, the FAA estimates the average total cost per operator to be \$7,650 (90 work-hours × \$85 per workhour).

Authority for This Rulemaking

Title 49 of the United States Code specifies the FAA's authority to issue rules on aviation safety. Subtitle I, section 106, describes the authority of the FAA Administrator. Subtitle VII: Aviation Programs, describes in more detail the scope of the Agency's authority.

The FAA is issuing this rulemaking under the authority described in Subtitle VII, Part A, Subpart III, Section 44701: General requirements. Under

that section, Congress charges the FAA with promoting safe flight of civil aircraft in air commerce by prescribing regulations for practices, methods, and procedures the Administrator finds necessary for safety in air commerce. This regulation is within the scope of that authority because it addresses an unsafe condition that is likely to exist or develop on products identified in this rulemaking action.

Regulatory Findings

This AD will not have federalism implications under Executive Order 13132. This AD will not have a substantial direct effect on the States, on the relationship between the national government and the States, or on the distribution of power and responsibilities among the various levels of government.

For the reasons discussed above, I certify that this AD:

(1) Is not a “significant regulatory action” under Executive Order 12866,
(2) Will not affect intrastate aviation in Alaska, and

(3) Will not have a significant economic impact, positive or negative, on a substantial number of small entities under the criteria of the Regulatory Flexibility Act.

List of Subjects in 14 CFR Part 39

Air transportation, Aircraft, Aviation safety, Incorporation by reference, Safety.

The Amendment

Accordingly, under the authority delegated to me by the Administrator, the FAA amends 14 CFR part 39 as follows:

PART 39—AIRWORTHINESS DIRECTIVES

■ 1. The authority citation for part 39 continues to read as follows:

Authority: 49 U.S.C. 106(g), 40113, 44701.

§ 39.13 [Amended]

■ 2. The FAA amends § 39.13 by adding the following new airworthiness directive:

2023–05–06 The Boeing Company:

Amendment 39–22375; Docket No. FAA–2022–1063; Project Identifier AD–2021–01339–T.

(a) Effective Date

This airworthiness directive (AD) is effective May 10, 2023.

(b) Affected ADs

None

(c) Applicability

This AD applies to The Boeing Company Model 737–8, 737–9, and 737–8200

airplanes, certificated in any category, identified in paragraphs (c)(1) and (2) of this AD.

(1) Airplanes with an original airworthiness certificate or original export certificate of airworthiness issued on or before April 1, 2021.

(2) Airplanes with line numbers 7668, 7678, and 7915.

(d) Subject

Air Transport Association (ATA) of America Code 28, Fuel.

(e) Unsafe Condition

This AD was prompted by significant changes made to airworthiness limitations (AWLs) related to the nitrogen generation system (NGS). The FAA is issuing this AD to prevent increasing the flammability exposure of the center fuel tank, which together with an ignition source in the fuel tank, could lead to a fuel tank explosion and consequent loss of the airplane.

(f) Compliance

Comply with this AD within the compliance times specified, unless already done.

(g) Maintenance or Inspection Program Revision

Within 60 days after the effective date of this AD, revise the existing maintenance or inspection program, as applicable, to incorporate the information specified in AWL No. 47–AWL–09, “Nitrogen Generation System—Oxygen Sensor,” of Boeing 737–7/8/8200/9/10 Special Compliance Items/Airworthiness Limitations, D626A011–9–04, dated January 2019; or the information specified in AWL No. 47–AWL–09, “Nitrogen Generation System (NGS)—Oxygen Sensor,” and AWL No. 47–AWL–10, “Nitrogen Generation System (NGS)—Oxygen Sensor Repair,” of Boeing 737–7/8/8200/9/10 Special Compliance Items/Airworthiness Limitations, D626A011–9–04, dated May 2022. The initial compliance time for accomplishing task AWL No. 47–AWL–09 is: Within 18,000 flight hours after the date of issuance of the original airworthiness certificate or the original export certificate of airworthiness, within 18,000 flight hours after the most recent replacement or test was performed as specified in AWL No. 47–AWL–09, or within 12 months after the effective date of this AD, whichever is latest.

(h) No Alternative Actions, Intervals, or Critical Design Configuration Control Limitations (CDCCLs)

After the existing maintenance or inspection program has been revised as required by paragraph (g) of this AD, no alternative actions (e.g., inspections), intervals, or CDCCLs may be used unless the actions, intervals, and CDCCLs are approved as an alternative method of compliance (AMOC) in accordance with the procedures specified in paragraph (i) of this AD.

(i) Alternative Methods of Compliance (AMOCs)

(1) The Manager, Seattle ACO Branch, FAA, has the authority to approve AMOCs for this AD, if requested using the procedures

found in 14 CFR 39.19. In accordance with 14 CFR 39.19, send your request to your principal inspector or responsible Flight Standards Office, as appropriate. If sending information directly to the manager of the certification office, send it to the attention of the person identified in paragraph (j) of this AD. Information may be emailed to: 9-ANM-Seattle-ACO-AMOC-Requests@faa.gov.

(2) Before using any approved AMOC, notify your appropriate principal inspector, or lacking a principal inspector, the manager of the responsible Flight Standards Office.

(3) An AMOC that provides an acceptable level of safety may be used for any repair, modification, or alteration required by this AD if it is approved by The Boeing Company Organization Designation Authorization (ODA) that has been authorized by the Manager, Seattle ACO Branch, FAA, to make those findings. To be approved, the repair method, modification deviation, or alteration deviation must meet the certification basis of the airplane, and the approval must specifically refer to this AD.

(j) Additional Information

For more information about this AD, contact Sam Dorsey, Aerospace Engineer, Propulsion Section, FAA, Seattle ACO Branch, 2200 South 216th St., Des Moines, WA 98198; phone and fax: 206–231–3415; email: samuel.j.dorsey@faa.gov.

(k) Material Incorporated by Reference

(1) The Director of the Federal Register approved the incorporation by reference (IBR) of the service information listed in this paragraph under 5 U.S.C. 552(a) and 1 CFR part 51.

(2) You must use this service information as applicable to do the actions required by this AD, unless the AD specifies otherwise.

(i) Boeing 737–7/8/8200/9/10 Special Compliance Items/Airworthiness Limitations, D626A011–9–04, dated January 2019.

(ii) Boeing 737–7/8/8200/9/10 Special Compliance Items/Airworthiness Limitations, D626A011–9–04, dated May 2022.

(3) For service information identified in this AD, contact Boeing Commercial Airplanes, Attention: Contractual & Data Services (C&DS), 2600 Westminister Blvd., MC 110–SK57, Seal Beach, CA 90740–5600; telephone 562–797–1717; website myboeingfleet.com.

(4) You may view this service information at the FAA, Airworthiness Products Section, Operational Safety Branch, 2200 South 216th St., Des Moines, WA. For information on the availability of this material at the FAA, call 206–231–3195.

(5) You may view this service information that is incorporated by reference at the National Archives and Records Administration (NARA). For information on the availability of this material at NARA, fr.inspection@nara.gov, or go to: www.archives.gov/federal-register/cfr/ibr-locations.html.

Issued on March 5, 2023.

Christina Underwood,

*Acting Director, Compliance & Airworthiness
Division, Aircraft Certification Service.*

[FR Doc. 2023-07034 Filed 4-4-23; 8:45 am]

BILLING CODE 4910-13-P

DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

14 CFR Part 97

[Docket No. 31476; Amdt. No. 4051]

Standard Instrument Approach Procedures, and Takeoff Minimums and Obstacle Departure Procedures; Miscellaneous Amendments

AGENCY: Federal Aviation
Administration (FAA), DOT.

ACTION: Final rule.

SUMMARY: This rule establishes, amends, suspends, or removes Standard Instrument Approach Procedures (SIAPs) and associated Takeoff Minimums and Obstacle Departure Procedures (ODPs) for operations at certain airports. These regulatory actions are needed because of the adoption of new or revised criteria, or because of changes occurring in the National Airspace System, such as the commissioning of new navigational facilities, adding new obstacles, or changing air traffic requirements. These changes are designed to provide safe and efficient use of the navigable airspace and to promote safe flight operations under instrument flight rules at the affected airports.

DATES: This rule is effective April 5, 2023. The compliance date for each SIAP, associated Takeoff Minimums, and ODP is specified in the amendatory provisions.

The incorporation by reference of certain publications listed in the regulations is approved by the Director of the Federal Register as of April 5, 2023.

ADDRESSES: Availability of matters incorporated by reference in the amendment is as follows:

For Examination

1. U.S. Department of Transportation, Docket Ops-M30. 1200 New Jersey Avenue SE, West Bldg., Ground Floor, Washington, DC 20590-0001.

2. The FAA Air Traffic Organization Service Area in which the affected airport is located;

3. The office of Aeronautical Information Services, 6500 South MacArthur Blvd., Oklahoma City, OK 73169 or,

4. The National Archives and Records Administration (NARA). For information on the availability of this material at NARA, email fr.inspection@nara.gov or go to: <https://www.archives.gov/federal-register/cfr/ibr-locations.html>.

Availability

All SIAPs and Takeoff Minimums and ODPs are available online free of charge. Visit the National Flight Data Center at nfdc.faa.gov to register. Additionally, individual SIAP and Takeoff Minimums and ODP copies may be obtained from the FAA Air Traffic Organization Service Area in which the affected airport is located.

FOR FURTHER INFORMATION CONTACT:

Thomas J. Nichols, Flight Procedures and Airspace Group, Flight Technologies and Procedures Division, Flight Standards Service, Federal Aviation Administration. Mailing Address: FAA Mike Monroney Aeronautical Center, Flight Procedures and Airspace Group, 6500 South MacArthur Blvd., STB Annex, Bldg. 26, Room 217, Oklahoma City, OK 73099. Telephone (405) 954-1139.

SUPPLEMENTARY INFORMATION: This rule amends 14 CFR part 97 by establishing, amending, suspending, or removes SIAPs, Takeoff Minimums and/or ODPs. The complete regulatory description of each SIAP and its associated Takeoff Minimums or ODP for an identified airport is listed on FAA form documents which are incorporated by reference in this amendment under 5 U.S.C. 552(a), 1 CFR part 51, and 14 CFR part 97.20. The applicable FAA Forms 8260-3, 8260-4, 8260-5, 8260-15A, 8260-15B, when required by an entry on 8260-15A, and 8260-15C.

The large number of SIAPs, Takeoff Minimums and ODPs, their complex nature, and the need for a special format make publication in the **Federal Register** expensive and impractical. Further, airmen do not use the regulatory text of the SIAPs, Takeoff Minimums or ODPs, but instead refer to their graphic depiction on charts printed by publishers or aeronautical materials. Thus, the advantages of incorporation by reference are realized and publication of the complete description of each SIAP, Takeoff Minimums and ODP listed on FAA form documents is unnecessary. This amendment provides the affected CFR sections and specifies the typed of SIAPs, Takeoff Minimums and ODPs with their applicable effective dates. This amendment also identifies the airport and its location, the procedure, and the amendment number.

Availability and Summary of Material Incorporated by Reference

The material incorporated by reference is publicly available as listed in the **ADDRESSES** section.

The material incorporated by reference describes SIAPs, Takeoff Minimums and/or ODPs as identified in the amendatory language for Part 97 of this final rule.

The Rule

This amendment to 14 CFR part 97 is effective upon publication of each separate SIAP, Takeoff Minimums and ODP as amended in the transmittal. Some SIAP and Takeoff Minimums and textual ODP amendments may have been issued previously by the FAA in a Flight Data Center (FDC) Notice to Airmen (NOTAM) as an emergency action of immediate flights safety relating directly to published aeronautical charts.

The circumstances that created the need for some SIAP and Takeoff Minimums and ODP amendments may require making them effective in less than 30 days. For the remaining SIAPs and Takeoff Minimums and ODPs, an effective date at least 30 days after publication is provided.

Further, the SIAPs and Takeoff Minimums and ODPs contained in this amendment are based on the criteria contained in the U.S. Standard for Terminal Instrument Procedures (TERPS). In developing these SIAPs and Takeoff Minimums and ODPs, the TERPS criteria were applied to the conditions existing or anticipated at the affected airports. Because of the close and immediate relationship between these SIAPs, Takeoff Minimums and ODPs, and safety in air commerce, I find that notice and public procedure under 5 U.S.C. 553(b) are impracticable and contrary to the public interest and, where applicable, under 5 U.S.C. 553(d), good cause exists for making some SIAPs effective in less than 30 days.

The FAA has determined that this regulation only involves an established body of technical regulations for which frequent and routine amendments are necessary to keep them operationally current. It, therefore—(1) is not a “significant regulatory action” under Executive Order 12866; (2) is not a “significant rule” under DOT Regulatory Policies and Procedures (44 FR 11034; February 26, 1979); and (3) does not warrant preparation of a regulatory evaluation as the anticipated impact is so minimal. For the same reason, the FAA certifies that this amendment will not have a significant economic impact on a substantial

number of small entities under the criteria of the Regulatory Flexibility Act.

Lists of Subjects in 14 CFR Part 97

Air Traffic Control, Airports, Incorporation by reference, Navigation (Air).

Issued in Washington, DC, on March 3, 2023.

Thomas J Nichols,

Aviation Safety, Flight Standards Service, Manager, Standards Section, Flight Procedures & Airspace Group, Flight Technologies & Procedures Division.

Adoption of the Amendment

Accordingly, pursuant to the authority delegated to me, 14 CFR part 97 is amended by establishing, amending, suspending, or removing Standard Instrument Approach Procedures and/or Takeoff Minimums and Obstacle Departure Procedures effective at 0901 UTC on the dates specified, as follows:

PART 97—STANDARD INSTRUMENT APPROACH PROCEDURES

■ 1. The authority citation for part 97 continues to read as follows:

Authority: 49 U.S.C. 106(f), 106(g), 40103, 40106, 40113, 40114, 40120, 44502, 44514, 44701, 44719, 44721–44722.

■ 2. Part 97 is amended to read as follows:

Effective 20 April 2023

Fayetteville/Springdale/Rogers, AR, KXNA, ILS OR LOC RWY 16, Amdt 4A, CANCELED

Fayetteville/Springdale/Rogers, AR, KXNA, ILS OR LOC RWY 16L, Orig

Fayetteville/Springdale/Rogers, AR, KXNA, ILS OR LOC RWY 34, Amdt 4A, CANCELED

Fayetteville/Springdale/Rogers, AR, KXNA, ILS OR LOC RWY 34R, Orig

Fayetteville/Springdale/Rogers, AR, KXNA, RNAV (GPS) RWY 16, Amdt 4A, CANCELED

Fayetteville/Springdale/Rogers, AR, KXNA, RNAV (GPS) RWY 16L, Orig

Fayetteville/Springdale/Rogers, AR, KXNA, RNAV (GPS) RWY 34, Amdt 2A, CANCELED

Fayetteville/Springdale/Rogers, AR, KXNA, RNAV (GPS) RWY 34R, Orig

Fayetteville/Springdale/Rogers, AR, KXNA, Takeoff Minimums and Obstacle DP, Amdt 5

St Petersburg-Clearwater, FL, KPIE, ILS OR LOC RWY 18, ILS RWY 18 (SA CAT I), ILS RWY 18 (SA CAT II), Amdt 1

Rome, GA, KRMG, ILS OR LOC RWY 1, Amdt 2

Rome, GA, KRMG, RNAV (GPS) RWY 1, Amdt 2

Rome, GA, KRMG, RNAV (GPS) RWY 7, Amdt 2

Rome, GA, KRMG, RNAV (GPS) RWY 19, Amdt 2

Rome, GA, KRMG, RNAV (GPS) RWY 25, Amdt 2

Rome, GA, KRMG, Takeoff Minimums and Obstacle DP, Amdt 5

Clinton, IA, KCWI, ILS OR LOC RWY 3, Amdt 6

Paris, ID, 1U7, BEAR LAKE ONE, GRAPHIC DP

Paris, ID, 1U7, FIROS ONE, GRAPHIC DP

Rexburg, ID, KRXE, RNAV (GPS) RWY 35, Amdt 2

Chicago, IL, KMDW, ILS OR LOC RWY 31C, Amdt 3A

Chicago, IL, KMDW, RNAV (GPS) Z RWY 22L, Amdt 2A

Chicago, IL, KMDW, RNAV (GPS) Z RWY 31C, Amdt 4A

Dodge City, KS, KDDC, VOR RWY 32, Amdt 5D

Hammond, LA, KHDC, RNAV (GPS) RWY 13, Orig

Hammond, LA, KHDC, RNAV (GPS) RWY 31, Amdt 1C

Fertile, MN, D14, RNAV (GPS) RWY 14, Orig

Fertile, MN, D14, RNAV (GPS) RWY 32, Orig

Fertile, MN, D14, Takeoff Minimums and Obstacle DP, Orig

Brookhaven, MS, 1R7, RNAV (GPS) RWY 23, Amdt 1

Natchez, MS, KHEZ, Takeoff Minimums and Obstacle DP, Orig-A

Manteo, NC, KMQI, RNAV (GPS) RWY 5, Orig-D

Manteo, NC, KMQI, RNAV (GPS) RWY 17, Orig-B

Manteo, NC, KMQI, RNAV (GPS) RWY 23, Orig-C

Grants, NM, KGNT, Takeoff Minimums and Obstacle DP, Amdt 1

Christmas Valley, OR, 62S, RNAV (GPS)-A, Orig

Christmas Valley, OR, 62S, Takeoff Minimums and Obstacle DP, Orig

Commerce, TX, 2F7, RNAV (GPS) RWY 18, Amdt 1

Jackson, WY, KJAC, ILS Z OR LOC Z RWY 19, Amdt 2

Jackson, WY, KJAC, RNAV (GPS) Z RWY 19, Amdt 3

[FR Doc. 2023-07049 Filed 4-4-23; 8:45 am]

BILLING CODE 4910-13-P

DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

14 CFR Part 97

[Docket No. 31477; Amdt. No. 4052]

Standard Instrument Approach Procedures, and Takeoff Minimums and Obstacle Departure Procedures; Miscellaneous Amendments

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Final rule.

SUMMARY: This rule amends, suspends, or removes Standard Instrument Approach Procedures (SIAPs) and associated Takeoff Minimums and Obstacle Departure Procedures for

operations at certain airports. These regulatory actions are needed because of the adoption of new or revised criteria, or because of changes occurring in the National Airspace System, such as the commissioning of new navigational facilities, adding new obstacles, or changing air traffic requirements. These changes are designed to provide for the safe and efficient use of the navigable airspace and to promote safe flight operations under instrument flight rules at the affected airports.

DATES: This rule is effective April 5, 2023. The compliance date for each SIAP, associated Takeoff Minimums, and ODP is specified in the amendatory provisions.

The incorporation by reference of certain publications listed in the regulations is approved by the Director of the Federal Register as of April 5, 2023.

ADDRESSES: Availability of matter incorporated by reference in the amendment is as follows:

For Examination

1. U.S. Department of Transportation, Docket Ops-M30, 1200 New Jersey Avenue SE, West Bldg., Ground Floor, Washington, DC 20590-0001;

2. The FAA Air Traffic Organization Service Area in which the affected airport is located;

3. The office of Aeronautical Information Services, 6500 South MacArthur Blvd., Oklahoma City, OK 73169 or,

4. The National Archives and Records Administration (NARA).

For information on the availability of this material at NARA, email fr.inspection@nara.gov or go to: <https://www.archives.gov/federal-register/cfr/ibr-locations.html>.

Availability

All SIAPs and Takeoff Minimums and ODPs are available online free of charge. Visit the National Flight Data Center online at nfdc.faa.gov to register. Additionally, individual SIAP and Takeoff Minimums and ODP copies may be obtained from the FAA Air Traffic Organization Service Area in which the affected airport is located.

FOR FURTHER INFORMATION CONTACT: Thomas J. Nichols, Flight Procedures and Airspace Group, Flight Technologies and Procedures Division, Flight Standards Service, Federal Aviation Administration. Mailing Address: FAA Mike Monroney Aeronautical Center, Flight Procedures and Airspace Group, 6500 South MacArthur Blvd., STB Annex, Bldg. 26,

Room 217, Oklahoma City, OK 73099. Telephone: (405) 954-1139.

SUPPLEMENTARY INFORMATION: This rule amends 14 CFR part 97 by amending the referenced SIAPs. The complete regulatory description of each SIAP is listed on the appropriate FAA Form 8260, as modified by the National Flight Data Center (NFDC)/Permanent Notice to Airmen (P-NOTAM), and is incorporated by reference under 5 U.S.C. 552(a), 1 CFR part 51, and 14 CFR 97.20. The large number of SIAPs, their complex nature, and the need for a special format make their verbatim publication in the **Federal Register** expensive and impractical. Further, airmen do not use the regulatory text of the SIAPs, but refer to their graphic depiction on charts printed by publishers of aeronautical materials. Thus, the advantages of incorporation by reference are realized and publication of the complete description of each SIAP contained on FAA form documents is unnecessary. This amendment provides the affected CFR sections, and specifies the SIAPs and Takeoff Minimums and ODPs with their applicable effective dates. This amendment also identifies the airport and its location, the procedure and the amendment number.

Availability and Summary of Material Incorporated by Reference

The material incorporated by reference is publicly available as listed in the **ADDRESSES** section.

The material incorporated by reference describes SIAPs, Takeoff Minimums and ODPs as identified in the amendatory language for Part 97 of this final rule.

The Rule

This amendment to 14 CFR part 97 is effective upon publication of each separate SIAP and Takeoff Minimums and ODP as amended in the transmittal.

For safety and timeliness of change considerations, this amendment incorporates only specific changes contained for each SIAP and Takeoff Minimums and ODP as modified by FDC permanent NOTAMs.

The SIAPs and Takeoff Minimums and ODPs, as modified by FDC permanent NOTAM, and contained in this amendment are based on criteria contained in the U.S. Standard for Terminal Instrument Procedures (TERPS). In developing these changes to SIAPs and Takeoff Minimums and ODPs, the TERPS criteria were applied only to specific conditions existing at the affected airports. All SIAP amendments in this rule have been previously issued by the FAA in a FDC NOTAM as an emergency action of immediate flight safety relating directly to published aeronautical charts.

The circumstances that created the need for these SIAP and Takeoff Minimums and ODP amendments require making them effective in less than 30 days.

Because of the close and immediate relationship between these SIAPs, Takeoff Minimums and ODPs, and safety in air commerce, I find that notice and public procedure under 5 U.S.C. 553(b) are impracticable and contrary to the public interest and, where applicable, under 5 U.S.C. 553(d), good cause exists for making these SIAPs effective in less than 30 days.

The FAA has determined that this regulation only involves an established body of technical regulations for which frequent and routine amendments are necessary to keep them operationally current. It, therefore—(1) is not a “significant regulatory action” under Executive Order 12866; (2) is not a “significant rule” under DOT regulatory Policies and Procedures (44 FR 11034; February 26, 1979); and (3) does not warrant preparation of a regulatory evaluation as the anticipated impact is

so minimal. For the same reason, the FAA certifies that this amendment will not have a significant economic impact on a substantial number of small entities under the criteria of the Regulatory Flexibility Act.

List of Subjects in 14 CFR Part 97

Air Traffic Control, Airports, Incorporation by reference, Navigation (Air).

Issued in Washington, DC, on March 3, 2023.

Thomas J Nichols,

Aviation Safety, Flight Standards Service, Manager, Standards Section, Flight Procedures & Airspace Group, Flight Technologies & Procedures Division.

Adoption of the Amendment

Accordingly, pursuant to the authority delegated to me, 14 CFR part 97 is amended by amending Standard Instrument Approach Procedures and Takeoff Minimums and ODPs, effective at 0901 UTC on the dates specified, as follows:

PART 97—STANDARD INSTRUMENT APPROACH PROCEDURES

■ 1. The authority citation for part 97 continues to read as follows:

Authority: 49 U.S.C. 106(f), 106(g), 40103, 40106, 40113, 40114, 40120, 44502, 44514, 44701, 44719, 44721-44722.

■ 2. Part 97 is amended to read as follows:

By amending: § 97.23 VOR, VOR/DME, VOR or TACAN, and VOR/DME or TACAN; § 97.25 LOC, LOC/DME, LDA, LDA/DME, SDF, SDF/DME; § 97.27 NDB, NDB/DME; § 97.29 ILS, ILS/DME, MLS, MLS/DME, MLS/RNAV; § 97.31 RADAR SIAPs; § 97.33 RNAV SIAPs; and § 97.35 COPTER SIAPs, Identified as follows:

* * * *Effective Upon Publication*

AIRAC date	State	City	Airport	FDC No.	FDC date	Subject
20-Apr-23 ...	IA	Grinnell	Grinnell Rgnl	2/1418	12/8/22	RNAV (GPS) RWY 31, Amdt 1
20-Apr-23 ...	LA	Lake Charles	Lake Charles Rgnl	2/1844	12/19/22	RNAV (GPS) RWY 23, Amdt 1
20-Apr-23 ...	TN	Sparta	Upper Cumberland Rgnl	2/5202	2/15/23	ILS OR LOC RWY 4, Amdt 1C
20-Apr-23 ...	MA	Boston	General Edward Law- rence Logan Intl.	2/5729	12/16/22	ILS OR LOC RWY 4R, ILS RWY 4R (SA CAT I), ILS RWY 4R (CAT II AND III), Amdt 11
20-Apr-23 ...	TX	Houston	David Wayne Hooks Meml.	3/0269	2/3/23	Takeoff Minimums and Obstacle DP, Amdt 3
20-Apr-23 ...	MN	Tracy	Tracy Muni	3/1509	2/8/23	RNAV (GPS) RWY 11, Orig-B
20-Apr-23 ...	MN	Tracy	Tracy Muni	3/1510	2/8/23	RNAV (GPS) RWY 29, Amdt 1
20-Apr-23 ...	MI	Gladwin	Gladwin Zettel Meml	3/1512	2/8/23	RNAV (GPS) RWY 27, Orig-C
20-Apr-23 ...	OH	Toledo	Eugene F Kranz Toledo Express.	3/1523	2/8/23	ILS Z OR LOC Z RWY 7, Amdt 29A
20-Apr-23 ...	OH	Bucyrus	Port Bucyrus/Crawford County.	3/1540	2/8/23	RNAV (GPS) RWY 4, Orig-A
20-Apr-23 ...	WY	Laramie	Laramie Rgnl	3/1543	2/14/23	RNAV (GPS) RWY 12, Orig-B
20-Apr-23 ...	SC	Laurens	Laurens County	3/1614	2/8/23	RNAV (GPS) RWY 26, Amdt 1
20-Apr-23 ...	SC	Laurens	Laurens County	3/1615	2/8/23	RNAV (GPS) RWY 8, Amdt 1

AIRAC date	State	City	Airport	FDC No.	FDC date	Subject
20-Apr-23 ...	TX	Tyler	Tyler Pounds Rgnl	3/1707	1/6/23	ILS OR LOC RWY 4, Orig
20-Apr-23 ...	TX	Tyler	Tyler Pounds Rgnl	3/1708	1/6/23	RNAV (GPS) RWY 4, Amdt 4A
20-Apr-23 ...	TX	Tyler	Tyler Pounds Rgnl	3/1709	1/6/23	VOR RWY 4, Amdt 5B
20-Apr-23 ...	KY	Hazard	Wendell H Ford	3/1719	2/8/23	RNAV (GPS) RWY 14, Amdt 1D
20-Apr-23 ...	FL	Apalachicola	Apalachicola Rgnl-Cleve Randolph Fld.	3/1857	1/6/23	RNAV (GPS) RWY 32, Amdt 2E
20-Apr-23 ...	OK	Enid	Enid Woodring Rgnl	3/3127	2/17/23	ILS OR LOC RWY 35, Amdt 7B
20-Apr-23 ...	WI	Wautoma	Wautoma Muni	3/3132	1/12/23	RNAV (GPS) RWY 31, Orig-A
20-Apr-23 ...	WI	Wautoma	Wautoma Muni	3/3133	1/12/23	RNAV (GPS) RWY 13, Orig-A
20-Apr-23 ...	FL	Clewiston	Airglades	3/3252	1/13/23	RNAV (GPS) RWY 13, Orig-B
20-Apr-23 ...	FL	Clewiston	Airglades	3/3253	1/13/23	RNAV (GPS) RWY 31, Orig-A
20-Apr-23 ...	NY	Syracuse	Syracuse Hancock Intl	3/5994	2/15/23	RNAV (GPS) Z RWY 10, Amdt 3
20-Apr-23 ...	CA	Arcata/Eureka	California Redwood Coast-Humboldt County.	3/6152	2/6/23	RNAV (GPS) RWY 1, Amdt 2A
20-Apr-23 ...	NH	Nashua	Boire Fld	3/6191	1/23/23	ILS OR LOC RWY 14, Amdt 2
20-Apr-23 ...	ME	Rangeley	Stephen A Bean Muni	3/6292	2/16/23	RNAV (GPS)-D, Amdt 1
20-Apr-23 ...	TX	El Paso	El Paso Intl	3/7061	1/27/23	VOR RWY 26L, Amdt 32C
20-Apr-23 ...	CO	Colorado Springs	City Of Colorado Springs Muni.	3/7619	2/24/23	RNAV (GPS) Y RWY 17L, Amdt 3B
20-Apr-23 ...	CO	Colorado Springs	City Of Colorado Springs Muni.	3/7620	2/24/23	RNAV (GPS) Y RWY 17R, Amdt 3A
20-Apr-23 ...	CO	Colorado Springs	City Of Colorado Springs Muni.	3/7621	2/24/23	ILS OR LOC RWY 17L, ILS RWY 17L (SA CAT I & II), Amdt 3C
20-Apr-23 ...	CO	Colorado Springs	City Of Colorado Springs Muni.	3/7635	2/24/23	RNAV (RNP) Z RWY 17R, Amdt 1A
20-Apr-23 ...	CO	Colorado Springs	City Of Colorado Springs Muni.	3/7639	2/24/23	RNAV (RNP) Z RWY 17L, Amdt 2A
20-Apr-23 ...	CO	Colorado Springs	City Of Colorado Springs Muni.	3/7641	2/24/23	VOR RWY 17L, Orig
20-Apr-23 ...	FL	Miami	Miami Intl	3/7767	2/21/23	ILS OR LOC RWY 30, Amdt 1B
20-Apr-23 ...	TX	Houston	David Wayne Hooks Meml.	3/7775	2/21/23	LOC RWY 17R, Amdt 3F
20-Apr-23 ...	TX	Houston	David Wayne Hooks Meml.	3/7776	2/21/23	RNAV (GPS) RWY 35L, Amdt 1E
20-Apr-23 ...	NY	New York	John F Kennedy Intl	3/8629	1/31/23	Takeoff Minimums and Obstacle DP, Amdt 9
20-Apr-23 ...	IL	Bloomington/Normal	Central II Rgnl/Bloom- ington-Normal.	3/8684	2/23/23	ILS OR LOC RWY 29, Amdt 11C

[FR Doc. 2023-07050 Filed 4-4-23; 8:45 am]
BILLING CODE 4910-13-P

FEDERAL COMMUNICATIONS COMMISSION

47 CFR Part 73

[GN Docket No. 16-142; FCC 23-11; FR ID 130372]

Authorizing Permissive Use of the “Next Generation” Broadcast Television Standard

AGENCY: Federal Communications Commission.

ACTION: Final rule; stay of effectiveness.

SUMMARY: In this document, the Federal Communications Commission (“FCC” or “Commission”) announces that it has temporarily stayed the March 6, 2023 sunset of the requirement for broadcaster primary streams to comply with the ATSC A/322 standard.

DATES: This rule is effective April 5, 2023. Effective April 5, 2023, 47 CFR 73.682(f)(2)(iii) is stayed indefinitely.

FOR FURTHER INFORMATION CONTACT: For additional information, contact Evan Baranoff, *Evan.Baranoff@fcc.gov*, of the Media Bureau, Policy Division, (202) 418-7142. Direct press inquiries to Janice Wise at (202) 418-8165.

SUPPLEMENTARY INFORMATION: This is a summary of the Commission’s Order, FCC 23-11, adopted on March 3, 2023 and released on March 6, 2023. The full text of this document is available electronically via the FCC’s website at <https://docs.fcc.gov/public/attachments/FCC-23-11A1.pdf> or at <https://www.fcc.gov/ecfs>. (Documents will be available electronically in ASCII, Microsoft Word, and/or Adobe Acrobat.) Alternative formats are available for people with disabilities (Braille, large print, electronic files, audio format), by sending an email to *fcc504@fcc.gov* or calling the Commission’s Consumer and Governmental Affairs Bureau at (202)

418-0530 (voice), (202) 418-0432 (TTY).

Synopsis

1. By this document the Commission temporarily stays the March 6, 2023 sunset of the requirement for broadcaster primary streams to comply with the ATSC A/322 standard.¹

2. In 2017, the Commission authorized television broadcasters to use the Next Gen TV transmission standard, also called “ATSC 3.0” or “3.0,” on a voluntary, market-driven basis. Under Commission rules, the requirement for broadcaster primary streams to comply with the ATSC A/322 standard, defining the waveforms that ATSC 3.0 signals may take, was scheduled to sunset on March 6, 2023. Last June, we issued the Sunsets further notice of proposed rulemaking (FNPRM)

¹ 47 CFR 73.682(f) (requiring that, until March 6, 2023, the transmission of at least one free over the air primary video programming stream comply with the ATSC A/322). The rule, including the sunset date, was established in the *First Next Gen TV Report and Order*, 83 FR 4998.

(87 FR 40465, July 7, 2022) seeking comment on, among other things, the expiration of this rule, whether to retain the requirement and, if so, for how long. That proceeding remains pending.

3. For the reasons set forth herein, we find good cause to stay, on our own motion, the expiration of this rule pending a Commission resolution of this issue in the above-referenced proceeding. In considering a stay, the Commission considers the four criteria set forth in Virginia Petroleum Jobbers Association.²

4. We conclude that an interim stay of the A/322 “sunset” is appropriate under the circumstances. Virtually all commenters addressing this question made arguments in favor of at least a temporary extension of the requirement to comply with A/322. It is unclear whether any consumer receive equipment could display 3.0 signals that were noncompliant with A/322, meaning the viewing public could lose all 3.0 service during any period of noncompliance by broadcasters. Furthermore, there is no information in the record indicating that any party will be harmed by the grant of an interim stay.³ In light of the arguments offered by commenters for at least a temporary extension, the possibility of harm to the viewing public from the disruption of eliminating and then potentially resuming the requirement, and the lack of any reasonable expectation of sunset by those currently deploying 3.0 service in light of the pendency of this proceeding, we find the public interest is best served by preserving the status quo during this brief period of time in order to consider this open question.

5. We therefore stay the sunset of the A/322 rule, pending resolution of the Sunsets FNPRM.

6. Accordingly, it is ordered, that, pursuant to sections 1, 4(i), 4(j), and 303 of the Communications Act of 1934, as amended, 47 U.S.C. 151, 154(i), 154(j), 303 and § 1.103 of the Commission’s rules, 47 CFR 1.103, § 73.682(f)(2) of the Commission’s rules, 47 CFR 73.682(f)(2), is amended as set forth in the amendments at the end of this

² *Virginia Petroleum Jobbers Ass’n v. Federal Power Commission*, 259 F.2d 921, 925 (D.C. Cir. 1958). See also *Implementation of Sections 309(j) and 337 of the Communications Act of 1934 as Amended*, Order, 18 FCC Rcd 25491, 25494, para. 6 (2003) (73 FR 21843, April 23, 2008) (*PLMR Narrowband Stay Order*). As described in the *PLMR Narrowband Stay Order*, these criteria are (1) a likelihood of success on the merits; (2) the threat of irreparable harm absent the grant of preliminary relief; (3) the degree of injury to other parties if relief is granted; and (4) the issuance of the order will further the public interest.

³ The only commenter in the record supporting an immediate sunset of this requirement identified no harms associated with this specific rule.

document and § 73.682(f)(2)(iii) of the Commission’s rules, 47 CFR 73.682(f)(2)(iii), is stayed effective immediately.

List of Subjects in 47 CFR Part 73

Communications equipment,
Television.

Federal Communications Commission.

Marlene Dortch,
Secretary.

For the reasons stated in the preamble, the Federal Communications Commission amends 47 CFR part 73 as set forth below:

PART 73—RADIO BROADCAST SERVICES

■ 1. The authority citation for part 73 continues to read as follows:

Authority: 47 U.S.C. 154, 155, 301, 303, 307, 309, 310, 334, 336, 339.

■ 2. Section 73.682 is amended by:

- a. Revising paragraph (f)(2); and
- b. Staying paragraph (f)(2)(iii) indefinitely.

The revision reads as follows:

§ 73.682 TV transmission standards.

* * * * *

(f) * * *

(2)(i) Effective March 5, 2018, transmission of Next Gen TV broadcast television (ATSC 3.0) signals shall comply with the standards for such transmissions set forth in ATSC A/321:2016, “System Discovery and Signaling” (March 23, 2016) (incorporated by reference, see § 73.8000). To the extent that virtual channels (specified in the DTV transmission standard referenced in ATSC A/65C:2006 in paragraph (d) of this section) are used in the transmission of Next Gen TV broadcasting, major channel numbers shall be assigned as required by ATSC A/65C:2006 Annex B (incorporated by reference, see § 73.8000).

(ii) In addition, such signals shall also comply with the standards set forth in ATSC A/322:2017 “Physical Layer Protocol” (June 6, 2017) (incorporated by reference, see § 73.8000) with respect to the transmission of at least one free over the air primary video programming stream.

(iii) Paragraph (f)(2)(ii) of this section will sunset on March 6, 2023.

* * * * *

[FR Doc. 2023–05047 Filed 4–3–23; 11:15 am]

BILLING CODE 6712-01-P

GENERAL SERVICES ADMINISTRATION

48 CFR Parts 538 and 552

[GSAR Case 2023–G504; Docket No. GSA–GSAR–2023–0011; Sequence No. 1]

General Services Administration Acquisition Regulation; Federal Supply Schedule Clause Corrections

AGENCY: Office of Acquisition Policy, General Services Administration (GSA).

ACTION: Final rule; technical amendment.

SUMMARY: The General Services Administration is issuing this final rule as a technical amendment to make corrections and editorial changes to remove outdated Federal Supply Schedule terminology and incorrect references in the General Services Administration Acquisition Regulation.

DATES: Effective May 5, 2023.

FOR FURTHER INFORMATION CONTACT: For clarification of content, contact Ms. Daria Giannotti, Procurement Analyst, at 215–446–2878 or GSARPolicy@gsa.gov. For information pertaining to status or publication schedules, contact the Regulatory Secretariat Division at GSARRegSec@gsa.gov or 202–501–4755. Please cite GSAR Case 2023–G504.

SUPPLEMENTARY INFORMATION:

I. Background

The General Services Administration (GSA) conducts routine reviews of its acquisition regulations to identify outdated content. As part of this review, GSA identified:

- Incorrect references to General Services Administration Acquisition Regulation (GSAR) subsections within a few GSAR clauses needing editorial updates.
- Several outdated Special Item Number (SIN) and Federal Supply Schedule (FSS) references resulting from the consolidation of the Multiple Award Schedule (MAS) needing editorial updates.
 - For additional background, a SIN is a type of labeling used on MAS to identify products and services contract holders offer.
 - MAS, also known as the Federal Supply Schedule (FSS) and the GSA Schedule, is a long-term governmentwide contract with commercial companies that provide access to millions of commercial products and services at fair and reasonable prices to the Federal Government.
 - Five clauses and three sections needing editorial updates resulting from the consolidation of the MAS.

○ For additional background, the consolidation of the MAS began in 2020 and resulted in the consolidation of 24 existing Schedules into one single Schedule for products, services, and solutions. This included Schedules 70 and 84. As part of the MAS consolidation, the SIN structure and category descriptions were updated. This technical amendment makes conforming changes.

Overview of Editorial Updates

In GSAR subpart 538.2, section 538.273 was amended to revise the clause title for section 552.238–74 in order to align the title with the Introduction of New Supplies and Services SIN resulting from the MAS consolidation. The clause prescription for section 552.238–109 was also amended to align with the consolidated MAS and SIN references.

In subpart 538.70, sections 538.7000 and 538.7001 were amended to remove references to Federal Supply Schedules 70 and 84, as these Schedules were part of the MAS consolidation.

In subpart 552.2, five clauses were amended as follows:

- The GSAM reference in the note to paragraph (b)(2) of section 552.216–75 was corrected to 507.103(b)(3).
- The title of clause 552.238–74 was revised to align with the Introduction of New Supplies and Services SIN. The text within this clause was also amended throughout to reflect the same.
- The GSAM reference in the note to paragraph (b)(2) of Alternate I of section 552.238–80 was corrected to 507.103(b)(3).
- Paragraph (a) of section 552.238–110 was amended to remove outdated SIN references and editorial changes were made in paragraph (c)(1).
- Paragraph (a) of section 552.238–113 was amended to remove outdated SIN references. Paragraph (d)(1) was amended to remove references to Federal Supply Schedules 70 and 84. Editorial changes were also made throughout paragraph (d).

In subpart 552.3, the title of clause 552.238–74 was revised to align with the Introduction of New Supplies and Services SIN as a result of the MAS consolidation.

II. Publication of This Final Rule for Public Comment Is Not Required by Statute

The statute that applies to the publication of the Federal Acquisition Regulation (FAR) is 41 U.S.C. 1707. Subsection (a)(1) of 41 U.S.C. 1707 requires that a procurement policy,

regulation, procedure, or form (including an amendment or modification thereof) must be published for public comment if it relates to the expenditure of appropriated funds, and has either a significant effect beyond the internal operating procedures of the agency issuing the policy, regulation, procedure, or form, or has a significant cost or administrative impact on contractors or offerors. This final rule is not required to be published for public comment because the change is technical in nature and makes conforming updates to the title and number of a referenced policy document.

III. Executive Orders 12866 and 13563

Executive Orders (E.O.s) 12866 and 13563 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). E.O. 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. The Office of Information and Regulatory Affairs (OIRA) in the Office of Management and Budget (OMB) has determined that this is not a significant regulatory action and, therefore, was not subject to review under Section 6(b) of Executive Order 12866, Regulatory Planning and Review, dated September 30, 1993.

IV. Congressional Review Act

The Congressional Review Act, 5 U.S.C. 801 *et seq.*, as amended by the Small Business Regulatory Enforcement Fairness Act of 1996, generally provides that before a “major rule” may take effect, the agency promulgating the rule must submit a rule report, which includes a copy of the rule, to each House of the Congress and to the Comptroller General of the United States. The General Services Administration will submit a report containing this rule and other required information to the U.S. Senate, the U.S. House of Representatives, and the Comptroller General of the United States. A major rule cannot take effect until 60 days after it is published in the **Federal Register**. OIRA has determined that this is not a major rule under 5 U.S.C. 804.

V. Regulatory Flexibility Act

The Regulatory Flexibility Act (5 U.S.C. 601 *et seq.*) does not apply to this rule, because an opportunity for public

comment is not required to be given for this rule under 41 U.S.C. 1707(a)(1) (see Section II. of this preamble). Accordingly, no regulatory flexibility analysis is required, and none has been prepared.

VI. Paperwork Reduction Act

The Paperwork Reduction Act does not apply because the changes to the GSAR do not impose recordkeeping or information collection requirements, or the collection of information from offerors, contractors, or members of the public that require the approval of the Office of Management and Budget under 44 U.S.C. 3501, *et seq.*

List of Subjects in 48 CFR Parts 538 and 552

Government procurement.

Jeffrey A. Koses,

Senior Procurement Executive, Office of Acquisition Policy, Office of Government-wide Policy, General Services Administration.

Therefore, GSA amends 48 CFR parts 538 and 552 as set forth below:

- 1. The authority citation for 48 CFR parts 538 and 552 continues to read as follows:

Authority: 40 U.S.C. 121(c).

PART 538—FEDERAL SUPPLY SCHEDULE CONTRACTING

538.273 [Amended]

- 2. Amend section 538.273 by removing from paragraph (b)(2) the phrase “New Supplies/Services (INSS)” and adding “New Supplies and Services Special Item Number (SIN)” in its place and revising paragraph (d)(33).

The revision reads as follows:

538.273 FSS solicitation provisions and contract clauses.

* * * * *

(d) * * *

(33) 552.238–109, Authentication Supplies and Services. Use in Federal Supply Schedule solicitations that contain information technology Special Item Numbers (SINs) only, and only contracts awarded SINs associated with the Homeland Security Presidential Directive 12 (HSPD–12).

* * * * *

- 3. Revise section 538.7000 to read as follows:

538.7000 Scope of subpart.

This subpart prescribes policies and procedures that implement statutory provisions authorizing non-federal organizations to use—

- (a) The Consolidated Schedule contracts containing information

technology or security and protection Special Item Numbers (SINs); and
 (b) Other Federal Supply Schedules as authorized in this subpart.

538.7001 [Amended]

■ 4. Amend section 538.7001 by removing the definitions of “Schedule 70” and “Schedule 84”.

PART 552—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

■ 5. Amend section 552.216–75 by—
 ■ a. Revising the date of the clause; and
 ■ b. Removing from the note to paragraph (b)(2) the citation “507.105(c)(3)” and adding “507.103(b)(3)” in its place.

The revision reads as follows:

552.216–75 Transactional Data Reporting.

* * * * *

Transactional Data Reporting (MAY 2023)

* * * * *

■ 6. Amend section 552.238–74 by—
 ■ a. Revising the section heading and the heading and date of the provision;
 ■ b. In paragraph (a) removing the definition heading “Introduction of New Supplies/Services Special Item Number (INSS SIN)” and adding “Introduction of New Supplies and Services Special Item Number (SIN)” in its place; and
 ■ c. Revising paragraphs (b), (c), and (d).
 The revisions read as follows:

552.238–74 Introduction of New Supplies and Services Special Item Number (SIN).

* * * * *

Introduction of New Supplies and Services Special Item Number (SIN) (MAY 2023)

(a) * * *

Introduction of New Supplies and Services Special Item Number (SIN)
 * * *

(b) Offerors are encouraged to introduce new or improved supplies or services via the “Introduction of New Supplies and Services SIN” at any time by clearly identifying this SIN item in the offer.

(c) The Contracting Officer has the sole discretion to determine whether a supply or service will be accepted as an “Introduction of New Supplies and Services SIN” item. The Contracting Officer will evaluate and process the offer and may perform a technical review. This SIN provides temporary placement until the Contracting Officer formally categorizes the new supply or service.

(d) If the Contractor has an existing schedule contract, GSA may, at the sole

discretion of the Contracting Officer, modify the existing contract to include the “Introduction of New Supplies and Services SIN” item in accordance with 552.238–82, Modifications (Federal Supply Schedules).

* * * * *

■ 7. Amend section 552.238–80 in Alternate I by—

■ a. Revising the date of the Alternate;
 ■ b. Removing from the note to paragraph (b)(2) the citation “507.105(c)(3)” and adding “507.103(b)(3)” in its place; and
 ■ c. Removing from the last sentence in paragraph (c)(1) the word “benefitting” and adding “benefiting” in its place.

The revision reads as follows:

552.238–80 Industrial Funding Fee and Sales Reporting.

* * * * *

Alternate I (MAY 2023). * * *

* * * * *

■ 8. Amend section 552.238–110 by revising the date of the clause and paragraph (a) to read as follows:

552.238–110 Commercial Satellite Communication (COMSATCOM) Services.

* * * * *

Commercial Satellite Communication (COMSATCOM) Services (MAY 2023)

(a) *General background.* A Special Item Number (SIN) has been established for Commercial Satellite Communications (COMSATCOM) services, focused on transponded capacity and fixed and mobile subscription services, to make available common COMSATCOM services to all Ordering Activities.

* * * * *

■ 9. Amend 552.238–113 by—
 ■ a. Revising the date of the clause;
 ■ b. Removing from the second sentence in paragraph (a) introductory text the phrase “Special Item Number 132–53, Wireless Services” and adding “the Wireless Mobility Services Special Item Number” in its place;
 ■ c. Revising paragraph (d)(1); and
 ■ d. Removing from paragraphs (d)(2), (3), and (4) the word “PROVIDED” and adding “provided” in its place, respectively.

The revisions read as follows:

552.238–113 Scope of Contract (Eligible Ordering Activities).

* * * * *

Scope of Contract (Eligible Ordering Activities) (MAY 2023)

(d) * * *

(1) State and local government may place orders against Consolidated

Schedule contracts containing information technology or security and protection Special Item Numbers, on an optional basis; provided, the Contractor accepts order(s) from such activities;

* * * * *

[FR Doc. 2023–07053 Filed 4–4–23; 8:45 am]

BILLING CODE 6820–61–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

50 CFR Part 622

[Docket No. 120404257–3325–02; RTID 0648–XC895]

Fisheries of the Caribbean, Gulf of Mexico, and South Atlantic; Re-Opening of the Commercial Longline Fishery for Golden Tilefish in the South Atlantic

AGENCY: National Marine Fisheries Service (NMFS), National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Temporary rule; re-opening.

SUMMARY: NMFS announces the re-opening of the commercial longline component for golden tilefish in the exclusive economic zone (EEZ) of the South Atlantic through this temporary rule. The most recent commercial longline landings data for golden tilefish indicate the commercial longline annual catch limit (ACL) for the 2023 fishing year has not yet been reached. Therefore, NMFS re-opens the commercial longline component to harvest golden tilefish in the South Atlantic EEZ for 3 days. The purpose of this temporary rule is to allow for the commercial longline ACL for golden tilefish to be harvested while minimizing the risk of exceeding the commercial ACL.

DATES: This temporary rule is effective from 12:01 a.m. eastern time on April 4, 2023, until 12:01 a.m. eastern time on April 7, 2023.

FOR FURTHER INFORMATION CONTACT: Mary Vara, NMFS Southeast Regional Office, telephone: 727–824–5305, email: mary.vara@noaa.gov.

SUPPLEMENTARY INFORMATION: The snapper-grouper fishery of the South Atlantic includes golden tilefish and is managed under the Fishery Management Plan for the Snapper-Grouper Fishery of the South Atlantic Region (FMP). The FMP was prepared by the South Atlantic Fishery Management Council (Council) and is implemented by NMFS under the

authority of the Magnuson-Stevens Fishery Conservation and Management Act (Magnuson-Stevens Act) by regulations at 50 CFR part 622.

The commercial sector for golden tilefish comprises the longline and hook-and-line components. The commercial golden tilefish ACL is allocated 75 percent to the longline component and 25 percent to the hook-and-line component. The commercial ACL (equivalent to the commercial quota) is 331,740 lb (150,475 kg) in gutted weight, and the longline component quota is 248,805 lb (112,856 kg) in gutted weight (50 CFR 622.190(a)(2)(iii)).

Under 50 CFR 622.193(a)(1)(ii), NMFS is required to close the commercial longline component for golden tilefish when the longline component's commercial quota specified under 50 CFR 622.190(a)(2)(iii) is reached or is projected to be reached by filing a notification to that effect with the Office of the Federal Register. After the longline component quota is reached or is projected to be reached, golden tilefish may not be commercially fished or possessed by a vessel with a golden tilefish longline endorsement. NMFS previously determined that the commercial quota for the golden tilefish longline component in the South Atlantic would be reached by February 26, 2023. Therefore, NMFS published a temporary rule to close the commercial longline component for South Atlantic golden tilefish from February 26, 2023, through the end of the 2023 fishing year (88 FR 11397, February 23, 2023). However, a more recent estimation of golden tilefish landings harvested by longline gear indicates that the commercial longline ACL for golden tilefish has not been met.

In accordance with 50 CFR 622.8(c), NMFS temporarily re-opens the commercial longline component for golden tilefish on April 4, 2023. The commercial longline component will remain open for 3 days to allow for the commercial longline ACL to be reached. The commercial longline component will be closed from 12:01 a.m. eastern time on April 7, 2023, until January 1, 2024, the start of the next fishing year. NMFS has determined that this re-opening will allow an additional opportunity to commercially harvest the golden tilefish longline component quota while minimizing the risk of exceeding the commercial ACL.

The operator of a vessel with a valid Federal commercial vessel permit for South Atlantic snapper-grouper and a valid commercial longline endorsement for golden tilefish having golden tilefish on board must have landed and

bartered, traded, or sold such golden tilefish before 12:01 a.m. eastern time on April 7, 2023. During the subsequent commercial longline closure, golden tilefish may still be commercially harvested using hook-and-line gear while the hook-and-line component is open. However, a vessel with a golden tilefish longline endorsement is not eligible to fish for or possess golden tilefish using hook-and-line gear under the hook-and-line commercial trip limit, as specified in 50 CFR 622.191(a)(2)(ii). The operator of a vessel with a valid Federal commercial vessel permit for South Atlantic snapper-grouper and a valid commercial longline endorsement for golden tilefish with golden tilefish on board must have landed and bartered, traded, or sold such golden tilefish before 12:01 a.m. eastern time on April 7, 2023. During the commercial longline closure, the recreational bag and possession limits specified in 50 CFR 622.187(b)(2)(iii) and (c)(1), respectively, apply to all harvest or possession of golden tilefish in or from the South Atlantic EEZ by a vessel with a golden tilefish longline endorsement.

The sale or purchase of longline-caught golden tilefish taken from the South Atlantic EEZ is prohibited during the commercial longline closure. The prohibition on sale or purchase does not apply to the sale or purchase of longline-caught golden tilefish that were harvested, landed ashore, and sold before 12:01 a.m. eastern time on April 7, 2023, and were held in cold storage by a dealer or processor. Additionally, the recreational bag and possession limits and the sale and purchase provisions of the commercial closure apply to a person on board a vessel with a golden tilefish longline endorsement, regardless of whether the golden tilefish are harvested in state or Federal waters, as specified in 50 CFR 622.190(c)(1).

Classification

NMFS issues this action pursuant to section 305(d) of the Magnuson-Stevens Act. This action is required by 50 CFR 622.190(a)(2)(iii) and 622.193(a)(1)(ii), issued pursuant to section 304(b), and is exempt from review under Executive Order 12866.

Pursuant to 5 U.S.C. 553(b)(B), there is good cause to waive prior notice and an opportunity for public comment on this action, as notice and comment is unnecessary. Such procedure is unnecessary, because the regulations associated with the commercial longline component quota for golden tilefish and a re-opening to provide an opportunity for the quota to be harvested have already been subject to notice and public comment, and all that remains is

to notify the public of the commercial longline component re-opening.

For the reasons stated earlier, the Assistant Administrator for Fisheries also finds good cause to waive the 30-day delay in the effectiveness of this action under 5 U.S.C. 553(d)(3).

Authority: 16 U.S.C. 1801 *et seq.*

Dated: March 30, 2023.

Jennifer M. Wallace,

Acting Director, Office of Sustainable Fisheries, National Marine Fisheries Service.

[FR Doc. 2023-07031 Filed 3-31-23; 4:15 pm]

BILLING CODE 3510-22-P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

50 CFR Part 679

[Docket No. 230306-0065; RTID 0648-XC860]

Fisheries of the Exclusive Economic Zone Off Alaska; Pacific Cod by Catcher Vessels Using Trawl Gear in the Bering Sea and Aleutian Islands Management Area

AGENCY: National Marine Fisheries Service (NMFS), National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Temporary rule; closure.

SUMMARY: NMFS is prohibiting directed fishing for Pacific cod by catcher vessels using trawl gear in the Bering Sea and Aleutian Islands management area (BSAI). This action is necessary to prevent exceeding the B season apportionment of the 2023 Pacific cod total allowable catch (TAC) allocated to catcher vessels using trawl gear in the BSAI.

DATES: Effective 1200 hours, Alaska local time (A.l.t.), April 2, 2023, through 1200 hours, A.l.t., June 10, 2023.

FOR FURTHER INFORMATION CONTACT: Krista Milani, 907-581-2062.

SUPPLEMENTARY INFORMATION: NMFS manages the groundfish fishery in the BSAI exclusive economic zone according to the Fishery Management Plan for Groundfish of the Bering Sea and Aleutian Islands Management Area (FMP) prepared by the North Pacific Fishery Management Council under authority of the Magnuson-Stevens Fishery Conservation and Management Act. Regulations governing fishing by U.S. vessels in accordance with the FMP appear at subpart H of 50 CFR part 600 and 50 CFR part 679.

The B season apportionment of the 2023 Pacific cod TAC allocated to

catcher vessels using trawl gear in the BSAI is 2,949 metric tons (mt) as established by the final 2023 and 2024 harvest specifications for groundfish in the BSAI (88 FR 14926, March 10, 2023).

In accordance with § 679.20(d)(1)(i), the Administrator, Alaska Region, NMFS (Regional Administrator), has determined that the B season apportionment of the 2023 Pacific cod TAC allocated to trawl catcher vessels in the BSAI will soon be reached. Therefore, the Regional Administrator is establishing a directed fishing allowance of 2,000 mt and is setting aside the remaining 949 mt as incidental catch to support other anticipated groundfish fisheries. In accordance with § 679.20(d)(1)(iii), the Regional Administrator finds that this directed fishing allowance has been reached. Consequently, NMFS is prohibiting

directed fishing for Pacific cod by catcher vessels using trawl gear in the BSAI.

While this closure is effective, the maximum retainable amounts at § 679.20(e) and (f) apply at any time during a trip.

Classification

NMFS issues this action pursuant to section 305(d) of the Magnuson-Stevens Act. This action is required by 50 CFR part 679, which was issued pursuant to section 304(b), and is exempt from review under Executive Order 12866.

Pursuant to 5 U.S.C. 553(b)(B), there is good cause to waive prior notice and an opportunity for public comment on this action, as notice and comment would be impracticable and contrary to the public interest, as it would prevent NMFS from responding to the most recent fisheries data in a timely fashion,

and would delay the closure of Pacific cod by catcher vessels using trawl gear in the BSAI. NMFS was unable to publish a notice providing time for public comment because the most recent, relevant data only became available as of March 30, 2023.

The Assistant Administrator for Fisheries, NOAA also finds good cause to waive the 30-day delay in the effective date of this action under 5 U.S.C. 553(d)(3). This finding is based upon the reasons provided above for waiver of prior notice and opportunity for public comment.

Authority: 16 U.S.C. 1801 *et seq.*

Dated: March 30, 2023.

Jennifer M. Wallace,

Acting Director, Office of Sustainable Fisheries, National Marine Fisheries Service.

[FR Doc. 2023-07014 Filed 3-31-23; 4:15 pm]

BILLING CODE 3510-22-P

Proposed Rules

Federal Register

Vol. 88, No. 65

Wednesday, April 5, 2023

This section of the FEDERAL REGISTER contains notices to the public of the proposed issuance of rules and regulations. The purpose of these notices is to give interested persons an opportunity to participate in the rule making prior to the adoption of the final rules.

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

33 CFR Part 117

[Docket No. USCG–2023–0113]

RIN 1625–AA09

Drawbridge Operation Regulation; Cheboygan River at Cheboygan, MI

AGENCY: Coast Guard, DHS.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Coast Guard proposes to modify the operating schedule that governs the US 23 Highway Bridge, mile 0.92, across the Cheboygan River—Part of the Inland Route, at Cheboygan, Michigan. The Cheboygan County Road Commission requested we extend the winter advance notice for the bridge. We invite your comments on this proposed rulemaking.

DATES: Comments and related material must reach the Coast Guard on or before June 5, 2023.

ADDRESSES: You may submit comments identified by docket number USCG–2023–0113 using Federal Decision Making Portal at <https://www.regulations.gov>.

See the “Public Participation and Request for Comments” portion of the **SUPPLEMENTARY INFORMATION** section below for instructions on submitting comments.

FOR FURTHER INFORMATION CONTACT: If you have questions on this proposed rule, call or email Mr. Lee D. Soule, Bridge Management Specialist, Ninth Coast Guard District; telephone 216–902–6085, email Lee.D.Soule@uscg.mil.

SUPPLEMENTARY INFORMATION:

I. Table of Abbreviations

CFR Code of Federal Regulations
 DHS Department of Homeland Security
 FR Federal Register
 IGLD85 International Great Lakes Datum of 1985
 MDNR Michigan Department of Natural Resources

MDOT Michigan Department of Transportation
 OMB Office of Management and Budget
 LWD Low Water Datum based on IGLD85
 NPRM Notice of Proposed Rulemaking (Advance, Supplemental)
 § Section
 U.S.C. United States Code

II. Background, Purpose, and Legal Basis

The Cheboygan River is part of the Michigan Inland Route. The Michigan Inland Route is the longest chain of rivers and lakes in the state of Michigan and is almost forty miles long. The waterway runs through Pickerel Lake, Crooked Lake, the Crooked River, Burt Lake, the Indian River, Mullett Lake, into the Cheboygan River, and eventually flowing into Lake Huron. The waterway is controlled by two Michigan Department of Natural Resources (MDNR) locks, one is in the Cheboygan River and the other is in the Crooked River.

The Michigan Inland Route can handle vessels up to sixty-five feet long with an eighteen-foot beam and has been open to interstate commerce since 1869 when the Cheboygan lock opened.

The US 23 Highway Bridge, mile 0.92, across the Cheboygan River is a double leaf bascule bridge providing a horizontal clearance of 60 feet and a vertical clearance of 9 feet above LWD in the closed position and an unlimited clearance in the open position. The current regulation in 33 CFR 117.627 requires the State Street (U.S. Route 23) Bridge, mile 0.92, across the Cheboygan River to open on signal from April 1 through May 15 and from September 16 through December 14. From May 16 through September 15 between the hours of 6 a.m. and 6 p.m. the draw opens on the quarter and three-quarter hours. From December 15 through March 31 the bridge operates with a 12-hour advance notice.

III. Discussion of Proposed Rule

Because the recreational vessel traffic going through the US 23 Highway Bridge, mile 0.92, across the Cheboygan River is controlled by the lock immediately upriver, there have been limited requests for bridge openings between 11 p.m. and 8 a.m., when the lock is closed. In accordance with the current bridge regulation in 33 CFR 117.627, the bridge opens twice an hour in sequence with the lock operations at

the top and bottom of the hour allowing vessels fifteen minutes to arrive at the bridge from the lock or to travel from the bridge to the lock.

There is one ferry serving the islands in the Straights of Mackinac and one passenger vessel that provides tour service to local wreck sites for divers. Most of the fall and spring requests for bridge openings are from these two boats. Both the ferry and the passenger vessel operate on a schedule and are predictable.

The ferry is the only means to deliver first responders to the islands and when operating under this condition is considered an emergency vessel as defined in 33 CFR 117.31.

We requested annual averaged daily vehicle crossing at the US 23 Highway Bridge, mile 0.92, across the Cheboygan River and discovered the bridge carries less than 8,000 vehicles each day and normally would not require limiting opening twice a day; however, after we examined the drawtender’s logs we found that if the bridge opened on signal, the monthly average openings would increase from an average of 152 openings a month to well over 380 openings a month.

We do not intend to change the two openings an hour concept, but we would change the hours of operations to better meet the needs of navigation and to make the rule easier to understand.

Cheboygan County requested to start the winter 12-hour advance notice requirement on November 1 to provide more snowplow drivers during winter squalls. We reviewed three years of drawtender logs and spoke to local stakeholders. We concluded that starting a 12-hour advance notice on November 1 would be impracticable because the bridge opens five to six times each day and November is deer season in Michigan, so the island residents have concerns with tourism to the island and the availability of emergency services to the island on the ferry vessel.

After reviewing three years of drawtender logs and speaking to local stakeholders, we concluded that the winter 12-hour advance notice could be extended to December 1 through April 30 providing the County with an additional 46 days of 12-hour advance notice.

From the drawtender logs we learned that there have been limited requests for

openings from 11 p.m. to 7 a.m., and we are proposing to place the bridge on a 2-hour advance during the evenings. No drawtender will be in attendance at the bridge and the County will provide a point of contact for the public to request bridge openings.

MDNR officers requested clearance gauges be installed at the bridge to prevent recreational vessels from hitting the bridge after a lock opening. When the locks open, they cause a temporary rise in water levels at the bridge reducing the vertical clearance at the bridge. We propose to require clearance gauges to be maintained on the upriver and down river sides of the bridge as required by 33 CFR 117.47.

Stakeholders also voiced concerns that bridge may delay ferries from delivering public utility repair teams to the island in the event of a storm, power loss, or fallen power lines. We propose to include this as part of the regulation.

In accordance with 33 CFR 117.55, the bridge owner shall keep in good repair signage that explains the bridge schedule and contact information when the bridge requires an advance notice. Annually the owner shall provide updated contact information to the District Commander to be included in the Local Notice to Mariners.

IV. Regulatory Analyses

We developed this proposed rule after considering numerous statutes and Executive Orders related to rulemaking. Below we summarize our analyses based on these statutes and Executive Orders.

A. Regulatory Planning and Review

Executive Orders 12866 and 13563 direct agencies to assess the costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits. This NPRM has not been designated a “significant regulatory action,” under Executive Order 12866. Accordingly, the NPRM has not been reviewed by the Office of Management and Budget (OMB).

This regulatory action determination is based on the ability that vessels can still transit the bridge given advanced notice.

B. Impact on Small Entities

The Regulatory Flexibility Act of 1980 (RFA), 5 U.S.C. 601–612, as amended, requires Federal agencies to consider the potential impact of regulations on small entities during rulemaking. The term “small entities” comprises small businesses, not-for-profit organizations that are independently owned and

operated and are not dominant in their fields, and governmental jurisdictions with populations of less than 50,000. The Coast Guard certifies under 5 U.S.C. 605(b) that this proposed rule would not have a significant economic impact on a substantial number of small entities.

While some owners or operators of vessels intending to transit the bridge may be small entities, for the reasons stated in section IV.A above this proposed rule would not have a significant economic impact on any vessel owner or operator.

If you think that your business, organization, or governmental jurisdiction qualifies as a small entity and that this proposed rule would have a significant economic impact on it, please submit a comment (see **ADDRESSES**) explaining why you think it qualifies and how and to what degree this proposed rule would economically affect it.

Under section 213(a) of the Small Business Regulatory Enforcement Fairness Act of 1996 (Pub. L. 104–121), we want to assist small entities in understanding this proposed rule. If the proposed rule would affect your small business, organization, or governmental jurisdiction and you have questions concerning its provisions or options for compliance, please contact the person listed in the **FOR FURTHER INFORMATION CONTACT** section. The Coast Guard will not retaliate against small entities that question or complain about this proposed rule or any policy or action of the Coast Guard.

C. Collection of Information

This proposed rule would call for no new collection of information under the Paperwork Reduction Act of 1995 (44 U.S.C. 3501–3520.).

D. Federalism and Indian Tribal Governments

A rule has implications for federalism under Executive Order 13132 (Federalism), if it has a substantial direct effect on the States, on the relationship between the National Government and the States, or on the distribution of power and responsibilities among the various levels of government. We have analyzed this proposed rule under that Order and have determined that it is consistent with the fundamental federalism principles and preemption requirements described in Executive Order 13132.

Also, this proposed rule does not have tribal implications under Executive Order 13175 (Consultation and Coordination with Indian Tribal Governments) because it would not have a substantial direct effect on one or

more Indian tribes, on the relationship between the Federal Government and Indian tribes, or on the distribution of power and responsibilities between the Federal Government and Indian tribes. If you believe this proposed rule has implications for federalism or Indian tribes, please contact the person listed in the **FOR FURTHER INFORMATION CONTACT** section.

E. Unfunded Mandates Reform Act

The Unfunded Mandates Reform Act of 1995 (2 U.S.C. 1531–1538) requires Federal agencies to assess the effects of their discretionary regulatory actions. In particular, the Act addresses actions that may result in the expenditure by a State, local, or tribal government, in the aggregate, or by the private sector of \$100,000,000 (adjusted for inflation) or more in any one year. Though this proposed rule will not result in such an expenditure, we do discuss the effects of this proposed rule elsewhere in this preamble.

F. Environment

We have analyzed this proposed rule under Department of Homeland Security Management Directive 023–01, Rev.1, associated implementing instructions, and Environmental Planning Policy COMDTINST 5090.1 (series), which guide the Coast Guard in complying with the National Environmental Policy Act of 1969 (NEPA) (42 U.S.C. 4321–4370f). The Coast Guard has determined that this action is one of a category of actions that do not individually or cumulatively have a significant effect on the human environment. This proposed rule promulgates the operating regulations or procedures for drawbridges. Normally such actions are categorically excluded from further review, under paragraph L49, of Chapter 3, Table 3–1 of the U.S. Coast Guard Environmental Planning Implementation Procedures.

Neither a Record of Environmental Consideration nor a Memorandum for the Record are required for this proposed rule. We seek any comments or information that may lead to the discovery of a significant environmental impact from this proposed rule.

V. Public Participation and Request for Comments

We view public participation as essential to effective rulemaking and will consider all comments and material received during the comment period. Your comment can help shape the outcome of this rulemaking. If you submit a comment, please include the docket number for this rulemaking, indicate the specific section of this

document to which each comment applies, and provide a reason for each suggestion or recommendation.

Submitting comments. We encourage you to submit comments through the Federal Decision-Making Portal at <https://www.regulations.gov>. To do so, go to <https://www.regulations.gov>, type USCG–2023–0113 in the search box and click “Search.” Next, look for this document in the Search Results column, and click on it. Then click on the Comment option. If your material cannot be submitted using <https://www.regulations.gov>, contact the person in the **FOR FURTHER INFORMATION CONTACT** section of this document for alternate instructions.

Viewing material in docket. To view documents mentioned in this proposed rule as being available in the docket, find the docket as described in the previous paragraph, and then select “Supporting & Related Material” in the Document Type column. Public comments will also be placed in our online docket and can be viewed by following instructions on the <https://www.regulations.gov> Frequently Asked Questions web page. We review all comments received, but we will only post comments that address the topic of the proposed rule. We may choose not to post off-topic, inappropriate, or duplicate comments that we receive. Additionally, if you go to the online docket and sign up for email alerts, you will be notified when comments are posted, or a final rule is published of any posting or updates to the docket.

We accept anonymous comments. Comments we post to <https://www.regulations.gov> will include any personal information you have provided. For more about privacy and submissions in response to this document, see DHS’s eRulemaking System of Records notice (85 FR 14226, March 11, 2020).

List of Subjects in 33 CFR Part 117

Bridges.

For the reasons discussed in the preamble, the Coast Guard proposes to amend 33 CFR part 117 as follows:

PART 117—DRAWBRIDGE OPERATION REGULATIONS

■ 1. The authority citation for part 117 continues to read as follows:

Authority: 33 U.S.C. 499; 33 CFR 1.05–1; DHS Delegation No. 0170.1, Revision No. 01.3.

■ 2. Revise § 117.627 to read as follows:

§ 117.627 Cheboygan River.

The draw of the US 23 highway bridge, mile 0.9 at Cheboygan shall operate as follows:

(a) From May 1 through November 31—

(1) Between the hours of 7 a.m. and 11 p.m. the draw need only open from three minutes before to three minutes after the quarter-hour and three-quarter hour.

(2) Between the hours of 11 p.m. and 7 a.m. no drawtender is required to be at the bridge and the bridge need not open unless a request to open the draw is given at least 2-hours in advance of a vessels intended time of passage through the draw.

(b) From December 1 through April 31, no drawtender is required to be at the bridge and the bridge need not open unless a request to open the draw is given at least 12-hours in advance of a vessels intended time of passage through the draw.

(c) At all times the draw shall open as soon as possible for the passage of vessels if carrying public safety or public utility vehicles and persons to or from the island.

(d) The owner of the bridge shall provide and keep in good legible condition two board gauges painted white with black figures not less than six inches high to indicate the vertical clearance under the closed draw at all water levels. The gages shall be placed on the bridge so that they are plainly visible to operators of vessels approaching the bridge either up or downstream.

M.J. Johnston,

Rear Admiral, U.S. Coast Guard, Commander, Ninth Coast Guard District.

[FR Doc. 2023–06925 Filed 4–4–23; 8:45 am]

BILLING CODE 9110–04–P

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

33 CFR Part 165

[Docket Number USCG–2023–0192]

RIN 1625–AA00

Safety Zone; Delaware Bay, Lower Township, NJ

AGENCY: Coast Guard, DHS.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Coast Guard is proposing to establish a temporary safety zone for certain navigable waters of the Delaware Bay, in Lower Township, NJ. The safety zone is needed to protect personnel,

vessels, and the marine environment from potential hazards created by a fireworks display. Entry of vessels or persons into this zone is prohibited unless specifically authorized by the Captain of the Port (COTP), Sector Delaware Bay. We invite your comments on this proposed rulemaking.

DATES: Comments and related material must be received by the Coast Guard on or before May 5, 2023.

ADDRESSES: You may submit comments identified by docket number USCG–2023–0192 using the Federal Decision-Making Portal at <https://www.regulations.gov>. See the “Public Participation and Request for Comments” portion of the **SUPPLEMENTARY INFORMATION** section for further instructions on submitting comments.

FOR FURTHER INFORMATION CONTACT: If you have questions on this rule, call or email Petty Officer Dylan Caikowski, Sector Delaware Bay, Waterways Management Division, U.S. Coast Guard; telephone (215) 271–4814, email SecDelBayWWM@uscg.mil.

SUPPLEMENTARY INFORMATION:

I. Table of Abbreviations

CFR Code of Federal Regulations
DHS Department of Homeland Security
FR Federal Register
NPRM Notice of proposed rulemaking
§ Section
U.S.C. United States Code

II. Background, Purpose, and Legal Basis

On February 18, 2023, Lower Township, New Jersey notified the Coast Guard that it will be conducting a fireworks display from 9:30 to 9:50 p.m. on July 3, 2023, or a rain date of July 5, 2023, to celebrate Independence Day. The fireworks are to be launched from a barge in the Delaware Bay approximately 350 yards west of North Cape May Beach, in Lower Township, NJ. Hazards from fireworks displays include accidental discharge of fireworks, dangerous projectiles, and falling hot embers or other debris. The COTP has determined that potential hazards associated with the fireworks to be used in this display would be a safety concern for anyone within a 300-yard radius of the barge.

The purpose of this rulemaking is to ensure the safety of vessels and the navigable waters within a 300-yard radius of the fireworks barge before, during, and after the scheduled event. The Coast Guard is proposing this rulemaking under authority in 46 U.S.C. 70034.

III. Discussion of Proposed Rule

The COTP is proposing to establish a safety zone from 9:15 to 10 p.m. on July 3, 2023, or a rain date of July 5, 2023. The safety zone would cover all navigable waters within 300 yards of a barge in the Delaware Bay located at approximate position latitude 38°59'7.08" N, longitude 074°57'49.47" W. The duration of the zone is intended to ensure the safety of vessels and these navigable waters before, during, and after the scheduled 9:30 to 9:50 p.m. fireworks display. No vessel or person would be permitted to enter the safety zone without obtaining permission from the COTP or a designated representative. The regulatory text we are proposing appears at the end of this document.

IV. Regulatory Analyses

We developed this proposed rule after considering numerous statutes and Executive orders related to rulemaking. Below we summarize our analyses based on a number of these statutes and Executive orders, and we discuss First Amendment rights of protestors.

A. Regulatory Planning and Review

Executive Orders 12866 and 13563 direct agencies to assess the costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits. This NPRM has not been designated a "significant regulatory action," under Executive Order 12866. Accordingly, the NPRM has not been reviewed by the Office of Management and Budget (OMB).

This regulatory action determination is based on the following factors: (1) although persons and vessels may not enter, transit through, anchor in, or remain within the safety zone without authorization from the COTP Delaware Bay or a designated representative, they may operate in the surrounding area during the enforcement period; (2) persons and vessels will still be able to enter, transit through, anchor in, or remain within the regulated area if authorized by the COTP Delaware Bay; and (3) the Coast Guard will provide advance notification of the safety zone to the local maritime community by Local Notice to Mariners and Broadcast Notice to Mariners.

B. Impact on Small Entities

The Regulatory Flexibility Act of 1980, 5 U.S.C. 601–612, as amended, requires Federal agencies to consider the potential impact of regulations on small entities during rulemaking. The term "small entities" comprises small

businesses, not-for-profit organizations that are independently owned and operated and are not dominant in their fields, and governmental jurisdictions with populations of less than 50,000. The Coast Guard certifies under 5 U.S.C. 605(b) that this proposed rule would not have a significant economic impact on a substantial number of small entities.

While some owners or operators of vessels intending to transit the safety zone may be small entities, for the reasons stated in section IV.A above, this proposed rule would not have a significant economic impact on any vessel owner or operator.

If you think that your business, organization, or governmental jurisdiction qualifies as a small entity and that this proposed rule would have a significant economic impact on it, please submit a comment (see **ADDRESSES**) explaining why you think it qualifies and how and to what degree this rule would economically affect it.

Under section 213(a) of the Small Business Regulatory Enforcement Fairness Act of 1996 (Pub. L. 104–121), we want to assist small entities in understanding this proposed rule. If the proposed rule would affect your small business, organization, or governmental jurisdiction and you have questions concerning its provisions or options for compliance, please call or email the person listed in the **FOR FURTHER INFORMATION CONTACT** section. The Coast Guard will not retaliate against small entities that question or complain about this proposed rule or any policy or action of the Coast Guard.

C. Collection of Information

This proposed rule would not call for a new collection of information under the Paperwork Reduction Act of 1995 (44 U.S.C. 3501–3520).

D. Federalism and Indian Tribal Governments

A rule has implications for federalism under Executive Order 13132 (Federalism), if it has a substantial direct effect on the States, on the relationship between the National Government and the States, or on the distribution of power and responsibilities among the various levels of government. We have analyzed this proposed rule under that Order and have determined that it is consistent with the fundamental federalism principles and preemption requirements described in Executive Order 13132.

Also, this proposed rule does not have tribal implications under Executive Order 13175 (Consultation and Coordination with Indian Tribal Governments) because it would not

have a substantial direct effect on one or more Indian tribes, on the relationship between the Federal Government and Indian tribes, or on the distribution of power and responsibilities between the Federal Government and Indian tribes. If you believe this proposed rule has implications for federalism or Indian tribes, please call or email the person listed in the **FOR FURTHER INFORMATION CONTACT** section.

E. Unfunded Mandates Reform Act

The Unfunded Mandates Reform Act of 1995 (2 U.S.C. 1531–1538) requires Federal agencies to assess the effects of their discretionary regulatory actions. In particular, the Act addresses actions that may result in the expenditure by a State, local, or tribal government, in the aggregate, or by the private sector of \$100,000,000 (adjusted for inflation) or more in any one year. Though this proposed rule would not result in such an expenditure, we do discuss the potential effects of this proposed rule elsewhere in this preamble.

F. Environment

We have analyzed this proposed rule under Department of Homeland Security Directive 023–01, Rev. 1, associated implementing instructions, and Environmental Planning COMDTINST 5090.1 (series), which guide the Coast Guard in complying with the National Environmental Policy Act of 1969 (42 U.S.C. 4321–4370f), and have made a preliminary determination that this action is one of a category of actions that do not individually or cumulatively have a significant effect on the human environment. This proposed rule involves a safety zone lasting 45 minutes that would prohibit entry within 300 yards of a fireworks barge. Normally, such actions are categorically excluded from further review under paragraph L60(a) of Appendix A, Table 1 of DHS Instruction Manual 023–01–001–01, Rev. 1. A preliminary Record of Environmental Consideration supporting this determination is available in the docket. For instructions on locating the docket, see the **ADDRESSES** section of this preamble. We seek any comments or information that may lead to the discovery of a significant environmental impact from this proposed rule.

G. Protest Activities

The Coast Guard respects the First Amendment rights of protesters. Protesters are asked to call or email the person listed in the **FOR FURTHER INFORMATION CONTACT** section to coordinate protest activities so that your message can be received without

jeopardizing the safety or security of people, places, or vessels.

V. Public Participation and Request for Comments

We view public participation as essential to effective rulemaking and will consider all comments and material received during the comment period. Your comment can help shape the outcome of this rulemaking. If you submit a comment, please include the docket number for this rulemaking, indicate the specific section of this document to which each comment applies, and provide a reason for each suggestion or recommendation.

Submitting comments. We encourage you to submit comments through the Federal Decision-Making Portal at <https://www.regulations.gov>. To do so, go to <https://www.regulations.gov>, type USCG–2023–0192 in the search box and click “Search.” Next, look for this document in the Search Results column, and click on it. Then click on the Comment option. If you cannot submit your material by using <https://www.regulations.gov>, call or email the person in the **FOR FURTHER INFORMATION CONTACT** section of this proposed rule for alternate instructions.

Viewing material in the docket. To view documents mentioned in this proposed rule as being available in the docket, find the docket as described in the previous paragraph, and then select “Supporting & Related Material” in the Document Type column. Public comments will also be placed in our online docket and can be viewed by following instructions on the <https://www.regulations.gov> Frequently Asked Questions web page. Also, if you click on the Dockets tab and then the proposed rule, you should see a “Subscribe” option for email alerts. The option will notify you when comments are posted, or a final rule is published.

We review all comments received, but we will only post comments that address the topic of the proposed rule. We may choose not to post off-topic, inappropriate, or duplicate comments that we receive.

Personal information. We accept anonymous comments. Comments we post to <https://www.regulations.gov> will include any personal information you have provided. For more about privacy and submissions to the docket in response to this document, see DHS’s eRulemaking System of Records notice (85 FR 14226, March 11, 2020).

List of Subjects in 33 CFR Part 165

Harbors, Marine safety, Navigation (water), Reporting and recordkeeping

requirements, Security measures, Waterways.

For the reasons discussed in the preamble, the Coast Guard is proposing to amend 33 CFR part 165 as follows:

PART 165—REGULATED NAVIGATION AREAS AND LIMITED ACCESS AREAS

■ 1. The authority citation for part 165 continues to read as follows:

Authority: 46 U.S.C. 70034, 70051, 70124; 33 CFR 1.05–1, 6.04–1, 6.04–6, and 160.5; Department of Homeland Security Delegation No. 00170.1, Revision No. 01.3.

■ 2. Add § 165.T05–0192 to read as follows:

§ 165.T05–0192 Safety Zone; Delaware Bay, Lower Township, NJ.

(a) *Location.* All navigable waters within 300 yards of a barge in the Delaware Bay located at approximate position latitude 38°59′7.08″ N, longitude 074°57′49.47″ W.

(b) *Definitions.* As used in this section, “designated representative” means a Coast Guard Patrol Commander, including a Coast Guard petty officer, warrant or commissioned officer on board a Coast Guard vessel or on board a federal, state, or local law enforcement vessel assisting the Captain of the Port (COTP), Sector Delaware Bay in the enforcement of the safety zone.

(c) *Regulations.*

(1) Under the general safety zone regulations in subpart C of this part, you may not enter the safety zone described in paragraph (a) of this section unless authorized by the COTP or the COTP’s designated representative.

(2) To seek permission to enter or remain in the zone, contact the COTP or the COTP’s representative via VHF–FM channel 16 or 215–271–4807. Those in the safety zone must comply with all lawful orders or directions given to them by the COTP or the COTP’s designated representative.

(3) No vessel may take on bunkers or conduct lightering operations within the safety zone during its enforcement period.

(4) This section applies to all vessels except those engaged in law enforcement, aids to navigation servicing, and emergency response operations.

(d) *Enforcement.* The U.S. Coast Guard may be assisted in the patrol and enforcement of the safety zone by Federal, State, and local agencies.

(e) *Enforcement period.* This zone will be enforced from approximately 9:15 to 10 p.m. on July 3, 2023, or a rain date of July 5, 2023.

Dated: March 30, 2023.

Jonathan D. Theel,

Captain, U.S. Coast Guard, Captain of the Port, Sector Delaware Bay.

[FR Doc. 2023–07054 Filed 4–4–23; 8:45 am]

BILLING CODE 9110–04–P

ENVIRONMENTAL PROTECTION AGENCY

40 CFR Part 52

[EPA–R09–OAR–2023–0036; FRL–10790–01–R9]

Air Plan Revisions; California; Sacramento Metropolitan Air Quality Management District

AGENCY: Environmental Protection Agency (EPA).

ACTION: Proposed rule.

SUMMARY: The Environmental Protection Agency (EPA) is proposing to partially approve and partially disapprove a revision to the Sacramento Metropolitan Air Quality Management District (SMAQMD) portion of the California State Implementation Plan (SIP) concerning the SMAQMD’s demonstration regarding reasonably available control technology (RACT) requirements and negative declarations for the 2008 8-hour ozone National Ambient Air Quality Standards (NAAQS or “standards”) in the portion of the Sacramento Metropolitan nonattainment area under the jurisdiction of the SMAQMD. We are proposing action on a SIP revision under the Clean Air Act (CAA or the Act). We are taking comments on this proposal and plan to follow with a final action.

DATES: Comments must be received on or before May 5, 2023.

ADDRESSES: Submit your comments, identified by Docket ID No. EPA–R09–OAR–2023–0036 at <https://www.regulations.gov>. For comments submitted at [Regulations.gov](https://www.regulations.gov), follow the online instructions for submitting comments. Once submitted, comments cannot be edited or removed from [Regulations.gov](https://www.regulations.gov). The EPA may publish any comment received to its public docket. Do not submit electronically any information you consider to be Confidential Business Information (CBI) or other information whose disclosure is restricted by statute. Multimedia submissions (audio, video, etc.) must be accompanied by a written comment. The written comment is considered the official comment and should include discussion of all points you wish to make. The EPA will generally not

consider comments or comment contents located outside of the primary submission (*i.e.*, on the web, cloud, or other file sharing system). For additional submission methods, please contact the person identified in the **FOR FURTHER INFORMATION CONTACT** section. For the full EPA public comment policy, information about CBI or multimedia submissions, and general guidance on making effective comments, please visit <https://www.epa.gov/dockets/commenting-epa-dockets>. If you need assistance in a language other than English or if you are a person with disabilities who needs a reasonable accommodation at no cost to you, please

contact the person identified in the **FOR FURTHER INFORMATION CONTACT** section.
FOR FURTHER INFORMATION CONTACT:
Eugene Chen, EPA Region IX, 75 Hawthorne St., San Francisco, CA 94105. By phone: (415) 947-4304 or by email at chen.eugene@epa.gov.

SUPPLEMENTARY INFORMATION:
Throughout this document, “we,” “us” and “our” refer to the EPA.

Table of Contents

- I. The State’s Submittal
 - A. What documents did the State submit?
 - B. Are there other versions of these documents?
 - C. What is the purpose of the submitted documents?

- II. The EPA’s Evaluation and Action
 - A. How is the EPA evaluating the submitted documents?
 - B. Do the documents meet the evaluation criteria?
 - C. What are the deficiencies?
 - D. Proposed Action and Public Comment
- III. Statutory and Executive Order Reviews

I. The State’s Submittal

A. What documents did the State submit?

Table 1 lists the documents addressed by this proposal with the dates that they were adopted by the local air agency and submitted by the California Air Resource Board (CARB).

TABLE 1—SUBMITTED DOCUMENTS

Local agency	Document	Adopted	Submitted
SMAQMD	Demonstration of Reasonably Available Control Technology for the 2008 Ozone National Ambient Air Quality Standard (NAAQS) (“2017 RACT SIP”).	03/23/2017	05/05/2017
SMAQMD	Negative Declaration for Control Technique Guidelines for Miscellaneous Metal and Plastic Parts Coatings (Pleasure Craft Coating Portion Only) (“Pleasure Craft Coating Negative Declaration”).	03/22/2018	06/11/2018

The submittals for the 2017 RACT SIP and Pleasure Craft Coating Negative Declaration were determined to meet the completeness criteria in 40 CFR part 51, Appendix V, in letters dated October 31, 2017 and August 23, 2018, respectively.

B. Are there other versions of these documents?

There are no previous versions of the RACT SIP or negative declarations in the SMAQMD portion of the California SIP for the 2008 ozone NAAQS.

C. What is the purpose of the submitted documents?

Emissions of volatile organic compounds (VOCs) and oxides of nitrogen (NO_x) contribute to the production of ground-level ozone, smog and particulate matter (PM), which harm human health and the environment. Section 110(a) of the CAA requires states to submit regulations that control VOC and NO_x emissions. Sections 182(b)(2) and (f) require that SIPs for ozone nonattainment areas classified as Moderate or above implement RACT for any source covered by a Control Techniques Guidelines (CTG) document and for any major source of VOCs or NO_x. The SMAQMD is subject to this requirement as it regulates the Sacramento County portion of the Sacramento Metropolitan ozone nonattainment area that was designated and classified as a Severe nonattainment area for the 2008 8-hour

ozone NAAQS.¹ Therefore, the SMAQMD must, at a minimum, adopt RACT-level controls for all sources covered by a CTG document and for all major non-CTG sources of VOCs or NO_x within the ozone nonattainment area that it regulates. Any stationary source that emits or has the potential to emit at least 25 tons per year (tpy) of VOCs or NO_x is a major stationary source in a Severe ozone nonattainment area (CAA section 182(d), (f) and 302(j)).

Section III.D of the preamble to the EPA’s final rule to implement the 2008 ozone NAAQS discusses RACT requirements.² It states, in part, that RACT SIPs must contain adopted RACT regulations, certifications (where appropriate) that existing provisions are RACT, and/or negative declarations that no sources in the nonattainment area are covered by a specific CTG.³ It also provides that states must submit appropriate supporting information for their RACT submissions as described in the EPA’s implementation rule for the 1997 ozone NAAQS.⁴ The SMAQMD’s RACT SIP submittal and negative declarations provide SMAQMD’s analyses of its compliance with the CAA section 182 RACT requirements for the 2008 8-hour ozone NAAQS.

The EPA’s technical support document (TSD) has more information about SMAQMD’s RACT SIP, negative

declarations, and the EPA’s evaluations thereof.

II. The EPA’s Evaluation and Action

A. How is the EPA evaluating the submitted documents?

Generally, SIP rules must require RACT for each category of sources covered by a CTG document as well as each major source of VOCs or NO_x in ozone nonattainment areas classified as Moderate or above (see CAA section 182(b)(2), (f)). The SMAQMD regulates the Sacramento County portion of the Sacramento Metropolitan ozone nonattainment area classified as Severe for the 2008 ozone standard (40 CFR 81.305). Therefore, SMAQMD rules must implement RACT.

States should also submit for SIP approval negative declarations for those CTGs for which they have no sources covered by the CTG, regardless of whether such negative declarations were made in a SIP for an earlier ozone standard.⁵ To do so, the submittal should provide reasonable assurance that no sources that fall under the CTG currently exist in the portion of the ozone nonattainment area that is regulated by the SMAQMD.

The District’s analysis must demonstrate that each major source of VOCs or NO_x in the ozone nonattainment area is covered by a RACT-level rule. In addition, for each CTG, the District must either

¹ 77 FR 30088 (May 21, 2012).

² 80 FR 12264 (March 6, 2015).

³ *Id.* at 12278.

⁴ *Id.*; 70 FR 71612, 71652 (November 29, 2005).

⁵ 57 FR 13498, 13512 (April 16, 1992).

demonstrate that a RACT-level rule is in place or submit a negative declaration. Guidance and policy documents that we use to evaluate CAA section 182 RACT requirements include the following:

1. "State Implementation Plans; General Preamble for the Implementation of Title I of the Clean Air Act Amendments of 1990," 57 FR 13498 (April 16, 1992); 57 FR 18070 (April 28, 1992).
2. "Issues Relating to VOC Regulation Cutpoints, Deficiencies, and Deviations," EPA, May 25, 1988 (the Bluebook, revised January 11, 1990).
3. "Guidance Document for Correcting Common VOC & Other Rule Deficiencies," EPA Region 9, August 21, 2001 (the Little Bluebook).
4. "State Implementation Plans; Nitrogen Oxides Supplement to the General Preamble; Clean Air Act Amendments of 1990 Implementation of Title I; Proposed Rule," (the NO_x Supplement), 57 FR 55620, November 25, 1992.
5. Memorandum dated May 18, 2006, from William T. Harnett, Director, Air Quality Policy Division, to Regional Air Division Directors, Subject: "RACT Qs & As—Reasonably Available Control Technology (RACT): Questions and Answers."
6. "Final Rule to Implement the 8-hour Ozone National Ambient Air Quality Standard—Phase 2," 70 FR 71612 (November 29, 2005).
7. "Implementation of the 2008 National Ambient Air Quality Standards for Ozone: State Implementation Plan Requirements," 80 FR 12264 (March 6, 2015).
8. "State Implementation Plans: Response to Petition for Rulemaking; Restatement and Update of EPA's SSM (startup, shutdown, malfunction) Policy

Applicable to SIPs; Findings of Substantial Inadequacy; and SIP Calls to Amend Provisions Applying to Excess Emissions During Periods of Startup, Shutdown and Malfunction" (80 FR 33839) June 12, 2015 (2015 SSM SIP Action).

9. "Inclusion of Provisions Governing Periods of Startup, Shutdown, and Malfunctions in State Implementation Plans," EPA, October 9, 2020.
10. "Withdrawal of the October 9, 2020, Memorandum Addressing Startup, Shutdown, and Malfunctions in State Implementation Plans and Implementation of the Prior Policy," EPA, September 30, 2021.

B. Do the documents meet the evaluation criteria?

SMAQMD's 2017 RACT SIP provides the District's demonstration that the applicable SIP for the SMAQMD satisfies CAA section 182 RACT requirements for the 2008 8-hour ozone NAAQS. The District based its demonstration on its analysis of SIP-approved requirements that apply to the following: (1) sources covered by a CTG, and (2) major non-CTG stationary sources of VOC or NO_x emissions.

With respect to CTG sources, SMAQMD identified several CTGs with covered sources (*i.e.*, sources covered by the CTG and operating within the nonattainment area), and provided an evaluation of the District rules it relies upon to meet RACT for these CTGs. We reviewed the District's evaluation and agree that its rules implement RACT for the applicable CTGs. Our TSD has additional information about our evaluation of these rules.

When there are no existing sources covered by a particular CTG document, or no major non-CTG sources of NO_x or

VOC, states may, in lieu of adopting RACT requirements for those sources, adopt negative declarations certifying that there are no such sources in the relevant nonattainment area. Appendix A of the 2017 RACT SIP lists SMAQMD's negative declarations for those instances where it has no sources subject to the applicable CTGs for the 2008 8-hour ozone NAAQS. These negative declarations are listed in Table 2 below. SMAQMD concludes that it has no sources subject to these listed CTGs based on a review of its permit files, emission inventory, business listings, and consultation with District permitting and enforcement staff. We reviewed SMAQMD's list of negative declarations and California Emissions Inventory data to verify the District's conclusion that it has no stationary sources subject to the CTGs for which it has adopted a negative declaration. We agree with the District's negative declarations in the 2017 RACT SIP and propose to approve them into the SIP.

With respect to non-CTG major sources of NO_x or VOC, SMAQMD identified twelve major sources exceeding the major source threshold for NO_x or VOC, which is 25 tpy in Severe ozone nonattainment areas. As described in more detail in our TSD, we conclude that SMAQMD properly identified all major non-CTG sources of NO_x or VOC requiring RACT. SMAQMD also identified several District rules, primarily NO_x rules, that it relies upon to implement RACT at these major sources. As discussed in more detail in Section C below, we have noted certain deficiencies in several of the identified District rules, and conclude that these District rules do not fully satisfy the RACT requirement.

TABLE 2—SMAQMD NEGATIVE DECLARATIONS

CTG document No.	CTG document title
EPA-450/2-77-008	Control of Volatile Organic Emissions from Existing Stationary Sources—Volume II: Surface Coating of Coils.
EPA-450/2-77-008	Control of Volatile Organic Emissions from Existing Stationary Sources—Volume II: Surface Coating of Paper.
EPA-450/2-77-008	Control of Volatile Organic Emissions from Existing Stationary Sources—Volume II: Surface Coating of Fabrics.
EPA-450/2-77-008	Control of Volatile Organic Emissions from Existing Stationary Sources—Volume II: Surface Coating of Automobiles and Light-Duty Trucks.
EPA-450/2-77-025	Control of Refinery Vacuum Producing Systems, Wastewater Separators, and Process Unit Turnarounds.
EPA-450/2-77-033	Control of Volatile Organic Emissions from Existing Stationary Sources—Volume IV: Surface Coating of Insulation of Magnet Wire.
EPA-450/2-77-034	Control of Volatile Organic Emissions from Existing Stationary Sources—Volume V: Surface Coating of Large Appliances.
EPA-450/2-78-030	Manufacture of Pneumatic Rubber Tires.
EPA-450/2-78-032	Factory Surface Coating of Flat Wood Paneling.
EPA-450/2-78-033	Graphic Arts-Rotogravure and Flexography (Rotogravure only).
EPA-450/2-78-03	Leaks from Petroleum Refinery Equipment.
EPA-450/3-82-009	Large Petroleum Dry Cleaners.
EPA-450/3-83-007	Leaks from Natural Gas/Gasoline Processing Plants.
EPA-450/3-83-008	Manufacture of High-Density Polyethylene, Polypropylene, and Polystyrene Resins.
EPA-450/3-84-015	Air Oxidation Processes in Synthetic Organic Chemical Manufacturing Industry.
EPA-453/R-94-032, 61 FR 44050; 8/27/96.	ACT Surface Coating at Shipbuilding and Ship Repair Facilities Shipbuilding and Ship Repair Operations (Surface Coating).

TABLE 2—SMAQMD NEGATIVE DECLARATIONS—Continued

CTG document No.	CTG document title
EPA-453/R-97-004, 59 FR 29216; 6/06/94.	Aerospace MACT and Aerospace (CTG & MACT).
EPA-453/R-06-004	Flat Wood Paneling Coatings.
EPA 453/R-07-003	Paper, Film, and Foil Coatings.
EPA 453/R-07-004	Large Appliance Coatings.
EPA 453/R-08-003	Miscellaneous Metal and Plastic Parts Coatings (Table 5—Pleasure Craft Surface Coating).
EPA 453/R-08-004	Fiberglass Boat Manufacturing Materials.
EPA 453/R-08-005	Miscellaneous Industrial Adhesives.
EPA 453/R-08-006	Automobile and Light-Duty Truck Assembly Coatings.

C. What are the deficiencies?

EPA's startup, shutdown and malfunction (SSM) policy, as defined in the 2015 SSM SIP Action,⁶ notes that CAA § 110(a)(2)(A) requires SIPs to include enforceable emission limitations and other control measures, means, or techniques as necessary to meet CAA requirements. The term "emission limitation" is defined in CAA § 302(k) as a requirement that "limits the quantity, rate, or concentration of emissions of air pollution on a continuous basis [. . .]." An emission limitation or requirement that exempts a period of source operation, such as startup, cannot be considered continuous and is not consistent with CAA requirements (absent an alternative emission limitation that applies during such periods). Since such rule limits cannot be considered continuous limits given the presence of an exemption for periods of startup and shutdown, they do not implement RACT during all operating conditions, despite the level of stringency they may establish outside of startup and shutdown periods. Moreover, section 110(a)(2) of the CAA requires SIP submissions to include enforceable emission limitations and other control measures, means, or techniques as may be necessary or appropriate to meet the applicable requirements of the Act. If a rule provides for an emission limitation during startup and shutdown, but that limitation is not enforceable, a state may not rely on this limit to establish RACT during startup and shutdown. Furthermore, if a rule establishes a limit during startup and shutdown, but expressly forbids the use of data generated during these times from use in establishing whether a violation occurred during these times, this

restriction is not consistent with the Credible Evidence Rule.⁷

As discussed in more detail in our TSD, several of the District rules relied upon to implement RACT for non-CTG major sources of NO_x contain provisions that are not consistent with EPA's SSM Policy. Rule 413 (Stationary Gas Turbines) contains a provision that explicitly exempts affected units from complying with rule standards during periods of startup and shutdown and does not provide for an alternative emissions limitation during such periods. Rule 411 (NO_x from Boilers, Process Heaters, and Steam Generators) and Rule 419 (NO_x from Miscellaneous Combustion Units) both contain monitoring provisions that preclude the use of specified data for compliance determinations during periods of startup and shutdown. The deficiencies in these three rules represent the basis for our partial disapproval of SMAQMD's 2017 RACT SIP for non-CTG major sources of NO_x, and must be remedied prior to full approval of the District's RACT SIP.

D. Proposed Action and Public Comment

For the reasons discussed above and explained in more detail in our TSD, the EPA proposes to partially approve and partially disapprove the SMAQMD 2017 RACT SIP. As authorized in section 110(k)(3) of the Act, we are proposing to approve the SMAQMD 2017 RACT SIP for each of the CTGs addressed either by District rule or by negative declaration, as well as for non-CTG major sources of VOC. Also under section 110(k)(3), we propose to disapprove the SMAQMD 2017 RACT SIP as it pertains to non-CTG major sources of NO_x, based upon our conclusion that several of the District rules relied upon to implement RACT for this element contain deficiencies related to startup and

shutdown. Table 3 contains a listing of each RACT element, the District rule or negative declaration relied upon to address RACT, as well as our proposed action for that RACT element.

The EPA is committed to working with SMAQMD to resolve the identified RACT deficiencies. However, should we finalize the proposed partial disapproval of the non-CTG major source NO_x element of SMAQMD's 2017 RACT SIP, section 110(c) would require the EPA to promulgate a federal implementation plan (FIP) within 24 months unless we approve subsequent SIP revisions that correct the deficiencies identified in our final action. In this instance, we note that the EPA already has an existing obligation to promulgate a FIP for any RACT SIP elements that we have not taken final action to approve. This FIP obligation originates from our February 3, 2017 (82 FR 9158) finding that SMAQMD failed to submit a RACT SIP for the 2008 8-hour ozone NAAQS by the required submittal deadline. This finding of failure to submit established a FIP obligation deadline of February 3, 2019. In addition, final action on the proposed partial disapproval would trigger the offset sanction in CAA section 179(b)(2) 18 months after the effective date of a final disapproval, and the highway funding sanction in CAA section 179(b)(1) six months after the offset sanction is imposed. A sanction will not be imposed if the EPA determines that a subsequent SIP submission corrects the deficiencies identified in our final action before the applicable deadline.⁸

We will accept comments from the public on this proposed partial approval and partial disapproval until May 5, 2023. If finalized, this action would incorporate the approved portions of the 2017 RACT SIP and negative declarations into the SIP.

⁶ 80 FR 33839 (June 12, 2015).

⁷ 62 FR 8314, February 24, 1997; 40 CFR 51.212. The Credible Evidence Rule provides that a SIP may not preclude the use of any credible evidence or information relevant to whether a source would

have been in compliance with applicable requirements if the appropriate performance or compliance test procedure had been performed.

⁸ Our February 7, 2017 finding of failure to submit also triggered offset sanctions and highway

funding sanctions. These sanctions clocks were extinguished by SMAQMD's submittal of its 2017 RACT SIP and our October 31, 2017 and August 23, 2018 letters determining that the District's RACT SIP submittal was complete.

TABLE 3—LIST OF RACT ELEMENTS—2008 OZONE NAAQS

CTG document No.	RACT element	District rule implementing RACT	Negative declaration submitted	EPA proposed action
EPA-450/R-75-102	Design Criteria for Stage I Vapor Control—Gasoline Service Stations.	448 (Gasoline Transfer Into Stationary Storage Containers).		Approval.
EPA-450/2-77-008	Surface Coating of Cans	452 (Can Coating)		Approval.
EPA-450/2-77-008	Surface Coating of Coils		Yes	Approval.
EPA-450/2-77-008	Surface Coating of Paper		Yes	Approval.
EPA-450/2-77-008	Surface Coating of Fabric		Yes	Approval.
EPA-450/2-77-008	Surface Coating of Automobiles and Light-Duty Trucks.		Yes	Approval.
EPA-450/2-77-022	Solvent Metal Cleaning	454 (Degreasing Operations)		Approval.
EPA-450/2-77-025	Refinery Vacuum Producing Systems, Wastewater Separators, and Process Unit Turnarounds.		Yes	Approval.
EPA-450/2-77-026	Tank Truck Gasoline Loading Terminals	447 (Organic Liquid Loading)		Approval.
EPA-450/2-77-032	Surface Coating of Metal Furniture	451 (Surface Coating of Miscellaneous Metal Parts and Products).		Approval.
EPA-450/2-77-033	Surface Coating of Insulation of Magnet Wire.		Yes	Approval.
EPA-450/2-77-034	Surface Coating of Large Appliances		Yes	Approval.
EPA-450/2-77-035	Bulk Gasoline Plants	447 (Organic Liquid Loading)		Approval.
EPA-450/2-77-036	Storage of Petroleum Liquids in Fixed-Roof Tanks.	446 (Storage of Petroleum Products)		Approval.
EPA-450/2-77-037	Cutback Asphalt	453 (Cutback and Emulsified Asphalt Paving Materials).		Approval.
EPA-450/2-78-015	Surface Coating of Miscellaneous Metal Parts and Products.	451 (Surface Coating of Miscellaneous Metal Parts and Products).		Approval.
EPA-450/2-78-029	Manufacture of Synthesized Pharmaceutical Products.	464 (Organic Chemical Manufacturing Operations).		Approval.
EPA-450/2-78-030	Manufacture of Pneumatic Rubber Tires		Yes	Approval.
EPA-450/2-78-032	Factory Surface Coating of Flat Wood Paneling.		Yes	Approval.
EPA-450/2-78-033	Graphic Arts-Rotogravure and Flexography	450 (Graphic Arts Operations)—Flexography only.	Yes—Rotogravure only.	Approval.
EPA-450/2-78-036	Leaks from Petroleum Refinery Equipment		Yes	Approval.
EPA-450/2-78-047	Petroleum Liquid Storage in External Floating Roof Tanks.	446 (Storage of Petroleum Products)		Approval.
EPA-450/2-78-051	Leaks from Gasoline Tank Trucks and Vapor Collection Systems.	447 (Organic Liquid Loading), 448 (Gasoline Transfer Into Stationary Storage Containers).		Approval.
EPA-450/3-82-009	Large Petroleum Dry Cleaners		Yes	Approval.
EPA-450/3-83-006	Leaks from Synthetic Organic Chemical Polymer and Resin Manufacturing Equipment.	443 (Leaks from Synthetic Organic Chemical and Polymer Manufacturing).		Approval.
EPA-450/3-83-007	Leaks from Natural Gas/Gasoline Processing Plants.		Yes	Approval.
EPA-450/3-83-008	Manufacture of High-Density Polyethylene, Polypropylene, and Polystyrene Resins.		Yes	Approval.
EPA-450/3-84-015	Air Oxidation Processes in Synthetic Organic Chemical Manufacturing Industry.		Yes	Approval.
EPA-450/4-91-031	Reactor Processes and Distillation Operations in Synthetic Organic Chemical Manufacturing Industry.	464 (Organic Chemical Manufacturing Operations).		Approval.
EPA-453/R-96-007	Wood Furniture Manufacturing Operations		Yes	Approval.
EPA-453/R-94-032, 61 FR 44050; 8/27/96.	ACT Surface Coating at Shipbuilding and Ship Repair Facilities Shipbuilding and Ship Repair Operations (Surface Coating).		Yes	Approval.
EPA-453/R-97-004, 59 FR 29216; 6/06/94.	Aerospace MACT and Aerospace (CTG & MACT).		Yes	Approval.
EPA-453/R-06-001	Industrial Cleaning Solvents	466 (Solvent Cleaning)		Approval.
EPA-453/R-06-002	Offset Lithographic Printing and Letterpress Printing.	450 (Graphic Arts Operations)		Approval.
EPA-453/R-06-003	Flexible Package Printing	450 (Graphic Arts Operations)		Approval.
EPA-453/R-06-004	Flat Wood Paneling Coatings		Yes	Approval.
EPA 453/R-07-003	Paper, Film, and Foil Coatings		Yes	Approval.
EPA 453/R-07-004	Large Appliance Coatings		Yes	Approval.
EPA 453/R-07-005	Metal Furniture Coatings	451 (Surface Coating of Miscellaneous Metal Parts and Products).		Approval.
EPA 453/R-08-003	Miscellaneous Metal Parts Coatings: Table 2—Metal Parts and Products.	451 (Surface Coating of Miscellaneous Metal Parts and Products).		Approval.
EPA 453/R-08-003	Miscellaneous Plastic Parts Coatings: Table 3—Plastic Parts and Products.	468 (Surface Coating of Plastic Parts and Products).		Approval.
EPA 453/R-08-003	Miscellaneous Plastic Parts Coatings: Table 4—Automotive/Transportation and Business Machine Plastic Parts.	468 (Surface Coating of Plastic Parts and Products).		Approval.
EPA 453/R-08-003	Miscellaneous Plastic Parts Coatings: Table 5—Pleasure Craft Surface Coating.		Yes	Approval.
EPA 453/R-08-003	Miscellaneous Plastic Parts Coatings: Table 6—Motor Vehicle Materials.	459 (Automotive, Truck, and Heavy Equipment Refinishing Operations).		Approval.
EPA 453/R-08-004	Fiberglass Boat Manufacturing Materials		Yes	Approval.
EPA 453/R-08-005	Miscellaneous Industrial Adhesives		Yes	Approval.

TABLE 3—LIST OF RACT ELEMENTS—2008 OZONE NAAQS—Continued

CTG document No.	RACT element	District rule implementing RACT	Negative declaration submitted	EPA proposed action
EPA 453/R-08-006	Automobile and Light-Duty Truck Assembly Coatings.	Yes	Approval.
	Non-CTG Major Sources of NO _x	411 (NO _x from Boilers, Process Heaters, and Steam Generators), 412 (Stationary Internal Combustion Engines), 413 (Stationary Gas Turbines), 419 (NO _x from Miscellaneous Combustion Units).	Disapproval. ⁹
	Non-CTG Major Sources of VOC	Source-specific Requirements	Approval.

III. Statutory and Executive Order Reviews

Additional information about these statutes and Executive Orders can be found at <https://www.epa.gov/laws-regulations/laws-and-executive-orders>.

A. Executive Order 12866: Regulatory Planning and Review and Executive Order 13563: Improving Regulation and Regulatory Review

This action is not a significant regulatory action and was therefore not submitted to the Office of Management and Budget (OMB) for review.

B. Paperwork Reduction Act (PRA)

This action does not impose an information collection burden under the PRA because this action does not impose additional requirements beyond those imposed by state law.

C. Regulatory Flexibility Act (RFA)

I certify that this action will not have a significant economic impact on a substantial number of small entities under the RFA. This action will not impose any requirements on small entities beyond those imposed by state law.

D. Unfunded Mandates Reform Act (UMRA)

This action does not contain any unfunded mandate as described in UMRA, 2 U.S.C. 1531–1538, and does not significantly or uniquely affect small governments. This action does not impose additional requirements beyond those imposed by state law. Accordingly, no additional costs to state, local, or tribal governments, or to the private sector, will result from this action.

⁹As described in greater detail in our Technical Support Document (Docket Item B-01), the proposed disapproval for the non-CTG major sources of NO_x element is based in the deficiencies noted in Rules 411 and 413, as well as the lack of SIP-approved RACT level controls for the Mitsubishi Chemical and Carbon Fiber Composites facility due to the deficiencies noted in the submitted version of Rule 419.

E. Executive Order 13132: Federalism

This action does not have federalism implications. It will not have substantial direct effects on the states, on the relationship between the national government and the states, or on the distribution of power and responsibilities among the various levels of government.

F. Executive Order 13175: Coordination With Indian Tribal Governments

This action does not have tribal implications, as specified in Executive Order 13175, because the SIP is not approved to apply on any Indian reservation land or in any other area where the EPA or an Indian tribe has demonstrated that a tribe has jurisdiction, and will not impose substantial direct costs on tribal governments or preempt tribal law. Thus, Executive Order 13175 does not apply to this action.

G. Executive Order 13045: Protection of Children From Environmental Health Risks and Safety Risks

The EPA interprets Executive Order 13045 as applying only to those regulatory actions that concern environmental health or safety risks that the EPA has reason to believe may disproportionately affect children, per the definition of “covered regulatory action” in section 2–202 of the Executive Order. This action is not subject to Executive Order 13045 because it does not impose additional requirements beyond those imposed by state law.

H. Executive Order 13211: Actions That Significantly Affect Energy Supply, Distribution, or Use

This action is not subject to Executive Order 13211, because it is not a significant regulatory action under Executive Order 12866.

I. National Technology Transfer and Advancement Act (NTTAA)

Section 12(d) of the NTTAA directs the EPA to use voluntary consensus standards in its regulatory activities

unless to do so would be inconsistent with applicable law or otherwise impractical. The EPA believes that this action is not subject to the requirements of section 12(d) of the NTTAA because application of those requirements would be inconsistent with the CAA.

J. Executive Order 12898: Federal Actions To Address Environmental Justice in Minority Populations and Low-Income Population

Executive Order 12898 (Federal Actions To Address Environmental Justice in Minority Populations and Low-Income Populations, 59 FR 7629, February 16, 1994) directs Federal agencies to identify and address “disproportionately high and adverse human health or environmental effects” of their actions on minority populations and low-income populations to the greatest extent practicable and permitted by law. EPA defines environmental justice (EJ) as “the fair treatment and meaningful involvement of all people regardless of race, color, national origin, or income with respect to the development, implementation, and enforcement of environmental laws, regulations, and policies.” EPA further defines the term fair treatment to mean that “no group of people should bear a disproportionate burden of environmental harms and risks, including those resulting from the negative environmental consequences of industrial, governmental, and commercial operations or programs and policies.”

Under the CAA, the Administrator is required to approve a SIP submission that complies with the provision of the Act and applicable federal regulations. 42 U.S.C. 740(k); 40 CFR 52.02(a). Thus, in reviewing SIP submissions, the EPA’s role is to review state choices, and approve those choices if they meet the minimum criteria of the Act. Accordingly, this proposed action partially approves and partially disapproves state law as meeting federal requirements and does not impose additional requirements beyond those imposed by state law.

The District did not evaluate environmental justice considerations as part of its SIP submittal; the CAA and applicable implementing regulations neither prohibit nor require such an evaluation. The EPA did not perform an EJ analysis and did not consider EJ in this action. Consideration of EJ is not required as part of this action, and there is no information in the record inconsistent with the stated goals of E.O. 12898 of achieving environmental justice for people of color, low-income populations, and indigenous peoples.

List of Subjects in 40 CFR Part 52

Environmental protection, Air pollution control, Incorporation by reference, Intergovernmental relations, Nitrogen oxides, Ozone, Reporting and recordkeeping requirements, Volatile organic compounds.

Authority: 42 U.S.C. 7401 *et seq.*

Dated: March 28, 2023.

Kerry Drake,

Acting Regional Administrator, Region IX.

[FR Doc. 2023-06829 Filed 4-4-23; 8:45 am]

BILLING CODE 6560-50-P

ENVIRONMENTAL PROTECTION AGENCY

40 CFR Parts 141 and 142

[EPA-HQ-OW-2022-0260; FRL-8464-02-OW]

RIN 2040-AG14

National Primary Drinking Water Regulations: Consumer Confidence Report Rule Revisions

AGENCY: Environmental Protection Agency (EPA).

ACTION: Proposed rule.

SUMMARY: The Environmental Protection Agency (EPA) is proposing to revise the Consumer Confidence Report (CCR) Rule in accordance with America's Water Infrastructure Act (AWIA) of 2018 (AWIA, 2018) and to require reporting of compliance monitoring data to EPA. The proposed revisions to improve the CCR would improve the readability, clarity, and understandability of CCRs as well as the accuracy of the information presented, improve risk communication in CCRs, incorporate electronic delivery options, provide supplemental information regarding lead levels and control efforts, and require systems who serve 10,000 or more persons to provide CCRs to customers biannually (twice per year). The proposed requirements for states to submit to EPA compliance monitoring data for all National Primary Drinking

Water Regulations (NPDWRs) submitted by systems to the State would enhance EPA's oversight capabilities.

DATES: Comments must be received on or before May 22, 2023. Under the Paperwork Reduction Act, comments on the information collection provisions are best assured of consideration if the Office of Management and Budget (OMB) receives a copy of your comments on or before May 5, 2023.

ADDRESSES: Submit your comments, identified by Docket ID No. EPA-HQ-OW-2022-0260, by one of the following methods:

- *Federal eRulemaking Portal:* <https://www.regulations.gov/> (our preferred method). Follow the online instructions for submitting comments.
- *Mail:* U.S. Environmental Protection Agency, EPA Docket Center, Mail Code 28221T, 1200 Pennsylvania Avenue NW, Washington, DC 20460.
- *Hand Delivery or Courier:* EPA Docket Center, WJC West Building, Room 3334, 1301 Constitution Avenue NW, Washington, DC 20004. The Docket Center's hours of operations are 8:30 a.m.–4:30 p.m., Monday–Friday (except Federal Holidays).

Instructions: All submissions received must include the Docket ID No. EPA-HQ-OW-2022-0260 for this rulemaking. Comments received may be posted without change to <https://www.regulations.gov/>, including any personal information provided. Additional instructions on commenting or visiting the docket, along with more information about dockets generally, is available at <https://www.epa.gov/dockets/>.

FOR FURTHER INFORMATION CONTACT:

For technical information contact: Sarah Bradbury, Drinking Water Capacity and Compliance Division, Office of Ground Water and Drinking Water, Environmental Protection Agency, 1200 Pennsylvania Ave. NW, Washington, DC 20460-0001; telephone number (202) 564-3116; email address: bradbury.sarah@epa.gov.

For general information contact: EPA at OGWDWCCRrevisions@epa.gov or visit the agency's website at: <https://www.epa.gov/ccr/consumer-confidence-report-rule-revisions>, for general information about the Consumer Confidence Report Rule Revisions.

SUPPLEMENTARY INFORMATION:

Preamble acronyms and abbreviations. Throughout this document the use of “we,” “us,” or “our” is intended to refer to EPA. We use acronyms in this preamble. For reference purposes, EPA defines the following acronyms here:

ACS American Community Survey

ALE Action Level Exceedance
 AWIA America's Water Infrastructure Act
 CCR Consumer Confidence Report
 CCT Corrosion Control Treatment
 CFR Code of Federal Regulations
 CMD Compliance Monitoring Data
 CWS Community Water System
 EJ Environmental Justice
 EPA Environmental Protection Agency
 GAO Government Accountability Office
 ICR Information Collection Request
 LCRR Lead and Copper Rule Revisions
 LEP Limited English Proficiency
 LOE Level of Effort
 LSL Lead Service Line
 MCL Maximum Contaminant Level
 NDWAC National Drinking Water Advisory Council
 NPDWR National Primary Drinking Water Regulations
 OMB Office of Management and Budget
 PN Public Notification
 ppb Parts per billion
 ppm Parts per million
 ppt Parts per trillion
 PRA Paperwork Reduction Act
 PWS Public Water System
 PWSS Public Water System Supervision
 RFA Regulatory Flexibility Act
 RTCR Revised Total Coliform Rule
 SBA Small Business Administration
 SDWA Safe Drinking Water Act
 SDWIS Safe Drinking Water Information System
 SISNOSE Significant Economic Impact on a Substantial Number of Small Entities
 UCMR Unregulated Contaminant Monitoring Rule
 UMRA Unfunded Mandates Reform Act

Organization of this document. The information in this preamble is organized as follows:

- I. General Information
 - A. Does this action apply to me?
 - B. What is the Agency's authority for taking this action?
 - C. What action is the Agency taking?
 - D. Why is the Agency taking this action?
- II. Background
 - A. Overview of Consumer Confidence Report Rule
 - B. Overview of Compliance Monitoring Data Requirements
 - C. Consultations
 - D. Other Stakeholder Engagement
 - E. Supplementary Stakeholder Engagement
- III. Discussion of Proposed Rule
 - A. Purpose and Applicability
 - B. Compliance Date
 - C. Lead Notification and Corrosion Control Requirements
 - D. Improving Readability, Clarity, Understandability
 - E. Improving Accuracy and Risk Communication
 - F. Report Delivery
 - G. Compliance Monitoring Data (CMD)
 - H. Special State Primacy Requirements and Rationale
 - I. Housekeeping
- IV. Request for Public Comment
 - A. General Matters Concerning Consumer Confidence Reports
 - B. Timing of Consumer Confidence Reports

- C. Increasing Readability, Clarity, and Understandability of the Consumer Confidence Report
- D. Corrosion Control and Action Level Exceedances
- E. General Matters Concerning CMD Requirements
- V. Cost of the Rule
 - A. Estimates of the Total Annualized Cost of the Proposed Rule Revisions
 - B. Revisions to Consumer Confidence Report
 - C. Compliance Monitoring Data (CMD) Costs
 - D. Qualitative Benefits
- VI. Statutory and Executive Order Reviews

- A. Executive Order 12866: Regulatory Planning and Review and Executive Order 13563 Improving Regulation and Regulatory Review
- B. Paperwork Reduction Act
- C. Regulatory Flexibility Act as Amended by the Small Business Regulatory Fairness Act
- D. Unfunded Mandates Reform Act
- E. Executive Order 13132: Federalism
- F. Executive Order 13175: Consultation and Coordination With Indian Tribal Governments
- G. Executive Order 13045: Protection of Children From Environmental Health and Safety Risks

- H. Executive Order 13211: Actions Concerning Regulations That Significantly Affect Energy Supply, Distribution or Use
- I. National Technology Transfer and Advancement Act
- J. Executive Order 12898: Federal Actions To Address Environmental Justice in Minority Populations and Low-Income Populations
- VII. References

I. General Information

- A. *Does this action apply to me?*
Potentially regulated persons are Community Water Systems (CWSs).

Category	Example of potentially affected entities
CWSs	Community water systems (a public water system that (A) serves at least 15 service connections used by year-round residents of the area served by the system; or (B) regularly serves at least 25 year-round residents).
State and tribal agencies	Agencies responsible for drinking water regulatory development and enforcement.

This table is not intended to be exhaustive, but rather provides a guide for readers regarding entities likely to be regulated by this action. This table lists the types of entities that EPA is now aware could potentially be regulated by this action. Other types of entities not listed in this table could also be regulated. To determine whether your facility is regulated by this action, you should carefully examine the applicability criteria in 40 CFR 141.151 of the rule. If you have any questions regarding the applicability of this proposed action to a particular entity, consult the technical information contact listed under **FOR FURTHER INFORMATION CONTACT**.

B. What is the Agency’s authority for taking this action?

The statutory authority for this rule is the Safe Drinking Water Act, including Sections 1413, 1414, 1445, and 1450. Congress passed America’s Water Infrastructure Act (AWIA) into law on October 23, 2018, (Pub. L. 115–270 U.S. Congress, 2018) to improve drinking water and water quality, deepen infrastructure investments, enhance public health and quality of life, increase jobs, and bolster the economy. AWIA Section 2008 amended the Safe Drinking Water Act (SDWA) Section 1414(c)(4)(F) to require certain revisions to the Consumer Confidence Report Rule within 24 months of the date of enactment (*i.e.*, by October 23, 2020). In response to a complaint filed by the Natural Resources Defense Council on January 19, 2021, and after public notice and the opportunity to comment, EPA entered into a consent decree that requires the agency to sign for

publication in the **Federal Register** revisions to the consumer confidence report regulations no later than March 15, 2024, to comply with AWIA amendments to SDWA Section 1414(c)(4) (Docket no. EPA–HQ–OGC–2021–0753). This action proposes revisions to fulfill the rulemaking requirements of SDWA Section 1414(c)(4)(F).

EPA first promulgated regulations in 1998 to require CCRs after the 1996 SDWA amendments added requirements for water systems to provide annual reports to each customer of a water system on the level of contaminants in the drinking water and related information. These annual reports were part of the “Right to Know” provisions added to the statute in 1996 and designed to increase the amount of information made available by community water systems (CWS) to their consumers. Section 2008 of America’s Water Infrastructure Act of 2018 (Pub. L. 115–270) amended SDWA Section 1414(c)(4) on Consumer Confidence Reports by adding a new paragraph 1414(c)(4)(F). This new paragraph requires EPA to revise the 1998 Consumer Confidence Report regulations to increase the readability, clarity, and understandability of the information presented in the CCRs; increase the accuracy of information presented and risk communication in the CCRs; mandate report delivery at least biannually by systems serving 10,000 or more; and allow electronic delivery consistent with methods described in the memorandum *Safe Drinking Water Act-Consumer Confidence Report Rule Delivery Options* (USEPA, 2013) issued by the

Environmental Protection Agency on January 3, 2013. The AWIA amendments also require CCRs to include information on corrosion control efforts and when corrective action to reduce lead levels throughout the system is required following a lead action level exceedance (ALE). As with the original Consumer Confidence Report Rule, the AWIA amendments direct that the revised regulations must be developed in consultation with public water systems, environmental groups, public interest groups, risk communication experts, the states, and other interested parties.

In addition, AWIA, Section 2011—Improved Accuracy and Availability of Compliance Monitoring Data—amended Section 1414 of the Safe Drinking Water Act to add a new section, 1414(j). SDWA Section 1414(j) required EPA to provide to Congress a strategic plan for improving the accuracy and availability of monitoring data collected to demonstrate compliance with NPDWRs by October 23, 2019. These amendments directed EPA to evaluate challenges with ensuring the accuracy and integrity of submitted data, challenges encountered by states and water systems in implementing electronic submission of data, and challenges faced by users in accessing the data. EPA was further directed to include in its strategic plan a summary of findings and recommendations on practicable, cost-effective methods and means that can be employed to improve the accuracy and availability of submitted data. To meet this statutory requirement, EPA coordinated with states, Public Water Systems (PWSs), and other interested stakeholders to inform this effort. These

discussions included staff from state drinking water programs, PWSs, and state laboratories, as well as staff from relevant EPA regions. Among other findings, the plan identified a strategic need for EPA to obtain and evaluate monitoring data already collected by states (USEPA, 2022a). Compliance monitoring data (CMD) supports the agency's oversight responsibilities by providing a more complete picture of water quality and water system compliance than simple violation information.

Section 1445(a) of the Safe Drinking Water Act authorizes EPA to require any person (including water systems and States) subject to SDWA to make such reports as EPA may reasonably require by regulation to assist the agency in determining whether such person has acted or is acting in compliance with SDWA. Under Section 1413(a)(1)–(3) of SDWA, states with primary enforcement authority are required to adopt drinking water regulations no less stringent than NPDWRs, adopt and implement adequate procedures for the enforcement of those regulations, and keep records and make reports with respect to those activities as EPA may reasonably require by regulation. EPA is proposing that an annual collection of CMD is needed to improve the agency's oversight of SDWA compliance. EPA's and states' primary method of monitoring PWS compliance with the SDWA is the review and evaluation of results of water samples and operating reports collected by PWSs. Currently EPA receives information only on water system violations identified and reported by the state. This does not allow EPA to fully determine if the water system is in compliance with all of the necessary sampling and other actions required by regulation. As such, EPA is proposing that an annual collection of CMD is needed to assist the agency in oversight of SDWA compliance.

The proposal for annual reporting of CMD is also consistent with Government Accountability Office report (GAO–11–381) recommendations to routinely evaluate the quality of selected drinking water data on health-based and monitoring violations that states provide to EPA in order to improve EPA's ability to oversee the states' implementation of the SDWA and provide Congress and the public with more complete and accurate information on compliance. A complete list of GAO recommendations can be found at: <https://www.gao.gov/assets/gao-11-381.pdf>. The annual reporting of CMD is also consistent with the Foundations for Evidence-Based

Policymaking Act of 2018 (also called the Evidence Act), which directs all Federal agencies to build and use evidence to improve policy, program, operational, budget, and management decision-making. The collection of CMD will give a more complete and accurate depiction of water system compliance, which will improve the decisions EPA makes on oversight, enforcement, and training and technical assistance actions.

C. What action is the Agency taking?

Consistent with the statutory provisions and purposes described above, EPA is proposing a rule to (1) revise the Consumer Confidence Report regulations and (2) establish requirements for states, territories, and tribes with primacy to report CMD annually to EPA.

D. Why is the Agency taking this action?

In passing AWIA's amendments to the CCR provisions of SDWA, Congress reaffirmed that Americans have a right to know what is in their drinking water and where it comes from and highlighted a need for improvements to the annual consumer confidence reports to increase the readability, clarity, and understandability of the information, as well as the accuracy of the information presented and the risk communication. These proposed revisions would address those needs as well as require CCRs to include certain information about lead in drinking water. The proposed rule would also require CCRs to be distributed more frequently to customers of systems serving at least 10,000 persons. These efforts to improve right-to-know access align with decades of Congressional direction, including the priorities in the Bipartisan Infrastructure Law as well as EPA's Justice40 Initiatives to support small, disadvantaged or underserved communities, who are likely to have the most difficult time accessing and understanding information about their drinking water. This proposed rule would improve public health protection and further the goal of the 1996 SDWA "right-to-know" provisions by improving access to and clarity of drinking water data so that customers of community water systems can make informed decisions about their health and the health of their families.

EPA needs more robust CMD to better understand nationwide trends, evaluate specific issues at individual public water supply facilities, conduct the agency's required oversight responsibilities, and provide effective compliance assistance. EPA's current limited access to only quarterly and

annual reports to the Administrator (40 CFR 142.15(a)) provides narrowly based information on system inventory, presence of violations, and other information. While EPA may ask for additional data from states on a case-by-case basis as part of the annual (or more frequent) file review conducted under 40 CFR 142.17, EPA does not receive CMD currently collected by all states for all NPDWRs. This means that EPA does not receive information necessary to identify national trends associated with contaminants. It also means that EPA is hindered in its attempts to identify and respond to issues at individual public water systems. Receiving the complete set of data for systems would allow EPA to identify trends nationally to evaluate and quantify the effectiveness of treatment methods, compliance with contaminant levels and other drinking water regulations, and water system operational issues. In turn, this data would help EPA more readily identify and respond to problems nationally and at specific systems that could pose a threat to public health. The complete set of CMD will provide ancillary benefits, including enabling a more comprehensive approach to identifying infrastructure needs, and informing how EPA and states can work together to deliver technical and funding assistance to water systems in a manner that more effectively addresses underlying technical, managerial, and financial capacity-building needs. This information will also allow the agency to identify trends both geographically and demographically, which will improve transparency and accountability, and amplify best practices that maximize direct benefits in these communities. Therefore, EPA is proposing a new regulatory requirement pursuant to Section 1445(a)(1)(A) and Section 1413(a)(3) of the SDWA requiring all states to submit CMD to EPA for all NPDWRs annually. EPA's proposed action will not require any additional data collection by water systems or primacy agencies, as water systems have been collecting and reporting CMD to primacy agencies for all NPDWRs for decades.

II. Background

A. Overview of Consumer Confidence Report Rule

CCRs are a centerpiece of the public right-to-know provisions in SDWA. The information contained in CCRs can raise consumers' awareness of where their water comes from, help them understand the process by which safe drinking water is delivered to their homes, and educate them about the

importance of preventative measures, such as source water protection, that ensure a safe drinking water supply. CCRs can promote a dialogue between consumers and their drinking water utilities, can encourage consumers to become more involved in decisions which may affect their health, and may allow consumers to make more informed decisions about their drinking water. CCRs also reveal important drinking water information on source water assessments, health effects data, and the water system.

The SDWA Amendments of 1996 originally created Section 1414(c)(4), which required community water systems to provide annual CCRs to their customers with the goal to better protect health of consumers by providing a detailed report on the state of their drinking water supply. EPA promulgated the Consumer Confidence Report Rule in August 1998 and the rule established content and delivery requirements for community water systems (USEPA, 1998). CCRs must include information on the water system; sources of water; definitions of key terms; detected contaminants; the presence of *Cryptosporidium*, radon, and other contaminants; compliance with the National Primary Drinking Water Regulations; variances and exemptions; and additional required information. Systems are required to deliver the reports annually by July 1st through mail or other direct delivery methods. As described in Section 1414(c)(4)(C) of SDWA and EPA's implementing regulations at 141.155(g), community water systems serving less than 10,000 people may obtain a waiver from the requirement to mail or otherwise directly deliver the CCR to each customer; such systems must meet requirements to provide notice of and access to the CCR in other ways.

Since the original CCR Rule was promulgated in 1998, the most significant update was to clarify the CCR regulations regarding electronic delivery in a policy memorandum that responded to Executive Order (E.O.) 13563 (2011). The E.O. charged each Federal agency to "develop a plan under which the agency will periodically review its existing significant regulations to determine whether any such regulations should be modified, streamlined, expanded, or repealed so as to make the agency's regulatory program more effective or less burdensome in achieving the regulatory objectives." EPA identified the Consumer Confidence Report Rule as one of the regulations to "explore ways to promote greater transparency and public participation in protecting the

Nation's drinking water in keeping with E.O. 13563's directive to promote participation and the open exchange of information." Stakeholders noted that there had been an increase in the number and type of communication tools available since 1998 when the Consumer Confidence Report Rule was promulgated. In 2013, EPA released an interpretive memorandum, *Safe Drinking Water Act—Consumer Confidence Report Rule Delivery Options*, along with an attachment entitled *Consumer Confidence Report Electronic Delivery Options and Considerations* (USEPA, 2013). The memorandum describes approaches and methods for electronic delivery that are consistent with the existing Consumer Confidence Report Rule requirement to "mail or otherwise directly deliver" a copy of the report to each customer and consistent with providing flexibility for alternative forms of communication.

B. Overview of Compliance Monitoring Data Requirements

Under SDWA, EPA authorizes states, Territories and Tribes for primary enforcement responsibility or "primacy" for public water systems. Public water systems are subject to primary drinking water regulations which include monitoring requirements to ensure compliance with those regulations. Under 40 CFR 142.14, states, territories, and tribes with primacy are required to maintain records, including CMD from these water systems to demonstrate compliance with NPDWRs. EPA currently requires states to submit quarterly and annual reports to the Administrator (40 CFR 142.15(a)). These reports are limited in scope and provide system inventory, violations, and other information. Under 40 CFR 142.17, EPA is required to review at least annually the compliance of the state, territory, or tribe with the regulatory requirements for primacy in 40 CFR part 142, which includes adoption and implementation of adequate procedures for enforcement of drinking water regulations, including the requirements for systems to conduct monitoring and collect data.

Compliance and public health protection rely on accurate and complete data. EPA's Drinking Water Compliance Monitoring Data Strategic Plan describes that EPA needs CMD to ensure data quality and national consistency in SDWA implementation, in addition to supporting informed decision making. EPA and other primacy agencies need data of known and documented quality and completeness to identify national trends, understand the effectiveness of

different treatment methodologies, develop effective and appropriate policy decisions, understand operational issues, and provide appropriate training and technical assistance. Accurate and timely monitoring data is critical to EPA's effective oversight of public water systems and primacy agencies.

Currently there is no national access to drinking water compliance monitoring data. Following the collection of CMD from primacy agencies, and in line with the action plan of the CMD Strategic Plan, EPA intends to make the CMD available to the public. Public access to drinking water data can empower communities to take necessary public health actions. Public access will also promote additional accountability for the water systems, which can lead to improved data quality and compliance.

C. Consultations

Section 1414(c)(4)(F)(i) of the SDWA requires the agency to consult with "public water systems, environmental groups, public interest groups, risk communication experts, and the States, and other interested parties" in developing revisions to the Consumer Confidence Report Rule. EPA consulted with various stakeholders to solicit input on the proposed rulemaking.

1. Initial Tribal Consultation on Consumer Confidence Reports

EPA sought input from tribal governments from March 14, 2022, through June 14, 2022, to better inform the development of the proposed Consumer Confidence Report Rule Revisions (USEPA, 2022c). Upon initiation of consultation, consultation notification letters were emailed to the tribal leaders of all federally recognized tribes using the Bureau of Indian Affairs's Tribal Leaders Directory. The letters provided background information about the forthcoming rulemaking and the consultation and coordination plan.

EPA also hosted two informational webinars for tribal officials, which included the opportunity for participants to ask questions and provide feedback. Tribes were able to comment on any aspect of the forthcoming rulemaking, and EPA requested specific input from tribal governments on elements related to potential regulatory requirements of the proposed Consumer Confidence Report Rule Revisions and suggestions that would assist tribal governments in implementing and complying with the rule. EPA requested tribal input on the following questions.

a. What concerns about your water do you look to be addressed in your water quality report?

b. What challenges, if any, do you have when trying to read and/or understand your water quality report?

c. What resources or tools are needed to support the creation of water quality reports?

d. What is your preferred delivery format and method for receiving your water quality report?

2. Supplemental Tribal Consultation With Navajo Nation Indian Tribe

After the initial tribal consultation, the agency expanded the scope of the rulemaking to include a requirement for primacy agencies to submit comprehensive CMD annually to the agency. EPA offered supplemental consultation to the Navajo Nation as a primacy agency who could be affected by the expanded scope. No additional comments were received during the Supplemental Tribal Consultation period. Tribal consultation and coordination were conducted in accordance with EPA Policy on Consultation and Coordination with Indian Tribes (<https://www.epa.gov/tribal/forms/consultation-and-coordination-tribes>).

3. Federalism Consultation

On August 25, 2022, EPA initiated a 60-day Federalism consultation by hosting a meeting with members of state and local government associations and invited water utility associations. EPA presented background information on the proposed rule and sought feedback on key considerations for the rulemaking. EPA requested feedback on the content of reports delivered twice a year, support for communities with large proportions of non-English speaking populations, and the inclusion of annual collection of compliance monitoring data within the rulemaking. A summary of the CCR Rule Revisions federalism consultation and comments received is included with supporting materials in the docket (USEPA, 2022d).

D. Other Stakeholder Engagement

1. National Drinking Water Advisory Council Consultation on the Consumer Confidence Report Rule Revisions

EPA sought recommendations from the National Drinking Water Advisory Council (NDWAC or Council) in four key areas: addressing accessibility challenges, including translating CCRs and meeting Americans with Disabilities Act (ADA) requirements; advancing environmental justice and supporting underserved communities;

improving readability, understandability, clarity, and accuracy of information and risk communication of CCRs; and CCR delivery manner and methods, including electronic delivery. EPA directed the NDWAC to establish a working group consisting of representatives of public water systems, environmental groups, public interest groups, risk communication experts, the states, and other interested parties to assist the Council.

The NDWAC's Consumer Confidence Report Rule Revisions working group consisted of twelve people from public water systems, environmental groups, public interest groups, and Federal, state, and tribal agencies. The working group included seven NDWAC members, and one member each from EPA's National Environmental Justice Advisory Council and Children's Health Protection Advisory Committee. The NDWAC working group held seventeen meetings to discuss the Consumer Confidence Report Rule Revisions that were open to the public. The working group heard presentations and received written public comments during the development of their recommendations to the NDWAC. Working group members also participated in a public meeting of the NDWAC, which included oral and written public comments, to discuss the working group's preliminary recommendations. The NDWAC working group provided its final recommendations to the NDWAC in November 2021. The NDWAC discussed the working group's final recommendations during a two-day public meeting of the Council on December 1–2, 2021. At that meeting, the NDWAC conducted deliberations on the working group's recommendations. The NDWAC provided EPA with its recommendations on December 14, 2021.

Materials from this NDWAC process, including the *Report of the Consumer Confidence Report Rule Revisions Working Group to the National Drinking Water Advisory Council*, and Letter to Administrator on CCR Rule Revision from the NDWAC are available in the docket at <https://www.epa.gov/system/files/documents/2022-02/ndwac-consumer-confidence-report-rule-revision-letter-december-2021.pdf>. (NDWAC, 2021).

2. Targeted Interviews

EPA conducted separate interviews with nine states, nine community water systems of varying sizes representing different regions, as well as a county health official (risk communication expert), a public interest group, and an environmental justice organization. The

purpose of the interviews with states and water systems was to identify level of effort, costs, and burden associated with CCR development, delivery, and compliance, in addition to other issues and challenges with implementing current rule provisions. The purpose of the interviews with the other organizations was to discuss experiences related to drinking water and/or CCRs, including concerns of their members, outreach and communication strategies, translations, and any other challenges they experience. A summary of the interviews is included with supporting materials in the docket (USEPA, 2022f).

3. Virtual Public Listening Session

On April 26, 2022, EPA hosted a virtual public listening session. During the session, EPA provided a brief introduction/overview of the project and purpose, and allowed registered attendees to provide input on 6 topics:

- Tools that address challenges to developing CCRs.
- CCR delivery methods, including electronic delivery options.
- Considerations and concerns related to underserved communities and environmental justice.
- Biannual delivery, including timing and content of reports.
- CCR accessibility challenges and solutions.
- Improving readability, clarity, understandability, accuracy, and risk communication of the information presented in CCRs.

EPA announced the listening session in the **Federal Register** (87 FR 23861, April 21, 2022) and held a 30-day comment period from April 23, 2022, through May 23, 2022. A summary of the verbal comments received during the listening session is available in the Docket.

E. Supplementary Stakeholder Engagement

The agency issued the final Lead and Copper Rule Revisions (Docket ID EPA–HQ–OW–2017–0300) on January 15, 2021. On January 20, 2021, President Biden issued the “Executive Order on Protecting Public Health and the Environment and Restoring Science to Tackle the Climate Crisis.” (86 FR 7037, January 25, 2021) (“Executive Order 13990”). Section 1 of E.O. 13990 states that it is “the policy of the Administration to listen to the science, to improve public health and protect our environment, to ensure access to clean air and water, . . . and to prioritize both environmental justice and the creation of the well-paying union jobs necessary to deliver on these

goals.” E.O. 13990 directed the heads of all Federal agencies to immediately review regulations that may be inconsistent with, or present obstacles to, the policy it establishes. In accordance with E.O. 13990, EPA reviewed the Lead and Copper Rule Revisions (LCRR) to engage meaningfully with the public regarding this important public health regulation before it took effect. As part of EPA’s commitment to Environmental Justice, EPA specifically sought engagement with communities that have been disproportionately impacted by lead in drinking water, especially lower-income people and communities of color that have been underrepresented in past rule-making efforts. Feedback from those discussions related to CCRs and drinking water notifications were summarized and considered for this rulemaking (USEPA, 2021b).

III. Discussion of Proposed Rule

A. Purpose and Applicability

EPA is proposing to revise the requirements for the content of CCRs in accordance with the requirements set forth in Section 1414(c)(4) of SDWA and as authorized under Section 1445(a)(1) and Section 1413(a)(3) to require states, territories, and tribes with primary enforcement responsibility to provide EPA compliance monitoring data on an annual basis. This proposal revises 40 CFR part 141 subpart O and 40 CFR part 142. The proposed changes to 40 CFR part 141 apply to existing and new CWSs. A CWS is a public water system that serves at least 15 service connections used by year-round residents or regularly serves at least 25 year-round residents. EPA considers a year-round resident to mean an individual whose primary residence is served by the water system, even if they may not live at the residence 365 days a year (USEPA, 1991). Out of the approximately 155,000 public water systems in the United States, about a third—approximately 49,000—are considered CWSs. These systems range from large municipal systems that serve millions of consumers to small systems that serve fewer than 100 consumers. The balance of the water systems in the United States, or approximately 106,000 systems, are either transient non-community systems, which do not serve the same people on a day-to-day basis (for example, highway rest stops), or non-transient non-community systems, which serve at least 25 of the same people at least 6 months of the year (for example, schools). Because this proposed rule applies only to CWSs, as provided by Congress in the 1996

Amendments to SDWA, transient and non-transient non-community systems are not affected by this proposed rule.

EPA notes that many water wholesalers are also considered CWSs. If such a system does not retail water to any customer, *i.e.*, billing unit or drinking water hook-up, the system will not have to prepare and submit a CCR. However, these systems will have to provide the relevant information to the purchaser, also known as a consecutive system, so that the purchaser can prepare a CCR and provide it to their customers.

States, tribes, and territories with primary enforcement responsibility, also called “primacy,” are those that have been authorized by EPA to implement the NPDWRs and associated requirements in their state or territory. Currently, all states and territories except Wyoming and the District of Columbia have primacy. The Navajo Nation is the only Indian tribe to have primacy. EPA is proposing that states, territories, and Tribes with primacy be required to report comprehensive compliance monitoring data to EPA on an annual basis. This proposed rule would not change existing reporting requirements for public water systems to report compliance data to their primacy agency.

B. Compliance Date

EPA is required by the Consent Decree to sign for publication “revisions” to the consumer confidence report regulation not later than March 15, 2024. EPA is proposing to require compliance with the CCR Rule Revisions beginning approximately one year after promulgation of the rule (effective 30 days after publication of the final rule in the **Federal Register**). EPA expects that beginning April 1, 2025, CWSs would have to comply with the new CCR content and delivery requirements in 40 CFR 141.151 through 141.156. Since CWSs have been preparing and delivering CCRs for over 20 years, EPA anticipates systems should be able to meet the additional content and delivery requirements by 2025. CWSs would need to continue to comply with 40 CFR 141.151 through 141.155, as codified in 40 CFR part 141, subpart O on July 1, 2023, until the compliance date of the new regulations. EPA is requesting comments on CCR compliance dates in Section IV of this preamble.

EPA is also proposing that the requirement for primacy agencies to report compliance monitoring data to EPA take effect in the CFR 30 days after publication of the final rule in the **Federal Register** in 2024 and primacy

agencies would be required to comply with requirements for annual compliance monitoring data reporting to EPA beginning one year after the effective date in 2025. Primacy agencies already are receiving CMD from all water systems regulated by the Public Water System Supervision (PWSS) program under § 142.14. Prior to the compliance date, EPA anticipates it will develop the database to maintain the collected data and provide a CMD extraction and sharing tool for primacy agencies that use the Safe Drinking Water Information System State (SDWIS State) and a database extract option for the primacy agencies that do not use SDWIS State. The agency believes the proposed compliance date for CMD reporting is practicable because these extraction tools are easy to use and familiar to many primacy agencies who currently use similar extraction tools to provide their data to the agency, for example under the 6-year review program.

C. Lead Notification and Corrosion Control Requirements

AWIA of 2018 amended Section 1414(c)(4)(B)(iv) and (vii) to require the information in CCRs on compliance with NPDWRs to include information on “corrosion control efforts” and identification of any lead action level exceedance (ALE) for which corrective action has been required during the monitoring period covered by the CCR.

Currently there are an estimated 6.3 to 9.3 million homes served by lead service lines (LSLs) in thousands of communities nationwide, in addition to millions of older buildings with lead solder, and brass/bronze fittings and faucets. Corrosion control treatment (CCT) involves changing water quality characteristics including alkalinity, pH, and dissolved inorganic carbon or involves the addition of a corrosion inhibitor such as orthophosphate to reduce the rate of metal release into the water. The type of corrosion control efforts implemented by individual systems vary based on several factors, including the applicable requirements of EPA’s regulations to control lead and copper. Besides CCT, systems also use other approaches to protect consumers from exposure to lead and copper, such as establishing a monitoring plan for lead, copper, and water quality parameters; treating source water for lead and copper; following state approved treatment methods of the source water; and/or replacing lead service lines (LSL). Lead and copper enter drinking water mainly from the corrosion of the pipes, fittings, and fixtures in the water distribution

system, including premise plumbing. EPA is proposing to require CWSs to describe their corrosion control and other efforts such as studies conducted to identify corrosion control treatments, application of corrosion control technologies, as well as regular water quality monitoring conducted to ensure effective implementation of the corrosion control treatment strategy. EPA is proposing to add to the CCR the following definition for corrosion control efforts: *Treatment (including pH adjustment, alkalinity adjustment, or corrosion inhibitor addition) or other efforts contributing to the control of the corrosivity of water, e.g., monitoring to assess the corrosivity of water.*

Rather than prescribing specific language to describe corrosion control efforts, EPA is proposing in the CCR Rule Revisions that systems develop their own statement to describe their corrosion control efforts. In Section IV of this preamble, EPA is requesting comments on whether the CCR Rule should instead include prescribed language.

As part of the LCRR (USEPA, 2021c), EPA revised the Consumer Confidence Report Rule to require CWSs to report the range of tap sample lead results in addition to the currently required 90th percentile lead concentration and the number of samples that are greater than the lead action level for each monitoring period. Systems are required to comply with the new LCRR CCR requirements beginning in reports delivered in 2025. In addition to including information on tap samples that exceed the lead action level, this rule proposes that the CCRs include details about what corrective actions are or were taken by systems to address an action level exceedance. Under the currently effective LCRR, following an ALE, systems must perform follow-up actions, including installing or re-optimizing corrosion control treatment, providing public education, and conducting lead service line replacement to address elevated levels of lead. The proposed changes to the CCR rule would require systems to clearly identify in their CCR that they have an ALE and describe in their CCR the follow-up or corrective actions they have taken or will take. While the LCRR took effect on December 16, 2021, and compliance is currently required beginning on October 16, 2024, the reporting on availability of tap sample lead results, and the status of service line inventory will not be required in the CCR until the first report required in calendar year 2025. This coincides with the proposed compliance date for this proposed rule. The proposed Revised CCR Rule adds a requirement for

systems to include a link to their lead service line inventory if it is available on a publicly accessible website.

D. Improving Readability, Clarity, Understandability

Consumer confidence reports contain a great deal of highly technical information. In amending SDWA 1414(c)(4), Congress directed EPA to revise the regulations to increase the readability, clarity, and understandability of the information in the CCRs and to increase the accuracy of information presented, and risk communication. EPA interprets this statutory directive as setting a goal to make CCRs easier for every American to understand so that they may make informed decisions about their health and any risks associated with their drinking water. This proposed rule would meet that goal and improve the readability, clarity, and understandability of CCRs by revising the current mandatory and prescribed language in § 141.153 *Content of the reports* and § 141.154 *Required additional health information*. The proposed rule would ensure clear and simple messaging that will streamline the report, focusing on information that is most useful to consumers. EPA is including new definitions to include in the reports as applicable, including definitions for “*corrosion control efforts*,” *parts per million (PPM)*, *parts per billion (PPB)*, *parts trillion (PPT)*, *pesticide*, and *herbicide*. Systems may use alternate definitions for PPM, PPB, PPT, pesticide and herbicide, if the system obtains written approval from the state to use alternate definitions. EPA is also proposing the following approaches to improve the readability, clarity, and understandability of the information presented in the reports: requiring each CCR to include a summary of key information at the beginning of the report; allowing water systems additional flexibility in presenting contaminant data; and supporting meaningful access to communities with limited English proficiency (LEP).

1. Report Summary

CCRs provide a valuable communication opportunity for the community water systems to provide information to consumers. As a result, in some cases, reports can be quite lengthy. During EPA’s Retrospective Review, feedback from stakeholders recommended that reports should include an at-a-glance summary to improve understandability of reports (USEPA, 2012). The NDWAC expanded on this idea in recommending that CCRs

include a summary page to convey important information and key messages in a simple, clear, and concise manner at the beginning of the report (NDWAC, 2021).

EPA agrees with these stakeholder recommendations, and this proposed rule proposes to add § 141.156 that requires the inclusion of a summary at the beginning of each CCR. At a minimum, systems would need to include a summary of violations and ALEs, information on how consumers can contact the system to receive additional information, and, if applicable, information on how consumers can receive assistance with accessibility needs, such as translating the report into other languages, and a statement identifying that public notifications (PN) of violations or other situations are delivered with the CCR, as allowed in 40 CFR part 141, subpart Q. Systems that include PNs in the CCRs often place them at the end of the report, which may be overlooked by consumers. Including a statement in the summary about PNs in the report will help consumers find important information about violations that may or may not be included in the CCR itself, for example, if the violation occurred outside of the CCR reporting period. This summary should, as much as possible, be accessible and understandable to the public. The proposed rule allows systems the flexibility to present the information as an infographic to improve clarity and understandability. EPA believes that a summary included at the beginning of the reports will allow consumers to quickly view key information and may lead to more people engaging with the reports. EPA is requesting comments on requirements for the summary in Section IV of this preamble.

2. Contaminant Data Section

The original Consumer Confidence Report Rule required that data for detected contaminants subject to mandatory monitoring be displayed in one or more tables. EPA’s intent was to make the presentation of the data as consumer friendly as possible, while providing sufficient flexibility so that reports can be improved based on feedback from customers (USEPA, 1998). Since then, advances in technology and graphics have allowed data to be presented in clearer and more understandable ways using readily available software.

EPA is proposing to allow water systems flexibility in formatting contaminant data to present the information in a more readable and understandable format. During EPA’s

consultations on this proposal, stakeholders identified the use of infographics to display information as one way to help improve understandability of technical concepts in the reports. To reflect this change, EPA is proposing to replace “contaminant data table(s)” with “contaminant data section.” As proposed, § 141.153(d), would require water systems to display the contaminant data in logical groupings that would make it easier for consumers to read and understand the contaminant information. For example, this could include grouping contaminants by source type, contaminant type (inorganics, organics, disinfection byproducts (DBPs), etc.), or detection values, e.g., grouping contaminants that have detection values above half the MCL together. Water systems should not obfuscate or attempt to conceal the information by presenting contaminant data in such a way that would make it difficult for consumers to read or understand; however, systems may continue to use one or more tables to display contaminant data. Despite allowing additional flexibility on how the information is presented, this proposed rule would not change the type of information on detected contaminants that systems need to report in § 141.153(d)(4), such as reporting the maximum contaminant level, maximum contaminant level goal, the highest contaminant level used to determine compliance with a National Primary Drinking Water Regulation, and the range of detected levels for each detected contaminant.

3. Explaining Unregulated Contaminant Monitoring Results in CCRs

The 1996 SDWA amendments require that once every five years EPA issue a new list of no more than 30 unregulated contaminants to be monitored by PWSS. EPA uses the Unregulated Contaminant Monitoring Rule (UCMR) to collect data for contaminants that are suspected to be present in drinking water and do not have health-based standards set under SDWA. The monitoring provides EPA and other interested parties with nationally representative data on the occurrence of contaminants in drinking water, the number of people potentially being exposed, and an estimate of the levels of that exposure. This data can support future regulatory determinations and other actions to protect public health and the environment.

Community water systems are required to report detected UCMR monitoring results in CCRs. According to § 141.153(d)(7), systems must present

the average and range of contaminants for which monitoring is required under § 141.40. In this proposed rule, systems will be required to include a brief explanation of the reasons for monitoring for unregulated contaminants such as, “*Unregulated contaminant monitoring helps EPA to determine where certain contaminants occur and whether the Agency should consider regulating those contaminants in the future.*” As proposed, § 141.153(d)(7) would allow a water system to write its own educational statement, but only with approval of the Primacy Agency. This will improve understandability for consumers by ensuring that systems explain the UCMR results.

4. Translation Support for Limited English Proficient Persons and Accessibility Considerations

In 2019, an estimated 22 percent of people in the United States (68 million people) spoke a language other than English in the home, and 8.3 percent of people in the United States (25 million people) were considered to have limited English proficiency (U.S. Census Bureau, 2021b). According to the American Community Survey (ACS), this is equivalent to approximately 23 million American households. Individuals who do not speak English as their primary language and who have a limited ability to read, write, speak, or understand English are considered Limited English Proficient, or “LEP.” Limited English proficiency can be a barrier to accessing important benefits, services, or information. CCRs are valuable tools to inform consumers and to allow them to make informed decisions about the health and safety of their drinking water. If LEP consumers are not able to read and understand the reports, or have sufficient access to that information, it raises equity concerns that some communities may not have as complete an understanding about the quality of their drinking water as more proficient English-speaking consumers.

To support implementation of Title VI regulations (40 CFR part 7) EPA has specified that “recipients of Federal financial assistance have an obligation to reduce language barriers that can preclude meaningful access by LEP persons to important government services” (EPA, 2004). States that EPA has authorized for primary enforcement responsibility (primacy) for the PWSS Programs are eligible to receive grants to assist with developing and implementing their PWSS program. Currently, all states and territories (except Wyoming and the District of Columbia), and the Navajo Nation have

primacy. In Fiscal Year 2021 (FY21) and 2022 (FY22), each of those primacy agencies received PWSS grant funds (USEPA, 2021a and 2022h).

EPA is proposing to revise 40 CFR 141.153(h)(3) to require primacy agencies to assist water systems in providing meaningful access to CCRs for LEP consumers in a manner consistent with the Guidance to Environmental Protection Agency Financial Assistance Recipients Regarding Title VI Prohibition Against National Origin Discrimination Affecting Limited English Proficient Persons, which can be found at: <https://www.federalregister.gov/documents/2004/06/25/04-14464/guidance-to-environmental-protection-agency-financial-assistance-recipients-regarding-title-vi> (EPA Title VI Guidance)(2004). As part of their primacy application or revision, states, territories, and tribes will need to include a description of how they intend to provide timely support to LEP drinking water consumers that need assistance with translation services. In communities with a large proportion of consumers with limited English proficiency (as determined by the primacy agency), systems will be required to include contact information to obtain a translated copy of the CCR or assistance in the appropriate language. For systems that have difficulty providing translation support, the primacy agencies are expected to provide contact information to assist LEP consumers. In addition, EPA is proposing to require that large community water systems serving 100,000 or more persons develop a plan describing how they intend to provide meaningful access to the LEP consumers they serve. These systems serve almost 50 percent of the population and several of these larger systems already provide translation resources to their consumers. All systems that receive Federal financial assistance are subject to the requirements of Title VI to provide meaningful access to limited English proficient consumers. Large community water systems may use tools such as the latest census data for the area served, data from school systems, or data from community organizations or from state and local governments to help identify LEP populations in their service area. These systems will need to include with their annual delivery certifications to their primacy agencies that they have evaluated and updated the plan as necessary to meet community needs.

For primacy agencies and systems that are recipients of Federal funding, EPA’s existing Title VI Guidance promotes balancing community needs

with available resources and allows considerable flexibility in how CWSs provide meaningful access by applying a flexible and fact-dependent individualized assessment that balances the following four factors: (1) the number or proportion of LEP persons eligible to be served or likely to be encountered by the program or grantee; (2) the frequency with which LEP individuals come in contact with the program; (3) the nature and importance of the program, activity, or service provided by the program to people's lives; and (4) the resources available to the grantee/recipient and costs. Community Water Systems that serve LEP persons on an unpredictable or infrequent basis should use the above four-factor analysis to determine what to do if an LEP individual seeks translation support services from the relevant CWS. There are steps that the Federal government can take to help primacy agencies reduce the costs of language services without sacrificing meaningful access for LEP persons. EPA will consider opportunities to share tools, resources, and guidance, such as model notification plans, examples of best practices, and cost-saving approaches, with water systems, recipient states, and LEP consumers. EPA is requesting comment on how CWSs and primacy agencies can best provide meaningful access to LEP customers and what the timeline for providing translation services to LEP customers should look like.

In EPA's charge to the NDWAC, EPA sought advice and recommendations from the NDWAC on addressing accessibility challenges in the Consumer Confidence Report Rule Revision (NDWAC, 2021). The NDWAC recognized that the specific needs of communities served by water systems vary greatly from water system to water system. The NDWAC members recognized that water systems may have customers with unique needs with respect to accessibility. For example, some customers may need large font copies of the CCR. In this rule, EPA is proposing that systems must make a reasonable effort to meet the needs of consumers that request accessibility accommodations.

E. Improving Accuracy and Risk Communication

AWIA amended Section 1414 of the Safe Drinking Water Act to require EPA to revise the Consumer Confidence Report Rule to increase the accuracy of information and risk communication presented in the CCR. EPA is proposing to prohibit misleading statements by CWSs and improve risk communication

by simplifying overly technical and confusing language.

1. Misleading Statements

Even though tap water delivered by most community water systems meets the stringent national primary drinking water regulations, systems sometimes experience problems resulting in contamination or loss in pressure that impact water quality. In addition, drinking water that is not properly treated or that travels through an improperly maintained distribution system (pipes) may also create conditions that increase risk of contamination.

EPA is proposing to prohibit water systems from including false or misleading statements in their CCRs. CCRs are intended to provide consumers, especially those with special health needs, with information they can use to make informed decisions regarding their drinking water. To make informed decisions, consumers need accurate, nuanced reports. Feedback received during the stakeholder engagement for this proposed rule indicated concern that some CCRs have misleading images and statements about the safety of the water that may not be supported by the contaminant data or other information in the reports. For example, stating the water is "safe" may not accurately reflect the safety of the water for sensitive populations, such as people with weakened immune systems, potential lead in drinking water exposure, or other inherent uncertainties and variabilities in the system, such as the potential presence of unregulated contaminants or fluctuation in water chemistry. EPA believes that consumers would benefit from messages tailored to the system and community to reflect local circumstances, that also acknowledge that water quality may fluctuate within the system, or may impact some populations differently, for example, children, immunocompromised, pregnant people, etc. The agency plans to support states and community water systems with tools and resources, such as templates and example language that improve risk communication without misleading consumers or undermining the public trust in drinking water.

2. Primacy Agency Approval for Revising Certain CCR Explanation

Consistent with the intent of the original CCR Rule, EPA believes that water systems should have the flexibility to tailor the information in their CCRs to reflect local circumstances. For the required

additional health information on lead, arsenic, and nitrate in § 141.154, systems currently may write their own educational statements in consultation with their primacy agency. EPA is proposing to extend this type of flexibility to specific new definitions in § 141.153(c)(5) (*i.e.*, *parts per million*, *parts per billion*, *parts per trillion*, *pesticide*, and *herbicide*); a new requirement for systems to include an explanatory statement with UCMR results in § 141.153(d)(7); and descriptions of assessments required under the Revised Total Coliform Rule (RTCR) in § 141.153(h)(7). To ensure consumers are receiving material that appropriately reflects water quality and potential health risks, EPA is proposing that systems may use the language provided in the CCR Rule, or they may develop their own language, but they will need approval by the primacy agency.

3. Improving Risk Communication

AWIA Section 2008 (SDWA Section 1414(c)(4)(F)(i)(I)(bb)) requires EPA to revise the Consumer Confidence Report Rule to increase the risk communication in the reports. EPA has received general feedback from consumers during pre-proposal outreach that the CCRs can be confusing, overly technical, and in certain circumstances unnecessarily alarming to some readers.

The NDWAC also made several recommendations that EPA agrees would improve risk communication. Specifically, the NDWAC recommended revising, simplifying, and clarifying language in § 141.154. EPA is proposing revisions to § 141.154(b) and 141.154(c) as part of this proposed rule. Some of these recommendations from NDWAC, such as communicating numbers and standards, may be better addressed through implementation than through rulemaking because of the need for flexibility to address specific circumstances. For example, EPA can offer tools and resources to provide examples of analogies to better convey the meaning of concentrations and units, or infographics to communicate units of measurements and potential risk, that would be more meaningful to consumers. Implementation approaches such as these allow CWSs to select from a suite of potential examples rather than forcing all CWSs to use identical approaches that may not reflect the diversity of water systems and communities.

F. Report Delivery

AWIA section 2008 (SDWA Section 1414(c)(4)(F)(i)(II) and (F)(ii)) requires EPA to revise delivery frequency and

format in the Consumer Confidence Report Rule Revisions. Systems serving more than 10,000 people will need to provide CCRs twice per year, or biannually. In addition, by adopting the option of electronic CCR delivery, AWIA emphasizes the importance of continuing to find effective ways to keep the public informed (*See* 164 Cong. Rec. H8184, H8226 (daily ed. September 13, 2018)). In today's modern society, many people receive information through sharing from trusted sources. In this rule, EPA is proposing to incorporate standard distribution language, similar to requirements in § 141.205(d)(3) of the Public Notification Rule, to encourage broader distribution of the reports.

1. Biannual Delivery

AWIA Section 2008 (SDWA Section 1414(c)(4)(F)(i)(II)) mandates that the Consumer Confidence Report Rule Revisions require community water systems serving 10,000 or more persons to provide CCRs to customers twice per year (biannually). This would affect slightly fewer than 5,000 water systems. A community water system that sells water (also known as a wholesaler) to another community water system (also known as a purchaser or consecutive system) that is required to provide reports biannually according to § 141.155 must provide the applicable information required by October 1, 2025, and annually thereafter, or a date mutually agreed upon by the seller and the purchaser, included in a contract between the parties. Systems currently are required to provide a CCR to each customer annually by July 1st of each year that contains information and data collected during the previous calendar year. EPA is proposing that systems serving 10,000 or more persons deliver a second CCR between July 2nd and December 31st of each year.

EPA is proposing that the report delivered by July 1st continue to contain information and data collected during the previous calendar year. The second report delivered by December 31st will include a 6-month update, if applicable, based on information and data collected between January 1st and June 30th of the current calendar year. EPA is proposing to allow a system without a violation or an ALE, or for which no new information is available for the six-month period between reports (*i.e.*, information between January and June of the current year) to resend the original annual report (summarizing January through December of the previous calendar year). However, a system that has a violation, an ALE, or new information between January and

June, such as newly available results for Unregulated Contaminant Monitoring Rule from the reporting year, will need to include this information in a 6-month update that accompanies the original annual report (summarizing January through December of the previous calendar year) they deliver between July 2nd and December 31st. Providing an update to reflect any new violations, ALEs, or information generated between January through June of the current year will provide consumers up-to-date information about the safety of their drinking water, without adding additional burden for most water systems.

EPA believes these changes will meet Congress' intent of providing critical updates on a timelier basis, while minimizing burden by only requiring a subset of community water systems to provide an update with the biannually delivered reports. EPA is requesting comments on delivery timing in Section IV of this preamble.

2. Electronic Delivery

As part of the Consumer Confidence Report Rule Revisions, SDWA Section 1414(c)(4)(F)(ii) requires EPA to "allow delivery consistent with methods described in the memorandum "*Safe Drinking Water Act—Consumer Confidence Report Rule Delivery Options*" issued by the Environmental Protection Agency on January 3, 2013" (USEPA, 2013). In the House Report accompanying the AWIA 2018, the Committee on Energy and Commerce noted that Americans are increasingly moving away from a paper-driven society and instead relying on electronic technologies to access data, including real-time information; however, they also recognized that "not all persons have access to or are comfortable using these means and [intend] that this new option not be used as an opportunity to avoid making paper copies available to those customers that want them." H.R. Rep. No. 115–380, at 27 (2017).

These are not new concerns. In 2013, EPA issued the *Safe Drinking Water Act—Consumer Confidence Report Rule Delivery Options* memorandum to improve the effectiveness of communicating drinking water information to the public, while lowering the burden on community water systems and primacy agencies by taking advantage of these newer forms of communication. The memorandum includes an attachment entitled *Consumer Confidence Report Electronic Delivery Options and Considerations* (USEPA, 2013). The memorandum interprets the existing rule language "mail or otherwise directly deliver" to

allow a variety of forms of delivery of the CCR, including electronic delivery, so long as the CWS is providing the report directly to each customer. The memorandum outlines a framework for what forms of electronic delivery are and are not acceptable under the original Consumer Confidence Report Rule.

In the Delivery Options policy memorandum, EPA identified two different approaches allowable under the current rule that a CWS could use in providing electronic delivery of CCRs to its bill-paying customers: (1) paper CCR delivery with a customer option to request an electronic CCR, or (2) electronic CCR delivery with a customer option to request a paper CCR. The memorandum also noted that community water systems should consider a combination of delivery methods for their CCRs based on available technology and the preferences of their customer base.

In § 141.155(a) of this proposed rule, consistent with statute, and the 2013 guidance and current practices, EPA is proposing to include options that allow community water systems to use electronic CCR delivery, with an option for customers to request a paper CCR. If a community water system is aware of a customer's inability to receive a CCR by the chosen electronic means, it must provide the CCR by an alternative means. Consistent with the 2013 delivery options memo, EPA is proposing that systems may mail a notification that the report is available on a website via a direct link; or email a direct link or electronic version of the report. When the community water system chooses to provide a link to the report, the notification must prominently display the link and include an explanation of the nature of the link. Links for CCRs must be active at time of delivery to prevent confusing customers. Systems that use a web page to convey the CCR must include all the required information in §§ 141.153, 141.154, and 141.156 so that the customer does not have to navigate to another web page to find any required CCR content. This proposed rule also incorporates the NDWAC's recommendation to require systems that post their CCR on a publicly accessible website to maintain a report on the website for three years following its issuance. This is consistent with existing record keeping requirements for community water systems in § 141.155(h).

While EPA encourages systems to use multiple outreach methods to enhance "good faith delivery" of the reports to

consumers who do not get water bills, the use of social media directed at bill-paying customers would not meet the requirement to “directly deliver” the report since these are membership internet outlets and would require a customer to join the website to read their CCR. The use of automated phone calls (e.g., emergency telephone notification systems) to distribute CCRs is not considered direct delivery, because the entire content of the CCR cannot be provided in the telephone call.

3. Good Faith Delivery

The proposed rule incorporates the NDWAC’s recommendations by expanding examples of “good faith” delivery methods to include mailing postcards to service addresses and/or postal addresses, holding public forums, sending alert text messages with a link to the CCR to interested consumers, and using a “Quick Response” code, also known as a QR code, or equivalent in posting materials. A QR code is a type of bar code that may be read by an imaging device such as a smart phone’s camera.

G. Compliance Monitoring Data (CMD)

Primacy agencies are required under § 142.14 to maintain records to determine compliance with NPDWRs, including monitoring data. EPA is proposing that primacy agencies report CMD to EPA annually. The CMD that primacy agencies would annually report to EPA under this proposed rule is data that primacy agencies are already receiving from all water systems regulated by the PWSS program under § 142.14.

The method of delivering the CMD to EPA is up to the primacy agency. To minimize the primacy agency reporting burden, the primacy agency could:

(1) Use EPA’s Safe Drinking Water Information System (SDWIS) State Data Extraction Tool

(2) Submit a database extract and share data documentation

For the first method mentioned above, use of EPA’s SDWIS State Data Extraction Tool, EPA currently provides states with a SDWIS Data Extraction Tool for state sharing of CMD with EPA for the Six-Year Review of Drinking Water Standards. For the 42 states that use SDWIS State, the Data Extraction Tool extracts CMD from the state’s SDWIS State database and packages it in a file that can be submitted to EPA. Prior to the implementation date for annual CMD sharing, utilizing EPA-state workgroup requirements input and testing, EPA will enhance the Data Extraction Tool to allow primacy

agencies to automatically extract and submit the CMD to EPA that would be required under this rule.

For the second method mentioned above, primacy agencies could submit to EPA a database extract and share data documentation that describes the data structure and element definitions. EPA expects this method to be used by the eight states, five territories, and one tribe with PWSS program primacy that do not currently use SDWIS State.

H. Special State Primacy Requirements and Rationale

1. What are the requirements for primacy?

EPA’s requirements for primacy include authority to require community water systems to provide CCRs. 40 CFR 142.10(b)(c)(vii). Each state, tribe or territory with primacy must submit complete and final requests for EPA approval of program revisions to adopt new or revised Federal regulations, such as this rule, no later than two years after the final rule is published in the **Federal Register**; primacy agencies may request an extension of up to two years in certain circumstances. 40 CFR 142.12(b). This section describes the proposed regulations and other procedures and policies that states would need to adopt, or have in place, to implement the Consumer Confidence Report Rule Revisions following publication of the final rule, while continuing to meet all other conditions of primacy in 40 CFR part 142.

2. What are the special primacy requirements?

As discussed in Section III.D.3 of this preamble, EPA is proposing to require states with primacy to provide meaningful access to CCRs for limited English proficiency (LEP) consumers, consistent with the Guidance to Environmental Protection Agency Financial Assistance Recipients Regarding Title VI Prohibition Against National Origin Discrimination Affecting Limited English Proficient Persons (69 FR 35602, June 25, 2004). As part of their primacy application in 142.16(f), states will need to include a description of how they intend to provide support for systems who are unable to provide the required translation assistance and LEP drinking water consumers that need translation assistance to meet the proposed requirements in 40 CFR 141.153(h)(6). Primacy agencies will also be required to maintain copies of translation support plans from large systems for 5 years. In addition, even though the mailing waiver is not a new

requirement, EPA is proposing that states submit with their primacy application a description of how the state implements provisions in 40 CFR 141.155(g).

As discussed in Section III.H of this preamble, EPA is also proposing to require that states, territories, and tribes with primacy over PWSs submit all CMD collected from the PWSs. EPA proposes revisions to the primacy requirements for annual reporting to EPA by states (40 CFR 142.15) to include all monitoring and related data for determining compliance for existing NPDWRs that is required by 40 CFR part 141 to be reported from a water system to the state to demonstrate compliance with national primary drinking water regulations.

I. Housekeeping

As part of the Consumer Confidence Report Rule Revisions, EPA is proposing minor technical corrections within subsections of 40 CFR part 141, subpart O—Consumer Confidence Reports, described below:

- 40 CFR 141.152 Effective dates

EPA proposes to revise language in *CFR 141.152 Effective dates*, by removing compliance dates which have passed or are no longer applicable.

- 40 CFR 141.153 Content of the reports

EPA proposes to revise language in *CFR 141.153 Content of the reports*, by removing regulatory text that has been superseded by new or existing regulations and removing compliance dates which have passed or are no longer applicable.

- 40 CFR 141.154 Required additional health information

EPA proposes to revise language in *CFR 141.154 Required additional health information*, by removing regulatory text that has been superseded by new or existing regulations and removing compliance dates which have passed or are no longer applicable.

The minor technical corrections being proposed in this rule will ensure consistency between the Consumer Confidence Report Rule Revisions and existing EPA drinking water regulations. EPA is not creating any new obligations with these technical corrections.

IV. Request for Public Comment

EPA is requesting comments on all aspects of the proposed revisions described in this document. While all comments relevant to the Consumer Confidence Report Rule Revisions and CMD collection proposed in this document will be considered by EPA, comments on the following issues will

be especially helpful to EPA in developing a final rule.

A. General Matters Concerning Consumer Confidence Reports

EPA is requesting comment on what information should be included in the CCR summary in 40 CFR 141.156. What specific additional information will increase the readability, clarity, and understandability of the reports? What information is most important to provide to consumers at the beginning of the reports, understanding that a summary may be the only information that some consumers read?

EPA is requesting comment on how to increase accessibility to the CCR for consumers with specific needs and what challenges those consumers may face with the current and proposed delivery options in 40 CFR 141.155. Are there any best management practices on accessibility that EPA should require in the Consumer Confidence Report Rule Revisions? Are there additional state guidelines that EPA could consider in the Consumer Confidence Report Rule Revisions or in guidance to help states and systems increase accessibility?

Current regulations require that public water systems make a good faith effort to provide the CCR to non-bill paying customers in 40 CFR 155(b). EPA is requesting comment on how to improve delivery of the CCR to non-bill paying customers, such as apartment residents. Should EPA consider additional outreach requirements to enhance awareness for non-bill paying customers? Would a requirement for water systems to post information on social media or online list-serves increase consumers awareness of and access to CCRs?

EPA is requesting comment on the feasibility of lowering the threshold for systems that are required to post their CCR on the internet in 40 CFR 141.155(f). Currently community water systems that serve 100,000 customers or more are required to post their CCR on the internet. EPA is considering lowering that threshold to include systems that serve 75,000 or more customers, 50,000 or more customers, or a different threshold. EPA is also interested in better understanding what challenges this new requirement may pose to smaller public water systems.

EPA is requesting comment on the feasibility for systems and states with primary enforcement responsibility to implement the revised CCR Rule by the proposed compliance date in 2025. EPA recognizes that the revisions to improve the readability, understandability, and clarity of the CCRs is valuable to consumers. However, unlike when

promulgating the original CCR rule, states have existing CCR regulations. Should EPA consider revising effective dates in § 141.152(a) as follows:

Community water systems in States with primacy for the public water system supervision (PWSS) program must comply with the requirements in this subpart no later than [DATE 2 YEARS AFTER PUBLICATION DATE OF FINAL RULE] or on the date the State-adopted rule becomes effective, whichever comes first. Community water systems in jurisdictions where EPA directly implements the PWSS program must comply with the requirements in this subpart on April 1, 2025. Prior to these dates, public water systems must continue to comply with the CCR requirements in this subpart as codified on July 1, 2023.

B. Timing of Consumer Confidence Reports

EPA requests comment on the timing and the delivery dates proposed in the Consumer Confidence Report Rule Revisions in 40 CFR 141.155(j). Per the AWIA amendments, community water systems who serve 10,000 or more customers will be required to deliver the CCR biannually (twice per year). Should EPA require water systems to deliver the first report sooner in the year, for example by April 1st and deliver the second report by October 1st of each year, and why or why not? EPA is requesting comments on the feasibility of delivering the first report earlier in the year, such as by April 1st. Should the deadline to deliver the second report be 3 months or 6 months after delivering the first report, or some other length of time? Should EPA require that each report cover the previous 6 months, rather than provide an annual summary and why or why not? For systems serving less than 10,000 consumers, should the original delivery deadline (by July 1st) remain, or should the CCR delivery deadline be updated to reflect the first delivery deadline for large systems (serving 10,000 or more people), if revised from July 1st following consideration of public comments?

EPA is requesting comment on the proposed revisions to the time period during which community water systems must certify delivery of the CCR in 141.155(c). Currently water systems must certify delivery of the CCR within 90 days of mailing the report, or by October 1st. Would requiring water systems to certify delivery of the CCR at the same time the CCR is distributed create any benefits or challenges? Would requiring public water systems to certify delivery of the CCR within 10 days or 30 days of delivery create any benefits or challenges? Are there

additional delivery certification dates EPA should consider?

C. Increasing Readability, Clarity, and Understandability of the Consumer Confidence Report

EPA is requesting comment on how to improve the readability, clarity, and understandability of the CCRs, especially with respect to how information on detected contaminants is presented in the CCR and any challenges community water systems face with presenting detected contaminants in 40 CFR 141.153. Are there revisions to the regulations that EPA could make that would allow for detected contaminants to be presented in a clearer and more concise manner?

EPA is requesting comment on how to improve the readability, clarity, and understandability of the information presented in 40 CFR 141.153(h)(1) that describes contaminants which may reasonably be expected to be found in drinking water, including bottled water. What revisions could EPA incorporate into the Consumer Confidence Report Rule Revisions that could make it easier for consumers to understand what contaminants may reasonably be expected to be present in drinking water, including bottled water, and what the health effects of those contaminants might be?

EPA is requesting comment on how to improve the readability, clarity, and understandability of the information required by the Consumer Confidence Report Rule Revisions in § 141.154 if a public water system detects arsenic at levels above half the maximum contaminant level (MCL), or 0.005 mg/L, but less than the MCL, (0.010 mg/L) and nitrate at levels above half the MCL, or 5 mg/L, but less than the MCL of 10 mg/L. How can EPA revise these educational statements for nitrate and arsenic to improve the risk communication for consumers when detections are elevated, but do not exceed the MCL?

EPA is requesting comment on how primacy agencies can best provide meaningful access to Limited English Proficient (LEP) customers and consumers in 40 CFR 142.16. How can primacy agencies best provide translation support to LEP customers and consumers so that they can better understand the information presented in the CCR? Some ideas for primacy agencies to provide meaningful access to LEP customers and consumers include providing a translation support hotline or having staff that can provide translation services. Additionally, EPA is requesting comment on what the timeline for providing translation

services to LEP customers should look like. How soon should a primacy agency be expected to provide translation services for CCRs to a LEP customer?

D. Corrosion Control and Action Level Exceedances

EPA is requesting comment on what information consumers would find most helpful in the CCR when a public water system identifies the actions being taken to address corrosion control efforts (40 CFR 141.153(h)(8)(iii)) or when a system is required to identify an action level exceedance (ALE) and describe any corrective actions the system has or will take (40 CFR 141.153(d)(8)). How can this information be presented so that consumers can understand what these actions will accomplish and why they're important? Should the regulation include either required or optional template language to identify an ALE? Example template language could be:

During the past year, our system exceeded the [lead or copper] action level, which means our system is taking corrective actions to minimize exposures to [lead or copper] in drinking water. Our system [include the following statements most relevant: is conducting a corrosion control study; is installing corrosion control treatment or re-optimizing its existing treatment; (is replacing or will replace) lead service lines (LSL); is monitoring source water quality to determine if source water treatment is necessary to reduce lead (and/or copper) levels at the water source; and/or is conducting public education, including on how to reduce your exposure to lead. There is no safe level of lead.].

Should the regulation include either required or optional template language

to describe corrosion control efforts? Example template language could be:

To minimize exposures to lead and copper in drinking water, our system (include one or more as appropriate) [regularly monitors lead, copper and/or corrosion control-related parameters in drinking water at selected households to evaluate treatment effectiveness; regularly treats source water for lead and copper; follows state approved treatment methods of the source water; follows state approved corrosion control treatment methods; and/or is conducting a study to identify corrosion control treatments].

E. General Matters Concerning CMD Requirements

EPA would appreciate specific suggestions and comments on the following areas related to the proposed rule in 40 CFR 142.15 for annual EPA collection of compliance monitoring data from primacy agencies:

- (1) Methods for limiting burden on primacy agencies as a result of the proposed requirement to report CMD to EPA, and
- (2) EPA and primacy agency partnerships and roles for assuring high quality compliance monitoring data.

V. Cost of the Rule

A. Estimates of the Total Annualized Cost of the Proposed Rule Revisions

EPA estimates the total average annual cost of this action would be \$22.2 million. The estimated costs for the CCR Rule Revisions include those incurred by primacy agencies and community water systems. EPA categorized the costs into three categories: program costs, CCR production costs, and CMD reporting

costs. EPA discusses the expected costs as well as documenting the assumptions and data sources used in preparation of this estimate in the Analysis of the Economic Impacts of the Proposed Consumer Confidence Reports Rule Revisions (USEPA, 2022e).

Estimated costs for the proposed CCR Rule Revision are heavily influenced by the following proposed requirements:

- CWSs serving 10,000 or more persons would provide two reports per year.
- All reports would include a report summary.
- Large systems serving 100,000 persons or more would be required to identify plans for providing meaningful access to the reports for consumers with limited English proficiency.
- All CWSs would provide new language explaining their corrosion control procedures and describe corrective actions they have taken to address any lead action level exceedances (ALE) that occurred in the system during the reporting year.
- Primacy agencies would report compliance monitoring data (CMD) to EPA.

Exhibit 1 of this preamble details the EPA estimated annual average national costs using a three and seven percent discount rate by major cost component. These numbers transform future anticipated costs associated with the proposed revised CCR rule requirements in the present value. The annualized cost for each category of cost, shown in Exhibit 1 is equal to the amortized present values of the costs in each category over the 25 years from the year of rule promulgation, 2024 to 2048.

EXHIBIT 1—ANNUALIZED COSTS OF ALTERNATIVE SECOND REPORT DELIVERY OPTIONS AT 3 AND 7 PERCENT DISCOUNT RATE

Cost component	Primacy agencies	Community water systems	Total
3% Discount Rate			
Program Costs	\$2,935,450	\$202,008	\$3,137,458
CCR Cost	1,723,115	17,300,670	19,023,785
Compliance Monitoring	67,254	0	67,254
Total	4,725,819	17,502,679	22,228,497
7% Discount Rate			
Program Costs	2,837,294	285,213	3,122,507
CCR Cost	1,723,540	17,035,740	18,759,280
Compliance Monitoring	67,842	0	67,842
Total	4,628,677	17,320,953	21,949,630

Additional details regarding EPA's cost assumptions and estimates can be found in the Draft Information

Collection Request (ICR) (USEPA, 2022g), ICR Number 2764.01, which presents estimated cost and labor hours

for the CCR Rule Revisions. Copies of the Draft ICR may be obtained from the EPA public docket for this proposed

rule, under Docket ID No. EPA-HQ-OW-2022-0260.

B. Revisions to Consumer Confidence Report

1. Program and Administrative Costs

“Program costs” refers to the actions primacy agencies will take to adapt their respective CCR programs. They include upfront program costs associated with revising their program and applying for primacy as well as ongoing costs associated with program maintenance. “Administrative” costs refer to CWS expenditures to prepare for the new CCR requirements. EPA estimates that upfront and ongoing program costs for primacy agencies and the upfront administrative costs to CWSs depend on the role the primacy agency plays in the CCR development process. EPA grouped primacy agencies into three categories based on the level of support they provide in the development of CCRs.

2. Ongoing Program Cost Burden Estimation

After adopting the rule revision, primacy agencies, including EPA regions that have primacy for the PWSS program in Wyoming, District of Columbia, and American Indian PWSs, incur costs on an ongoing basis to administer the rule. In the case of the CCR Revisions, each primacy agency will collect and review data annually to determine which CWSs will have additional reporting requirements, *i.e.*, biannual delivery and translation. EPA assumed that primacy agencies will not incur general program maintenance activities (such as ongoing staff training) because they already conduct those activities under the original rule. Similarly, EPA assumed ongoing administrative costs for CWSs will be zero because CWS already perform ongoing program administrative activities for the original CCR Rule.

3. Community Water System Administrative Costs

EPA assumed that CWSs will incur upfront administrative costs not directly related to the production of CCRs. These costs include reviewing training materials received from primacy agencies and training staff to produce CCRs in compliance with the rule revisions. EPA assumed ongoing administrative costs for CWSs will be zero because CWS already perform ongoing program administrative activities for the original CCR Rule. EPA assumed that upfront administrative costs for CWSs will depend on the level of assistance the primacy agency

provides to CWSs in the development of their CCRs.

4. Costs To Revise the Consumer Confidence Report

The proposed rule will require CWSs incorporate new content requirements in their CCRs. EPA also estimated the costs for primacy agencies that provide support to CWS to comply with new CCR requirements. For purposes of cost modeling, “CCR production costs” refer to the burden that CWSs, and primacy agencies that support CWSs, would incur because of content changes and delivery changes to the CCR. These changes include:

- Costs of providing access to the CCR to populations with limited English proficiency
- Costs of developing a summary page for the CCR
- Costs of developing corrosion control language and descriptions of corrective actions following an ALE (if applicable) for the CCR
- Costs of providing a second CCR each year for CWSs serving 10,000 or more people

C. Compliance Monitoring Data (CMD) Costs

As part of the CCR revisions, EPA is proposing to collect CMD from primacy agencies on an annual basis. EPA estimated that the change will require updates to 66 “data systems” reporting CMD. These include data systems for 49 states, five territories, the Navajo Nation, nine direct implementation tribal programs (as EPA Regions), DC (as EPA Region 3), and Wyoming (as EPA Region 8). The cost estimate includes the upfront costs associated with setting up and running the software necessary to extract the CMD for the first time, and ongoing costs associated with subsequent data extraction and submittals.

To capture this difference more accurately in costs, EPA assigned reporting agencies to two data system categories:

- *Reporting agencies that use SDWIS State:* 48.
- *Reporting agencies that do not use SDWIS State:* 18.

1. Upfront Costs

Before adopting the CMD reporting provisions of the CCR Rule Revisions, reporting agencies must first adjust their existing programs to support its implementation or develop a new program to do so. These upfront costs include staff training and setting up a reporting system. That is, reporting agencies that currently use SDWIS State

will have a lower level of effort (LOE) burden than those that do not currently use SDWIS State.

2. Ongoing Costs

After adopting the CMD reporting provisions of the Consumer Confidence Report Rule Revisions, primacy agencies, including EPA regions that have primacy for the PWSS program in Wyoming, DC, and American Indian PWSs, will incur costs on an ongoing basis to report CMD to EPA. Specifically, each reporting agency will need resources to maintain their reporting systems.

D. Qualitative Benefits

The effects of the revisions to the CCR are difficult to quantify, however,

EPA anticipated that the primary benefit of the proposed Revised CCR Rule is that the public will be more informed, given the following reasons: increased accessibility for Limited English proficiency consumers; improved readability by allowing CWSs the flexibility to present contaminant data in a more consumer-friendly format; enhanced clarity by including report summaries at the beginning of the report; improved accuracy by prohibiting false or misleading statements in their reports; expanded communication related to lead by including corrosion control efforts and corrective actions being taken following an action level exceedance (ALE); increased frequency of delivery by large systems; added delivery method options; and enhanced transparency for the public and EPA oversight as a result of collecting comprehensive CMD from primacy agencies.

Together, these changes will lead to better-informed consumers. A more informed public is better equipped to make decisions about their health, including when deciding whether to use water filters or to use bottled water to bottle-feed infants. A more informed public may also be more likely to engage in the decision-making process with their local water system. When a drinking water consumer has more information and a better understanding, their confidence can increase, consequently building their trust in their CWS. This is especially critical given that many CWSs choose to use the CCRs as a communication piece with their consumers to inform them about other relevant issues for the system.

VI. Statutory and Executive Order Reviews

A. Executive Order 12866: Regulatory Planning and Review and Executive Order 13563: Improving Regulation and Regulatory Review

This action is a non-significant regulatory action. EPA prepared an analysis of the potential costs and benefits associated with this action. This analysis, the Economic Analysis of the Proposed Consumer Confidence Report Rule Revisions, is available in the docket and is summarized in Section V of this preamble.

B. Paperwork Reduction Act

The information collection activities in this proposed rule have been submitted for approval to the Office of Management and Budget (OMB) under the Paperwork Reduction Act (PRA). The Information Collection Request (ICR) document that EPA prepared has been assigned the Agency's ICR number 2764.01. You can find a copy of the ICR in the docket for this rule, and it is briefly summarized here. The major information requirements concern public water system (PWS), primacy agency, and laboratory activities to implement the rule including recordkeeping and reporting requirements (*i.e.*, the burden and costs for complying with drinking water information requirements that are not associated with contaminant-specific rulemakings), providing training to state and PWS employees on EPA information collection tool, updating their monitoring data systems, and reviewing system monitoring data.

This ICR provides preliminary burden and cost estimates for the Consumer Confidence Report Rule Revisions and CMD collection.

Respondents/affected entities: The respondents/affected entities are community water systems and states.

Respondent's obligation to respond: Under this proposed rule the respondent's obligation to respond is mandatory. Section 1414(c)(4) requires "each community water system to mail, or provide by electronic means, to each customer of the system at least once annually a report on the level of contaminants in the drinking water conveyed by that system" Furthermore, section 1445(a)(1)(A) of the SDWA requires that "[e]very person who is subject to any requirement of this subchapter or who is a grantee, shall establish and maintain such records, make such reports, conduct such monitoring, and provide such information as the Administrator may reasonably require by regulation to

assist the Administrator in establishing regulations under this subchapter, in determining whether such person has acted or is acting in compliance with this subchapter . . ." In addition, section 1413(a)(3) of the SDWA requires states to "keep such records and make such reports . . . as the Administrator may require by regulation."

Estimated number of respondents: Total respondents, as proposed, include 66 primacy agencies (50 states plus the District of Columbia, U.S. territories, EPA Regions conducting direct implementation of tribal primacy, and one tribal nation), 48,529 are CWSs, for a total of 48,595 respondents.

Frequency of response: The frequency of response varies across respondents and year of implementation. In the initial 3-year ICR period for the CCR Rule Revision, systems will continue to deliver reports annually until the proposed compliance date of 2025. Beginning in 2025, systems serving 10,000 or more people will be required to provide report biannually, or twice per year. Systems serving 100,000 or more will be required to submit a plan to provide meaningful access by July 1, 2025. Primacy agencies will be required to submit comprehensive compliance monitoring data to EPA beginning in 2025.

Total estimated burden: 331,967 hours (per year). Burden is defined at 5 CFR 1320.3(b).

Total estimated cost: \$22.2 million (per year), includes \$6.71 million annualized capital or operation & maintenance costs.

An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number. The OMB control numbers for EPA's regulations in 40 CFR are listed in 40 CFR part 9.

Submit your comments on the agency's need for this information, the accuracy of the provided burden estimates and any suggested methods for minimizing respondent burden to EPA using the docket identified at the beginning of this proposed rule. EPA will respond to any ICR-related comments in the final rule. You may also send your ICR-related comments to OMB's Office of Information and Regulatory Affairs using the interface at <https://www.reginfo.gov/public/do/PRAMain>. Find this particular information collection by selecting "Currently under Review—Open for Public Comments" or by using the search function. OMB must receive comments no later than June 5, 2023.

C. Regulatory Flexibility Act as Amended by the Small Business Regulatory Fairness Act

I certify that this action will not have a significant economic impact on a substantial number of small entities under the RFA. For purposes of assessing the impacts of this proposed rule on small entities, EPA considered small entities to be PWSs serving 10,000 people or fewer. This is the threshold specified by Congress in the 1996 Amendments to the SDWA for small water system flexibility provisions. As required by the Regulatory Flexibility Act (RFA), EPA proposed using this alternative definition in the **Federal Register** (FR) (63 FR 7620, February 13, 1998), sought public comment, consulted with the Small Business Administration (SBA), and finalized the small water system threshold in the agency's Consumer Confidence Report regulation (63 FR 44524, August 19, 1998). As stated in that final rule, the alternative definition is applied to this proposed regulation.

There are approximately 45,000 small entities subject to the requirements of the proposed CCR Rule Revisions that serve fewer than 10,000 people.

The agency has determined that no small entities (zero percent) will experience an impact of greater than one percent of average annual revenues. Details of this analysis are presented in the Docket (EPA-HQ-OW-2022-0260).

D. Unfunded Mandates Reform Act

This action does not contain an unfunded mandate of \$100 million or more as described in UMRA, 2 U.S.C. 1531–1538, and does not significantly or uniquely affect small governments. The action imposes minimal enforceable duties on any state, local or tribal governments or the private sector.

Based on the cost estimates detailed in Section V of this preamble, EPA determined that compliance costs in any given year would be below the threshold set in UMRA, with maximum single-year costs of approximately \$22.2 million dollars. EPA has determined that this proposed rule contains a Federal mandate that would not result in expenditures of \$100 million or more for state, local, and tribal governments, in the aggregate, or the private sector in any one year.

This rule will establish requirements that affect small community water systems. However, EPA has determined that this rule contains no regulatory requirements that might significantly or uniquely affect small governments because the regulation requires minimal expenditure of resources.

E. Executive Order 13132: Federalism

EPA has determined that this action will have minor federalism implications. It will not have substantial direct effects on the states, on the relationship between the national government and the states, or on the distribution of power and responsibilities among the various levels of government.

EPA did conclude that this proposed rule may be of interest to states because it may impose direct compliance costs on public water systems and/or primacy agencies and the Federal government will not provide the funds necessary to pay those costs. As a result of this determination, EPA held a Federalism Consultation with state and local government and partnership organizations on August 25, 2022, to allow them the opportunity to provide meaningful and timely input into its development. EPA invited the following national organizations representing state and local government and partnership organizations to participate in the consultation: the National Governors Association, National Association of Counties, National League of Cities, United States Conference of Mayors, National Conference of State Legislatures, Environmental Council of the States, Association of Metropolitan Water Agencies, American Water Works Association, Association of State Drinking Water Administrators, Association of Clean Water Administrators, Association of State and Territorial Health Officials, National Rural Water Association, National Water Resources Association, and Western States Water Council to request their input on this rulemaking.

In addition to input received during the meetings, EPA provided an opportunity to receive written input within 60 days after the initial meeting. A summary report of the views expressed during the Federalism consultation is available in the Docket.

F. Executive Order 13175: Consultation and Coordination With Indian Tribal Governments

This action has tribal implications. However, it will neither impose substantial direct compliance costs on federally recognized tribal governments, nor preempt tribal law. As described previously, the proposed CCR Rule Revision would apply to all CWS, and would require systems serving more than 10,000 people to provide reports biannually, or twice per year. Information in the SDWIS/Fed water system inventory indicates there are approximately 711 total tribal systems,

including 19 large tribal CWSs (serving more than 10,001 customers). The rule would also impact a tribal government that has primary enforcement authority (primacy) for PWSs on tribal lands.

Consistent with EPA Policy on Consultation and Coordination with Indian Tribes (May 4, 2011), EPA consulted with Tribal officials during the development of this action to gain an understanding of Tribal views of potential revisions to specific areas of the Consumer Confidence Report Rule. The start of the initial tribal consultation and coordination period began on March 14, 2022, during which a tribal consultation notification letter was mailed to tribal leaders of federally recognized tribes. During the initial consultation period EPA hosted two identical national webinars with interested tribes on March 22, 2022, and April 7, 2022, to request input and provide rulemaking information to interested parties. The close of the initial consultation period and deadline for feedback and written comments to EPA was June 14, 2022. EPA received both verbal and written comments during the two informational webinars. A summary of the CCR Rule Revisions tribal consultation and comments received is included with supporting materials in the docket (USEPA, 2022c).

Preceding the conclusion of the initial tribal consultation period, EPA began considering additional revisions to the forthcoming CCR Rule Revision that would expand the scope of the rule revision to include a requirement for primacy agencies to submit comprehensive CMD annually to the agency. However, this revision was not described during the initial consultation and coordination period. EPA identified the Navajo Nation as the lone tribal government with primacy and offered supplemental consultation and coordination with the Navajo Nation to discuss any potential impacts or concerns about how the Compliance Monitoring Data submission requirement would affect the Navajo Nation. All supplemental consultation and coordination processes were conducted in accordance with EPA Policy on Consultation and Coordination with Indian Tribes. The supplemental tribal consultation period was open from August 30, 2022, through October 14, 2022. EPA did not receive any additional comments on the proposed rule during the supplemental tribal consultation process.

G. Executive Order 13045: Protection of Children From Environmental Health and Safety Risks

Executive Order 13045 (62 FR 19885, April 23, 1997) directs federal agencies to include an evaluation of the health and safety effects of the planned regulation on children in federal health and safety standards and explain why the regulation is preferable to potentially effective and reasonably feasible alternatives. This action is not subject to Executive Order 13045 because it is not economically significant as defined in Executive Order 12866, and because the EPA does not believe the environmental health or safety risks addressed by this action present a disproportionate risk to children. The requirements in this proposed rule apply to potential health risks to all consumers and vulnerable populations and are not targeted specifically to address a disproportionate risk to children.

However, EPA's Policy on Children's Health may apply to this action. The proposed revisions to the CCR Rule would continue to address risks to children from contaminants in drinking water by informing parents and guardians and will strengthen EPA oversight of public water systems by requiring the submittal of compliance monitoring data.

H. Executive Order 13211: Actions Concerning Regulations That Significantly Affect Energy Supply, Distribution or Use

This action is not a "significant energy action" because it is not likely to have a significant adverse effect on the supply, distribution or use of energy and has not otherwise been designated by the Administrator of the Office of Information and Regulatory Affairs as a significant energy action. The entities affected by this action do not, as a rule, generate power. This action does not regulate any aspect of energy distribution as the water systems and states, territories, and tribal agencies that are proposed to be regulated by this rule already have electrical service. As such, EPA does not anticipate that this rule will have a significant adverse effect on the supply, distribution, or use of energy.

I. National Technology Transfer and Advancement Act

Under section 12(d) of the National Technology Transfer and Advancement Act, the agency is required to use voluntary consensus standards in its regulatory and procurement activities unless to do so would be inconsistent

with applicable law or otherwise impractical. Voluntary consensus standards are technical standards (*e.g.*, materials specifications, test methods, sampling procedures, business practices, etc.) which are developed or adopted by voluntary consensus standard bodies. Where available and potentially applicable voluntary consensus standards are not used by EPA, the Act requires the agency to provide Congress, through the Office of Management and Budget, an explanation of the reasons for not using such standards. Because this proposal does not involve or require the use of any technical standards, EPA does not believe that this Act is applicable to this rule. Moreover, EPA is unaware of any voluntary consensus standards relevant to this rulemaking. Therefore, even if the Act were applicable to this kind of rulemaking, EPA does not believe that there are any “available or potentially applicable” voluntary consensus standards.

J. Executive Order 12898: Federal Actions To Address Environmental Justice in Minority Populations and Low-Income Populations

Executive Order 12898 (59 FR 7629, February 16, 1994) directs Federal agencies, to the greatest extent practicable and permitted by law, to make environmental justice part of their mission by identifying and addressing, as appropriate, disproportionately high and adverse human health or environmental effects of their programs, policies, and activities on minority populations (people of color and/or Indigenous peoples) and low-income populations.

EPA believes that the human health or environmental conditions that exist prior to this action have the potential to result in disproportionate and adverse human health or environmental effects on people of color, low-income populations and/or Indigenous peoples. EPA believes that this action is likely to reduce existing disproportionate and adverse effects on people of color, low-income populations and/or Indigenous peoples by increasing the availability of drinking water compliance data to the public, improving delivery options of CCRs for non-bill paying customers and improving the ability of limited English proficiency (LEP) customers to access translation support in order to understand the information in their reports. Improved access to critical information in CCRs can also encourage these consumers to become more involved in decisions which may affect their health and promote dialogue

between consumers and their drinking water utilities.

CCRs are communication tools used by water systems to provide consumers information about drinking water quality, including, but not limited to, detected contaminants and violations. In enacting AWIA of 2018, Congress recognized that EPA needed to improve the availability and understandability of information contained in CCRs. Members of many underserved communities may be renters, making them less likely to receive the same CCR information that bill-paying customers who own their homes receive through direct delivery. Based on 2021 Census information (U.S. Census Bureau, 2021a), households who rent are much more likely to be below the poverty level than households who own their homes. Often renters do not receive copies of the CCR, as these reports are often delivered by CWSs to the billing address on file for these communities, which is often a central management office or property owner. While these systems are required to make a “good faith effort” to deliver CCRs to non-bill paying customers, often times the reports are not distributed to all community members. At the NDWAC meeting on September 30, 2021, members specifically expressed their concern about non-bill paying customers not receiving the CCR (NDWAC, 2021).

EPA is considering options to expand the existing language in the rule at 40 CFR 144.155(b) for “good faith” delivery methods to include examples of more modern outreach efforts, such as social media options. EPA is also requesting comment in the rule on how to improve delivery of the CCR to non-bill paying customers and whether EPA should consider additional outreach requirements to enhance awareness for non-bill paying customers, such as requiring landlords to deliver postcards that alert them when CCRs are available.

In addition to CCRs being difficult for residents of some communities to access, they often contain technical language that may be particularly difficult for consumers with limited English proficiency (LEP) to understand. Based on 2021 data from the U.S. Census Bureau (U.S. Census Bureau, 2021b), people in limited English households (*i.e.*, households where no one in the household age 14 and over speaks English only or speaks English “very well”) are roughly two times as likely to be people of color as people in all other households (*i.e.*, households where at least one person in the household age 14 and over speaks English only or speaks English “very

well.”). Limited English proficiency can be a barrier to accessing and understanding the information presented in CCRs. If LEP consumers are not able to read and understand the reports, or have sufficient access to that information, it raises equity concerns that some communities may not have as complete an understanding about the quality of their drinking water as more proficient English-speaking consumers. During an interview with a consumer protection organization, the participants noted that based on their experience, members with limited English proficiency that lived in manufactured housing communities had difficulties getting translation assistance with Consumer Confidence Reports. The statement in the CCR that suggest LEP consumers should speak to someone that can help, creates a burden on the consumer to seek out translation assistance (USEPA, 2022f). See proposed changes to support LEP consumers in Section III.D in the preamble.

In developing this proposal, EPA provided meaningful involvement by engaging with a variety of stakeholders to better understand and address environmental justice concerns. This included interviewing an environmental justice organization and a consumer protection organization (USEPA, 2022f). The NDWAC CCR Rule Revisions working group consisted of twelve people from public water systems, environmental groups, public interest groups, and Federal, state, and tribal agencies, including a member from EPA’s National Environmental Justice Advisory Council. EPA specifically sought engagement with communities that have been disproportionately impacted by lead in drinking water for the LCRR, especially lower-income people and communities of color that have been underrepresented in past rule-making efforts as part of EPA’s commitment to Environmental Justice. In considering revisions to the CCR Rule, EPA reviewed comments from those meetings related to notifications and CCRs, see Section III.E of this preamble for more information. Additional information on consultations and stakeholder engagement can be found in Section II. C through E of this preamble.

The information supporting this Executive Order review is contained in Section II. C. Consultations, Section II. D. Other Stakeholder Engagement, Section II. E. Supplementary Stakeholder Engagement, Section III. D. Improving Readability, Clarity, Understandability, and 3. Translation Support for Limited English Proficient

Persons and Accessibility
Considerations of this preamble.

VII. References

- 164 Cong. Rec. H8184 (daily ed. September 13, 2018) (statement of Rep. Dingell) <https://www.congress.gov/congressional-record/volume-164/issue-153/house-section/article/H8184-4>.
- NDWAC. (December 14, 2021). [NDWAC recommendations to the U.S. Environmental Protection Agency on targeted issues related to revisions to the Consumer Confidence Report Rule].
- The White House. (2011). Executive Order 13563. Improving Regulation and Regulatory Review. **Federal Register** 76(14):3821. January 21, 2011. Washington, DC: Government Printing Office.
- U.S. House. Committee on Energy and Commerce. Drinking Water System Improvement Act of 2017. (H. Rpt. 115–380). Washington: Government Printing Office, 2017. (Y.1.1/8: 115–380).
- United States. America’s Water Infrastructure Act. 2018. Public Law 115–270, 132 Stat. 3765, Title II (October 23, 2018).
- U.S. Census Bureau. (2021a). *American Housing Survey (AHS)*. Table Creator, available at https://www.census.gov/programs-surveys/ahs/data/interactive/ahstablecreator.html?s_areas=00000&s_2021&s_tablename=TABLE9&s_bygroup1=2&s_bygroup2=1&s_filtergroup1=1&s_filtergroup2=1.
- U.S. Census Bureau. (2021b). *DP02: Selected Social Characteristics in the United States*. U.S. Census Bureau, 2016–2020 American Community Survey 5-Year Estimates. Available at: [https://data.census.gov/table?t=Language+Spoken+at+Home&g=0100000US\\$1600000&tid=ACSDP5Y2020.DP02](https://data.census.gov/table?t=Language+Spoken+at+Home&g=0100000US$1600000&tid=ACSDP5Y2020.DP02).
- US EPA. (1991). WSG 61A. U.S. Environmental Protection Agency. Memorandum to Drinking Water/ Groundwater Protection Branch Chiefs, Regions I–X, from Connie Bosma (signed by Ray Enyeart), Drinking Water Branch. Definitions of Types of Public Water Systems and Populations Served by Those Systems. (August 21, 1991).
- US EPA. (1998). National Primary Drinking Water Regulations: Consumer Confidence Reports; Final rule. **Federal Register**. 63 FR 44524. August 19, 1998.
- US EPA. (2004). Guidance to Environmental Protection Agency Financial Assistance Recipients Regarding Title VI Prohibition Against National Origin Discrimination Affecting Limited English Proficient Persons. **Federal Register**. 69 FR 35602. June 25, 2004.
- US EPA. (2009). 2006 Community Water System Survey. EPA 815–R–09–001. February 2009. <https://www.epa.gov/dwreginfo/community-water-system-survey>.
- US EPA. (2012). Consumer Confidence Report (CCR) Rule Retrospective Review Summary (EPA Publication No. EPA 816–S–12–001). U.S. Environmental Protection Agency. <https://www.epa.gov/sites/default/files/2014-05/documents/epa816s12004.pdf>.
- US EPA. (2013). WSG 189. U.S. Environmental Protection Agency. Memorandum to Water Division Directors, Regions I–X, from Peter Grevatt, Office of Ground Water & Drinking Water. Safe Drinking Water Act—Consumer Confidence Report Rule Delivery Options (January 3, 2013).
- US EPA. (2021a). Final Allotments for the FY2021 Public Water System Supervision (PWSS) State and Tribal Support Program Grants, from Catherine Davis, Office of Ground Water & Drinking Water. (March 2, 2021).
- US EPA. (2021b). Consumer Confidence Report Rule Revisions Stakeholder Engagement: Summary of LCRR Engagement. Office of Water.
- US EPA. (2021c). National Primary Drinking Water Regulations: Lead and Copper Rule Revisions; Final rule. **Federal Register**. 86 FR 4198. January 15, 2021.
- US EPA. (2022a). Drinking Water Compliance Monitoring Data Strategic Plan (EPA Publication No. EPA 810–R–19–002). U.S. Environmental Protection Agency.
- US EPA. (2022b). FY2022–FY2026 Strategic Plan. U. S. Environmental Protection Agency. <https://www.epa.gov/system/files/documents/2022-03/fy-2022-2026-epa-strategic-plan.pdf>.
- US EPA. (2022c). Summary Report on Tribal Consultation: Consumer Confidence Report Rule Revisions. Office of Water.
- US EPA. (2022d). Summary Report on Federalism: Consumer Confidence Report Rule Revisions. Office of Water.
- US EPA. (2022e). Analysis of the Economic Impacts of the Proposed Consumer Confidence Reports Rule Revisions. Office of Water.
- US EPA. (2022f). Consumer Confidence Report Rule Revisions Stakeholder Engagement: Interview Summary. Office of Water.
- US EPA. (2022g). Draft Information Collection Request for the Consumer Confidence Report Rule Revisions and Compliance Monitoring Data Collection. Office of Water.
- US EPA. (2022h). Final Allotments for the FY2022 Public Water System Supervision (PWSS) State and Tribal Support Program Grants, from Catherine Davis, Office of Ground Water & Drinking Water. (April 21, 2022).
- US GAO. (2011). Drinking Water: Unreliable State Data Limit EPA’s Ability to Target Enforcement Priorities and Communicate Water Systems’ Performance. (GAO publication No. GAO–11–381). U.S. Government Accountability Office. <https://www.gao.gov/products/gao-11-381>.

List of Subjects

40 CFR Part 142

Environmental protection, Copper, Indians—lands, Intergovernmental relations, Lead, Lead service line, National Primary Drinking Water Regulation, Reporting and

recordkeeping requirements, Water supply.

40 CFR Part 142

Environmental protection, Administrative practice and procedure, Copper, Indians—lands, Intergovernmental relations, Lead, Lead service line, National Primary Drinking Water Regulation, Reporting and recordkeeping requirements, Water supply.

Michael S. Regan,
Administrator.

For the reasons stated in the preamble, the Environmental Protection Agency proposes to amend 40 CFR parts 141 and 142 as follows:

PART 141—NATIONAL PRIMARY DRINKING WATER REGULATIONS

- 1. The authority citation for part 141 continues to read as follows:

Authority: 42 U.S.C. 300f, 300g–1, 300g–2, 300g–3, 300g–4, 300g–5, 300g–6, 300j–4, 300j–9, and 300j–11.

- 2. Amend § 141.151 by:
 - a. Revising paragraphs (a), (c), and (f); and
 - b. Adding paragraph (g).
 The revisions and additions read as follows:

§ 141.151 Purpose and applicability of this subpart.

(a) This subpart establishes the minimum requirements for the content of reports that community water systems must deliver to their customers. These reports must contain information on the quality of the water delivered by the systems and characterize the risks (if any) from exposure to contaminants detected in the drinking water in an accurate and understandable manner. This subpart also establishes minimum requirements large systems must include in plans to provide meaningful access to these reports for limited English-proficient consumers.

* * * * *

(c) For the purpose of this subpart, *customers* are defined as billing units or service connections to which water is delivered by a community water system. For the purposes of this subpart, *consumers* are defined as people served by the water system, including customers, and people that do not receive a bill.

* * * * *

(f) For purpose of this subpart, the term “primacy agency” refers to the State or tribal government entity that has jurisdiction over, and primary enforcement responsibility for, public water systems, even if that government

does not have interim or final primary enforcement responsibility for this rule. Where the State or tribe does not have primary enforcement responsibility for public water systems, the term “primacy agency” refers to the appropriate EPA regional office.

(g) The reports must not contain false or misleading statements or representations.

■ 3. Amend § 141.152 by:

- a. Revising the section heading and paragraphs (a), (b), (c), and (d)(1);
- b. Removing the period at the end of paragraph (d)(2) and adding “; and” in its place; and
- c. Adding paragraph (d)(3).

The revisions and additions read as follows:

§ 141.152 Compliance dates.

(a) Between [EFFECTIVE DATE OF FINAL RULE], and [DATE 1 YEAR AFTER PUBLICATION DATE OF FINAL RULE], community water systems must comply with §§ 141.151 through 141.155, as codified in 40 CFR part 141, subpart O, on July 1, 2023. Beginning April 1, 2025, community water systems must comply with § 141.151 through 141.156.

(b) Each existing community water system must deliver reports according to § 141.155 by July 1 each year. Each report delivered by July 1 must contain data collected during the previous calendar year, or the most recent calendar year before the previous calendar year.

(c) A new community water system must deliver its first report by July 1 of the year after its first full calendar year in operation.

(d) * * *

(1) By April 1, 2025 and annually thereafter; or

* * * * *

(3) A community water system that sells water to another community water system that is required to provide reports biannually according to § 141.155(i) must provide the applicable information required in § 141.155(j) by October 1, 2025, to the buyer system, and annually thereafter, or a date mutually agreed upon by the seller and the purchaser, included in a contract between the parties.

■ 4. Amend § 141.153 by:

- a. Revising paragraphs (a) and (b)(2);
- b. Adding paragraphs (c)(1)(iii) and (c)(3)(v);
- c. Revising paragraph (c)(4) introductory text;
- d. Adding paragraph (c)(5);
- e. Revising paragraphs (d)(1)(i) and (ii);
- f. Removing paragraph (d)(1)(iii);

- g. Revising paragraphs (d)(2), (d)(3) introductory text, (d)(3)(i), (d)(4), (d)(4)(iii) and (iv), and (d)(4)(iv)(B);
- h. Removing paragraph (d)(4)(iv)(C);
- i. Removing and reserving paragraphs (d)(4)(vii) and (viii);
- j. Revising paragraphs (d)(4)(ix) and (x);
- k. Removing paragraphs (d)(4)(xi) and (xii);
- l. Revising paragraphs (d)(5), (6), and (7);
- m. Adding paragraph (d)(8);
- n. Revising paragraphs (e)(1) introductory text, (f) introductory text, (f)(2) and (3), (h)(1)(i), (h)(1)(ii) introductory text, (h)(1)(ii)(B) and (E), (h)(1)(iii) and (iv), (h)(2) and (3);
- o. Revising paragraphs (h)(6) introductory text, (h)(6)(i) introductory text, (h)(7) introductory text, (h)(7)(i) introductory text, (h)(7)(i)(A) through (C), (h)(7)(i)(D)(1), (h)(7)(ii) introductory text, (h)(7)(ii)(A) and (B), (h)(7)(ii)(C)(2), and (h)(7)(iii)(D); and
- p. Adding paragraph (h)(8).

The revisions and additions read as follows:

§ 141.153 Content of the reports.

(a) Each community water system must provide to its customers a report(s) that contains the information specified in this section, § 141.154, and include a summary as specified in § 141.156.

(b) * * *

(2) If a source water assessment has been completed, the report must notify consumers of the availability of this information, the year it was completed or most recently updated, and the means to obtain it. In addition, systems are encouraged to highlight in the report significant sources of contamination in the source water area if they have readily available information. Where a system has received a source water assessment from the primacy agency, the report must include a brief summary of the system’s susceptibility to potential sources of contamination, using language provided by the primacy agency or written by the operator.

(c) * * *

(1)

(iii) *Contaminant*: Any physical, chemical, biological, or radiological substance or matter in water.

* * * * *

(3) * * *

(v) *Corrosion control efforts*:

Treatment (including pH adjustment, alkalinity adjustment, or corrosion inhibitor addition) or other efforts contributing to the control of the corrosivity of water, e.g., monitoring to assess the corrosivity of water.

(4) A report that contains information regarding a Level 1 or Level 2

Assessment required under Subpart Y—*Revised Total Coliform Rule* of this part must include the applicable definitions:

* * * * *

(5) Systems must use the following definitions for the terms listed below if the terms are used in the report unless the system obtains written approval from the state to use an alternate definition:

(i) *Parts per million (ppm)*: Parts per million (ppm) is a measurement of the quantity of a substance in the water. A concentration of one ppm means that there is one part of that substance for every one million parts of water.

(ii) *Parts per billion (ppb)*: Parts per billion (ppb) is a measurement of the quantity of a substance in the water. A concentration of one ppb means that there is one part of that substance for every one billion parts of water.

(iii) *Parts per trillion (ppt)*: Parts per trillion (ppt) is a measurement of the quantity of a substance in the water. A concentration of one ppt means that there is one part of that substance for every one trillion parts of water.

(iv) *Pesticide*: Generally, any substance or mixture of substances intended for preventing, destroying, repelling, or mitigating any pest.

(v) *Herbicide*: Any chemical(s) used to control undesirable vegetation.

(d) * * *

(1) * * *

(i) Contaminants subject to a MCL, action level, maximum residual disinfectant level, or treatment technique (regulated contaminants); and
(ii) Contaminants for which monitoring is required by § 141.40 (unregulated contaminants).

(2) The data relating to these contaminants must be presented in the reports in a manner that is clear and understandable for consumers. For example, the data may be displayed in one table or in several adjacent tables. Any additional monitoring results which a community water system chooses to include in its report must be displayed separately.

(3) The data must be derived from data collected to comply with EPA and State monitoring and analytical requirements during the previous calendar year, or the most recent calendar year before the previous calendar year except that:

(i) Where a system is allowed to monitor for regulated contaminants less often than once a year, the contaminant data section must include the date and results of the most recent sampling and the report must include a brief statement indicating that the data presented in the report are from the

most recent testing done in accordance with the regulations. No data older than 5 years need be included.

* * * * *

(4) For each detected regulated contaminant (listed in appendix A to this subpart), the contaminant data section(s) must contain:

* * * * *

(iii) If there is no MCL for a detected contaminant, the contaminant data section(s) must indicate that there is a treatment technique, or specify the action level, applicable to that contaminant, and the report must include the definitions for treatment technique and/or action level, as appropriate, specified in paragraph (c)(3) of this section;

(iv) For contaminants subject to an MCL, except turbidity and *E. coli*, the contaminant data section(s) must contain the highest contaminant level used to determine compliance with an NPDWR and the range of detected levels, as follows:

* * * * *

(B) When compliance with the MCL is determined by calculating a running annual average of all samples taken at a monitoring location: the highest average of any of the monitoring locations and the range of individual sample results for all monitoring locations expressed in the same units as the MCL. For the MCLs for TTHM and HAA5 in § 141.64(b)(2), systems must include the highest locational running annual average for TTHM and HAA5 and the range of individual sample results for all monitoring locations expressed in the same units as the MCL. If more than one location exceeds the TTHM or HAA5 MCL, the system must include the locational running annual averages for all locations that exceed the MCL.

* * * * *

(vii) [Reserved]

(viii) [Reserved]

(ix) The likely source(s) of detected contaminants to the best of the operator's knowledge. Specific information regarding contaminants may be available in sanitary surveys and source water assessments and should be used when available to the operator. If the operator lacks specific information on the likely source, the report must include one or more of the typical sources for that contaminant listed in appendix A to this subpart that is most applicable to the system; and

(x) For *E. coli* analytical results under subpart Y-*Revised Total Coliform Rule*: The total number of *E. coli* positive samples.

(5) If a community water system distributes water to its customers from multiple hydraulically independent distribution systems that are fed by different raw water sources, the contaminant data section(s) should differentiate contaminant data for each service area and the report should identify each separate distribution system. For example, if displayed in a table, it should contain a separate column for each service area. Alternatively, systems could produce separate reports tailored to include data for each service area.

(6) The detected contaminant data section(s) must clearly identify any data indicating violations of MCLs, MRDLs, or treatment techniques, and the report must contain a clear and readily understandable explanation of the violation including: the length of the violation, the potential adverse health effects, and actions taken by the system to address the violation. To describe the potential health effects, the system must use the relevant language of appendix A to this subpart.

(7) For detected unregulated contaminants for which monitoring is required, the reports must present the average and range at which the contaminant was detected. The report must include a brief explanation of the reasons for monitoring for unregulated contaminants such as:

(i) Unregulated contaminant monitoring helps EPA to determine where certain contaminants occur and whether the Agency should consider regulating those contaminants in the future.

(ii) A system may write its own educational statement with approval by the Primacy Agency.

(8) For systems that exceeded the lead action level in § 141.80(c) (or a prescribed level of lead that the Administrator establishes for public education or notification in a successor regulation), the detected contaminant data section must clearly identify the exceedance if any corrective action has been required by the Administrator or the State during the monitoring period covered by the report. The report must include a clear and readily understandable explanation of the exceedance, the steps consumers can take to reduce their exposure to lead, and a description of any corrective actions the system has or will take to address the exceedance.

(e) * * *

(1) If the system has performed any monitoring for *Cryptosporidium* which indicates that *Cryptosporidium* may be

present in the source water or the finished water, the report must include:

* * * * *

(f) Compliance with NPDWR. In addition to the requirements of § 141.153(d)(6), the report must note any violation that occurred during the period covered by the report of a requirement listed below, and include a clear and readily understandable explanation of the violation, any potential adverse health effects, and the steps the system has taken to correct the violation.

* * * * *

(2) Filtration and disinfection prescribed by subpart H-Filtration and Disinfection of this part. For systems which have failed to install adequate filtration or disinfection equipment or processes, or have had a failure of such equipment or processes which constitutes a violation, the report must include the following language as part of the explanation of potential adverse health effects: Inadequately treated water may contain disease-causing organisms. These organisms include bacteria, viruses, and parasites which can cause symptoms such as nausea, cramps, diarrhea, and associated headaches.

(3) Lead and copper control requirements prescribed by subpart I-Control of Lead and Copper of this part. For systems that fail to take one or more actions prescribed by §§ 141.80(d), 141.81, 141.82, 141.83, 141.84, or 141.93, the report must include the applicable language of appendix A to this subpart for lead, copper, or both.

* * * * *

(h) * * *

(1) * * *

(i) Both tap water and bottled water come from rivers, lakes, streams, ponds, reservoirs, springs, and wells. As water travels over the surface of the land or through the ground, it dissolves naturally occurring minerals and, in some cases, radioactive material. The water can also pick up and transport substances resulting from the presence of animals or from human activity. These substances are also called contaminants.

(ii) Contaminants are any physical, chemical, biological, or radiological substance or matter in water. Contaminants that may be present in source water include:

* * * * *

(B) *Inorganic contaminants*, such as salts and metals, which can occur naturally in the soil or groundwater or may result from urban stormwater runoff, industrial or domestic

wastewater discharges, oil and gas production, mining, or farming.

* * * * *

(E) *Radioactive contaminants*, which can occur naturally or be the result of oil and gas production and mining activities.

(iii) To protect public health, the Environmental Protection Agency prescribes regulations which limit the amount of certain contaminants in tap water provided by public water systems. The Food and Drug Administration regulations establish limits for contaminants in bottled water which must provide the same protection for public health.

(iv) Drinking water, including bottled water, may reasonably be expected to contain at least small amounts of some contaminants. The presence of contaminants does not necessarily mean that water poses a health risk. More information about contaminants and potential health effects can be obtained by calling the Environmental Protection Agency's Safe Drinking Water Hotline (800-426-4791).

(2) The report must include the telephone number of the owner, operator, or designee of the community water system as a source of additional information concerning the report. If a system uses a website or social media to share additional information, EPA recommends including information about how to access such media platforms in the report.

(3) In communities with a large proportion of consumers with limited English proficiency, as determined by the Primacy Agency, the report must contain information in the appropriate language(s) regarding the importance of the report and contain a telephone number, address, or contact information where such consumers may obtain a translated copy of the report, or assistance in the appropriate language, or the report must be in the appropriate language.

(i) Systems that are a recipient of EPA assistance, as defined in 40 CFR 7.25, must provide meaningful access to information in the reports to persons served by the water system with limited English proficiency.

(ii) Systems unable to provide translation support must include contact information to obtain translation assistance from the State. As described in § 142.16(f), States are required, as a condition of primacy to provide water systems with contact information where consumers can obtain translation assistance from the State.

* * * * *

(6) *Systems required to comply with subpart S-Ground Water Rule.*

(i) Any ground water system that receives notice from the State of a significant deficiency or notice from a laboratory of a fecal indicator-positive ground water source sample that is not invalidated by the State under § 141.402(d) must inform its customers of any significant deficiency that is uncorrected at the time of the next reporting period or of any fecal indicator-positive ground water source sample in the next report or 6-month update according to § 141.155. The system must continue to inform the public annually until the State determines that particular significant deficiency is corrected or the fecal contamination in the ground water source is addressed under § 141.403(a). Each report must include the following elements:

* * * * *

(7) *Systems required to comply with subpart Y-Revised Total Coliform Rule.*

(i) Any system required to comply with the Level 1 assessment requirement or a Level 2 assessment requirement that is not due to an *E. coli* MCL violation must include in the report the text found in paragraph (h)(7)(i)(A) and paragraphs (h)(7)(i)(B) and (C) of this section as appropriate, filling in the blanks accordingly and the text found in paragraphs (h)(7)(i)(D)(1) and (2) of this section if appropriate. Systems may write their own assessment statement with equivalent information for paragraphs (h)(7)(i)(B) and (C) of this section, with approval by the Primacy Agency.

(A) Coliforms are bacteria that occur naturally in the environment and are used as an indicator that other, potentially harmful, waterborne organisms may be present or that a potential pathway exists through which contamination may enter the drinking water distribution system. We found coliforms indicating the need to look for potential problems in water treatment or distribution. When this occurs, we are required to conduct assessment(s) to identify problems and to correct any problems that were found during these assessments.

(B) Because we found coliforms during sampling, we were required to conduct [INSERT NUMBER OF LEVEL 1 ASSESSMENTS] assessment(s) of the system, also known as a Level 1 assessment, to identify possible sources of contamination. [INSERT NUMBER OF LEVEL 1 ASSESSMENTS] Level 1 assessment(s) were completed. In addition, we were required to take [INSERT NUMBER OF CORRECTIVE ACTIONS] corrective actions and we completed [INSERT NUMBER OF

CORRECTIVE ACTIONS] of these actions.

(C) Because we found coliforms during sampling, we were required to conduct [INSERT NUMBER OF LEVEL 2 ASSESSMENTS] detailed assessments, also known as a Level 2 assessment, to identify possible sources of contamination. [INSERT NUMBER OF LEVEL 2 ASSESSMENTS] Level 2 assessments were completed. In addition, we were required to take [INSERT NUMBER OF CORRECTIVE ACTIONS] corrective actions and we completed [INSERT NUMBER OF CORRECTIVE ACTIONS] of these actions.

(D) * * *

(1) During the past year we failed to conduct all the required assessment(s).

* * * * *

(ii) Any system required to conduct a Level 2 assessment due to an *E. coli* MCL violation must include in the report the text found in paragraphs (h)(7)(ii)(A) and (B) of this section, and health effects language in appendix A of this section, filling in the blanks accordingly and the text found in paragraphs (h)(7)(ii)(C)(1) and (2) of this section, if appropriate. Systems may write their own assessment statement with equivalent information for paragraphs (h)(7)(ii)(A), (B) and (C) of this section, with approval by the Primacy Agency.

(A) We found *E. coli* bacteria, indicating the need to look for potential problems in water treatment or distribution. When this occurs, we are required to conduct assessment(s), also known as a Level 1 assessment, to identify problems and to correct any problems that were found during these assessments.

(B) We were required to complete a detailed assessment of our water system, also known as a Level 2 assessment, because we found *E. coli* in our water system. In addition, we were required to take [INSERT NUMBER OF CORRECTIVE ACTIONS] corrective actions and we completed [INSERT NUMBER OF CORRECTIVE ACTIONS] of these actions.

(C) * * *

* * * * *

(2) We failed to correct all defects that were identified during the assessment that we conducted.

(iii) * * *

(D) We failed to test for *E. coli* when any repeat sample tested positive for total coliform.

* * * * *

(8) *Systems required to comply with subpart I-Control of Lead and Copper.*

(i) The report must notify consumers that complete lead tap sampling data are

available for review and must include information on how to access the data.

(ii) The report must include a statement that a service line inventory (including inventories consisting only of a statement that there are no lead service lines) has been prepared and include instructions to access the publicly available service line inventory. If the service line inventory is available online, the report must include the direct link to the inventory.

(iii) The report must contain a brief and plainly worded explanation of the *corrosion control efforts* the system is taking in accordance with 40 CFR part 141, subpart I *Control of Lead and Copper*.

■ 5. Amend § 141.154 by:

■ a. Revising paragraphs (a), (b), (c)(1) and (2), and (d)(2); and

■ b. Removing paragraphs (e) and (f).

The revisions read as follows:

§ 141.154 Required additional health information.

(a) All reports must prominently display the following language: Some people may be more vulnerable to contaminants in drinking water than the general population. Immuno-compromised persons such as persons with cancer undergoing chemotherapy, persons who have undergone organ transplants, people with HIV/AIDS or other immune system disorders, some elderly, and infants can be particularly at risk from infections. These people should seek advice about drinking water from their health care providers. EPA/CDC guidelines on appropriate means to lessen the risk of infection by *Cryptosporidium* and other microbial contaminants are available from the Safe Drinking Water Hotline (800-426-4791) or on EPA's website epa.gov/safewater.

(b) A system that detects arsenic above 0.005 mg/L and up to and including 0.010 mg/L:

(1) Must include in its report a short informational statement about arsenic, using language such as: Arsenic is known to cause cancer in humans. Arsenic also may cause other health effects such as skin damage and circulatory problems. [NAME OF UTILITY] meets the EPA arsenic drinking water standard, also known as a Maximum Contaminant Level (MCL). However, you should know that EPA's MCL for arsenic balances the scientific community's understanding of arsenic-related health effects and the cost of removing arsenic from drinking water. The highest concentration of arsenic found in [YEAR] was [INSERT MAX ARSENIC LEVEL per § 141.153(d)(4)(iv)] ppb, which is less than the EPA's MCL of 10 ppb.

(2) May write its own educational statement, with approval by the Primacy Agency.

(c) * * *

(1) Must include a short informational statement about the impacts of nitrate on children using language such as: Even though [NAME OF UTILITY] meets the EPA nitrate drinking water standard, also known as a Maximum Contaminant Level (MCL), if you are caring for an infant and using tap water to prepare formula, you may want to use alternate sources of water or ask for advice from your health care provider. Nitrate levels above 10 ppm pose a particularly high health concern for infants under 6 months of age and can interfere with the capacity of the infant's blood to carry oxygen, resulting in a serious illness. Symptoms of serious illness include shortness of breath and blueness of the skin, known as "blue baby syndrome." Nitrate levels in drinking water can increase for short periods of time due to high levels of rainfall or agricultural activity, therefore we test for nitrate [INSERT APPLICABLE SAMPLING FREQUENCY]. The highest level for nitrate found during [YEAR] was [INSERT MAX NITRATE LEVEL per § 141.153(d)(4)(iv)] ppm, which is less than the EPA's MCL of 10 ppm.

(2) May write its own educational statement, with approval by the Primacy Agency.

(d) * * *

(2) A system may write its own educational statement, with approval by the State.

■ 6. Amend § 141.155 by:

■ a. Revising the section heading and paragraphs (a), (b), (c), (e), (g) introductory text, (g)(1)(i), (g)(2); and

■ b. Adding paragraphs (i) and (j).

The revisions and additions read as follows:

§ 141.155 Report delivery, reporting and recordkeeping.

(a) Except as provided in paragraph (g) of this section, each community water system must directly deliver a copy of the report to each customer.

(1) Systems must use at a minimum, one of the following forms of delivery:

(i) Mail a paper copy of the report;

(ii) Mail a notification that the report is available on a website via a direct link; or

(iii) Email a direct link or electronic version of the report.

(2) Systems using delivery methods in paragraph (a)(1)(ii) and (iii) of this section must provide a paper copy of the report to any customer upon request. The notification method must prominently display directions for requesting such copy.

(3) For systems that choose to electronically deliver the reports by posting the report to a website and providing a notification either by mail or email, the report must be publicly available on the website at time notification is made. Notifications must prominently display the link and include an explanation of the nature of the link.

(i) Systems may use a web page to convey the information required in §§ 141.153, 141.154, and 141.156.

(4) Systems that use a publicly available website to provide reports must maintain public access to the report for no less than 3 years.

(b) The system must make a good faith effort to reach consumers who do not get water bills, using means recommended by the primacy agency. EPA expects that an adequate good faith effort will be tailored to the consumers who are served by the system but are not bill-paying customers, such as renters or workers. A good faith effort to reach consumers includes a mix of methods to reach the broadest possible range of persons served by the water system such as, but not limited to: Posting the reports on the internet; mailing reports or postcards with links to the reports to all service addresses and/or postal customers; using an opt in notification system to send emails and/or texts with links to the reports to interested consumers; advertising the availability of the report in the news media and on social media; publication in a local newspaper; posting a copy of the report or notice of availability with links (or equivalent, such as QR codes) in public places such as cafeterias or lunch rooms of public buildings; delivery of multiple copies for distribution by single-biller customers such as apartment buildings or large private employers; delivery to community organizations; and holding a public meeting to educate consumers on the reports.

(c) No later than the date the system is required to distribute the report to its customers, each community water system must provide a copy of the report to the primacy agency, followed within 3 months by a certification that the report(s) has/have been distributed to customers, and that the information is correct and consistent with the compliance monitoring data previously submitted to the primacy agency.

* * * * *

(e) Each community water system must make its reports available to the public upon request. Systems must make a reasonable effort to provide the reports in an accessible format to

anyone who requests an accommodation.

* * * * *

(g) The Governor of a State or their designee, or the Tribal Leader where the tribe has met the eligibility requirements contained in § 142.72 for the purposes of waiving the mailing requirement, can waive the requirement of paragraph (a) of this section for community water systems serving fewer than 10,000 persons. In consultation with the tribal government, the Regional Administrator may waive the requirement of § 141.155(a) in areas in Indian country where no tribe has been deemed eligible.

(1) * * *

(i) Publish the reports in one or more local newspapers or on one or more local online news sites serving the area in which the system is located;

* * * * *

(2) Systems serving 500 or fewer persons may forego the requirements of paragraphs (g)(1)(i) and (ii) of this section if they provide notice that the report is available upon request at least once per year to their customers by mail, door-to-door delivery or by posting in one or more locations where persons served by the system can reasonably be expected to see it.

* * * * *

(i) Systems serving 100,000 or more persons, must develop a plan for providing meaningful access to reports for limited English-proficient consumers. The system must evaluate the languages spoken by limited English-proficient persons served by the water system, and the system's anticipated approach to address translation needs. The first plan must be provided to the state with the first report in 2025. Plans must be evaluated annually and updated as necessary and reported with the certification required in § 141.155(c).

(j) Delivery timing and biannual delivery.

(1) Each community water system must distribute reports by July 1 each year. Each report distributed by July 1 must use data collected during, or prior to, the previous calendar year using methods described in paragraph (a) of this section.

(2) Each community water system serving 10,000 or more persons must distribute the report biannually, or twice per calendar year, by December 31 using methods described in paragraph (a) of this section.

(3) Systems required to comply with paragraph (j)(2) of this section, with a violation or action level exceedance that occurred between January 1st and June

30th of the current year, or have received monitoring results from required monitoring under § 141.40 Unregulated Contaminants Monitoring Rule, must include a 6-month update with the second report with the following:

(i) A short description of the nature of the 6-month update and the biannual delivery.

(ii) If a system receives an MCL, MRDL, or treatment technique violation, the 6-month update must include the applicable contaminant section information in § 141.153(d)(4), and a readily understandable explanation of the violation including: the length of the violation, the potential adverse health effects, actions taken by the system to address the violation, and timeframe the system expects to complete those actions. To describe the potential health effects, the system must use the relevant language of appendix A to this subpart.

(iii) If a system receives any other violation, the 6-month update must include the information in § 141.153(f).

(iv) If a system exceeded the lead action level following monitoring conducted between January 1st and June 30th of the current year, the system must include information identified in § 141.153(d)(4)(vi) and 141.153(d)(8).

(v) For systems monitoring under § 141.40 that become aware of results for samples collected during the reporting year but were not included in the reports distributed by July 1, the system must include information as required by § 141.153(d)(7).

■ 7. Adding § 141.156 to read as follows:

§ 141.156 Summary of report contents

(a) Each report must include a summary displayed prominently at the beginning of the report.

(b) Systems must include, at a minimum, the following information in the summary:

(1) Summary of violations and compliance information included in the report required by §§ 141.153(d)(6), 141.153(d)(8), 141.153(f), 141.153(h)(6), and 141.153(h)(7).

(2) Contact information for owner, operator, or designee of the community water system as a source of additional information concerning the report, per § 141.153(h)(2).

(c) If applicable, systems must include the following in the summary:

(1) For systems using delivery methods in § 141.155(a)(1)(ii) or (iii), the summary must include directions for consumers to request a paper copy of the report, as described in § 141.155(a)(2).

(2) Translation contact information to receive assistance with translating

information in the report, per § 141.153(h)(3).

(3) For systems using the report to also meet the public notification requirements of subpart Q—Public Notification of Drinking Water Violations, the summary must specify that it is also serving to provide public notification of one or more violations or situations, provide a brief statement about the nature of the notice(s), and a brief description of how to locate the notice(s) in the report.

(d) The summary should be written in plain language and may use infographics.

(e) For those systems required to include a 6-month update with the second report under § 141.155(j)(2), the summary should include a brief description of the nature of the report and update, noting the availability of new information for the current year (between January and June).

(f) The report summary must include the following standard language to encourage the distribution of the report to all persons served:

Please share this information with anyone who drinks this water (or their guardians), especially those who may not have received this report directly (for example, people in apartments, nursing homes, schools, and businesses). You can do this by posting this report in a public place or distributing copies by hand, mail, email, or another method.

PART 142—NATIONAL PRIMARY DRINKING WATER REGULATIONS IMPLEMENTATION

■ 8. The authority citation for part 142 continues to read as follows:

Authority: 42 U.S.C. 300f, 300g–1, 300g–2, 300g–3, 300g–4, 300g–5, 300g–6, 300j–4, 300j–9, and 300j–11.

■ 9. Amend § 142.14 by adding paragraph (h) to read as follows:

§ 142.14 Records kept by States.

* * * * *

(h) Each State that has primary enforcement responsibility must maintain the following records under subpart O of this part:

(1) A copy of the consumer confidence reports for a period of one year and the certifications obtained pursuant to 40 CFR 141.155(c) for a period of 5 years.

(2) A copy of the plans submitted pursuant to 40 CFR 141.153(h)(3)(i) for a period of 5 years.

■ 10. Amend § 142.15 by:

■ a. Revising paragraph (b) introductory text;

■ b. Removing in paragraph (b)(2), the period at the end of the paragraph and adding “; and” in its place; and

■ c. Adding paragraph (b)(3).

The revisions and additions read as follows:

§ 142.15 Reports by States.

* * * * *

(b) Each State which has primary enforcement responsibility must submit annual reports to the Administrator on a schedule and in a format prescribed by the Administrator, consisting of the following information:

* * * * *

(3) Compliance monitoring data and related data necessary for determining compliance for all existing National Primary Drinking Water Regulations (NPDWRs) in 40 CFR part 141. Related compliance data include specified records kept by the State in § 142.14.

* * * * *

■ 11. Amend § 142.16 by revising paragraphs (f)(1), (3), and (4) to read as follows:

§ 142.16 Special primacy requirements.

* * * * *

(f) * * *

(1) Each State that has primary enforcement responsibility must adopt the revised requirements of 40 CFR part 141, subpart O no later than [DATE TWO YEARS AFTER DATE OF FINAL RULE IN THE FEDERAL REGISTER]. States must submit revised programs to EPA for approval using the procedures in § 142.12(b) through (d).

* * * * *

(3) Each State must, as a condition of primacy, provide water systems with translation assistance to consumers upon request and provide contact information where consumers can obtain translation assistance for inclusion in the system’s report.

(4) Each application for approval of a revised program must include:

(i) A description of how the State will meet the requirements in § 141.153(h)(6) to provide translation assistance to consumers and contact information for translation assistance to water systems; and

(ii) A description of procedures for waiving the mailing requirement for small systems consistent with 40 CFR 141.155(g).

* * * * *

[FR Doc. 2023-06674 Filed 4-4-23; 8:45 am]

BILLING CODE 6560-50-P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

50 CFR Part 648

[Docket No. 230330-0087]

RIN 0648-BL61

Fisheries of the Northeastern United States; Improvement and Modernization of Atlantic Surfclam and Ocean Quahog Vessel Reporting Regulations

AGENCY: National Marine Fisheries Service (NMFS), National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Proposed rule; request for comments.

SUMMARY: NMFS proposes regulation changes to integrate the vessel reporting requirements for the Atlantic surfclam and ocean quahog fisheries with the reporting requirements for all other commercial fisheries in the Greater Atlantic Region. These changes are intended to simplify the regulations and make it easier for surfclam and ocean quahog vessel operators to submit the required fishing trip reports electronically. This action would result in improved administration and management of the surfclam and ocean quahog fisheries.

DATES: Comments must be received on May 5, 2023.

ADDRESSES: You may submit comments on this document, identified by NOAA-NMFS-2022-0100, by any of the following methods:

- *Electronic Submission:* Submit all electronic public comments via the Federal e-Rulemaking Portal. Go to www.regulations.gov and enter NOAA-NMFS-2022-0100 in the Search box. Click on the “Comment” icon, complete the required fields, and enter or attach your comments.

- *Mail:* Submit written comments to Michael Pentony, Regional Administrator, NMFS, Greater Atlantic Regional Fisheries Office, 55 Great Republic Drive, Gloucester, MA 01930. Mark the outside of the envelope: “Comments on Surfclam/Ocean Quahog Vessel Reporting Rule.”

Instructions: Comments sent by any other method, to any other address or individual, or received after the end of the comment period, may not be considered by NMFS. All comments received are part of the public record and will generally be posted for public viewing on www.regulations.gov without change. All personal identifying

information (e.g., name, address, etc.), confidential business information, or otherwise sensitive information submitted voluntarily by the sender will be publicly accessible. NMFS will accept anonymous comments (enter “N/A” in the required fields if you wish to remain anonymous).

Written comments regarding the burden-hour estimates or other aspects of the collection-of-information requirements contained in this proposed rule may be submitted to the Greater Atlantic Regional Fisheries Office and to www.reginfo.gov/public/do/PRAMain. Find this particular information collection by selecting “Currently under 30-day Review—Open for Public Comments” or by using the search function.”

FOR FURTHER INFORMATION CONTACT: Douglas Potts, Fishery Policy Analyst, (978) 281-9341, douglas.potts@noaa.gov.

SUPPLEMENTARY INFORMATION:

Background

The Mid-Atlantic Fishery Management Council (Council) manages the Atlantic surfclam and ocean quahog fisheries under the Atlantic Surfclam and Ocean Quahog Fishery Management Plan (FMP). The FMP has included a requirement for fishing vessels to maintain and submit a log of fishing operations since it was first implemented (42 FR 60438, November 25, 1977). Over the years, other species also became subject to management under the Magnuson-Stevens Fishery Conservation and Management Act (Magnuson-Stevens Act) and additional fishing vessel reporting requirements were added to the regulations. To cover the reporting requirements of these other fisheries, a standardized fishing vessel trip report (VTR) form was developed. For a number of reasons, including the specific requirements of the Atlantic Surfclam and Ocean Quahog Individual Transferable Quota (ITQ) management system, the surfclam and ocean quahog vessel reporting regulations have remained separate from the vessel reporting regulations that apply to all other commercial fisheries in the Greater Atlantic Region, and surfclam and ocean quahog vessels have used a form separate from the VTR, often referred to as the clam logbook, to report fishing trips that specifically target surfclam or ocean quahog.

Until recently, all VTR and clam logbook submissions were made using paper forms completed by the vessel operator and then submitted to NMFS. Because there were two separate sets of reporting regulations, a surfclam or

ocean quahog fishing vessel that incidentally caught another federally managed species was required to submit two separate forms for the trip: A clam logbook for their surfclam or ocean quahog catch and a standard VTR for all other species. This was inconvenient, but could reasonably be accomplished as long as the vessel operator had both paper forms readily available.

As of November 10, 2021, NMFS required all commercial fishing vessel trip reports be submitted electronically (85 FR 71575, November 10, 2020). Surfclam and ocean quahog vessels were allowed to continue submitting paper trip reports because a suitable electronic reporting application that addressed the unique requirements of that fishery was not available at that time. Since then, NMFS has completed the necessary changes to our Fish Online electronic VTR (eVTR) application to accommodate the unique reporting requirements of the surfclam and ocean quahog ITQ fisheries. On December 1, 2022, NMFS announced that all surfclam and ocean quahog trip reports must be submitted electronically as of February 1, 2023. While Fish Online may be the only reporting application initially available to surfclam or ocean quahog fishermen, the proposed regulatory changes will make it easier for developers of other eVTR applications to accommodate surfclam and ocean quahog vessels, if the application developers choose to incorporate reporting for these fisheries in the future.

The regulatory changes proposed in this action would eliminate the requirement for a separate surfclam/ocean quahog logbook and would instead authorize surfclam and ocean quahog vessel operators to complete the standard eVTR with additional fields added to collect information specific to the ITQ fishery, including the ITQ allocation number, the cage tag numbers for all cages being landed, and price per bushel. This information is already reported by the fishery on the surfclam/ocean quahog logbook, so there would be no change to reporting burden on fishermen. Overall, the reporting burden would decrease as surfclam and ocean quahog trips that also land other regulated species would no longer be required to submit two reports, instead fulfilling all reporting requirements through a single electronic submission.

If this proposed action is implemented, surfclam and ocean quahog vessel operators would report some information in a different format than is currently used on the surfclam and ocean quahog logbook. However, because vessel operators are already

required to complete and submit the standard eVTR for incidentally caught species, they are already familiar with the fields used for this electronic format.

In this proposed rule, one data field would be removed from the regulations. The current list of required data fields on the clam logbook includes “Crew share by percentage” (50 CFR 648.7(b)(1)(iii)(H)). However, that field has not been included on the paper forms for at least 20 years. This information is not collected for other commercial fisheries in the region and is not necessary for the management of the surfclam and ocean quahog fishery. Because it has not been collected, we propose removing this requirement from the regulations.

Classification

NMFS is issuing this rule pursuant to section 305(d) of the Magnuson-Stevens Act. The reason for using this regulatory authority is: Pursuant to Magnuson-Stevens Act section 305(d), this action is necessary to carry out the provisions of the Atlantic Surfclam and Ocean Quahog FMP, because the initial provisions adopted in 1977 have become inconsistent with other reporting requirements leading to an unnecessary additional reporting burden on the fishing industry. The NMFS Assistant Administrator has determined that this proposed rule is consistent with the Atlantic Surfclam and Ocean Quahog FMP, other provisions of the Magnuson-Stevens Act, and other applicable law, subject to further consideration after public comment.

This proposed rule has been determined to be not significant for purposes of Executive Order 12866.

The Chief Counsel for Regulation of the Department of Commerce certified to the Chief Counsel for Advocacy of the Small Business Administration (SBA) that this proposed rule, if adopted, would not have a significant economic impact on a substantial number of small entities.

The measures proposed by this action apply to surfclam and ocean quahog vessel owners. There were 677 total vessels that hold a surfclam and/or an ocean quahog vessel permit. Some entities own more than one fishing vessel, resulting in 399 regulated entities.

For Regulatory Flexibility Act purposes only, NMFS has established a small business size standard for businesses, including their affiliated operations, whose primary industry is commercial fishing (see 50 CFR 200.2). A business primarily engaged in commercial fishing (NAICS code 11411)

is classified as a small business if it is independently owned and operated, is not dominant in its field of operation (including its affiliates), and has combined annual receipts not in excess of \$11 million for all its affiliated operations worldwide. Using this definition, there are 389 small entities and 10 large entities that would potentially be affected by this action.

The proposed measures are administrative in nature and are not expected to have impacts on the surfclam and ocean quahog fisheries, including landings levels (no changes in surfclam or ocean quahog ex-vessel revenues are expected), fishery distribution, or fishing methods and practices. The proposed action is not expected to result in changes to the nature or operation of the surfclam and ocean quahog fisheries. In addition, the proposed measures are not expected to disproportionately affect small entities. As a result, an initial regulatory flexibility analysis is not required and none has been prepared.

This proposed rule contains a collection-of-information requirement subject to review and approval by OMB under the Paperwork Reduction Act (PRA). This rule revises the existing requirements for the collection of information under the following OMB Control Number: 0648-0212, Greater Atlantic Region Logbook Family of Forms, by eliminating the shellfish log (NOAA Form 88-140). All respondents and responses that would have used this form would use the Fishing Vessel Trip Report (NOAA Form 88-30) instead. This form takes less time to complete and is submitted electronically resulting in a small decrease in estimated time burden and eliminates postage costs. Public reporting burden for the Fishing Vessel Trip Report is estimated to average five minutes, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information.

Public comment is sought regarding: whether this proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility; the accuracy of the burden estimate; ways to enhance the quality, utility, and clarity of the information to be collected; and ways to minimize the burden of the collection of information, including through the use of automated collection techniques or other forms of information technology. Submit comments on these or any other aspects

of the collection of information at www.reginfo.gov/public/do/PRAMain.

Notwithstanding any other provisions of the law, no person is required to respond or, nor shall any person be subject to a penalty for failure to comply with, a collection of information subject to the requirements of the PRA, unless that collection of information displays a currently valid OMB Control Number.

List of Subjects in 50 CFR Part 648

Fisheries, Fishing, Reporting and recordkeeping requirements.

Dated: March 30, 2023.

Samuel D. Rauch, III,

Deputy Assistant Administrator for Regulatory Programs, National Marine Fisheries Service.

For the reasons set out in the preamble, NMFS proposes to amend 50 CFR part 648 as follows:

PART 648—FISHERIES OF THE NORTHEASTERN UNITED STATES

■ 1. The authority citation for part 648 continues to read as follows:

Authority: 16 U.S.C. 1801 *et seq.*

■ 2. In § 648.7, revise the introductory text of paragraph (b)(1)(i) and paragraph (b)(1)(iii) to read as follows:

§ 648.7 Recordkeeping and reporting requirements.

* * * * *

(b) * * *

(1) * * *

(i) *Vessel owners or operators.* At least the following information as applicable and any other information required by the Regional Administrator must be provided:
* * * * *

(iii) *Surfclam and Ocean Quahog owners or operators.* In addition to the information listed under paragraph (b)(1)(i) of this section, the owner or operator of any vessel conducting any surfclam or ocean quahog fishing operations in the ITQ program must provide at least the following information and any other information required by the Regional Administrator:

- (A) Total amount in bushels of surfclams and/or ocean quahogs taken;
- (B) Price per bushel;
- (C) Tag numbers from cages used; and
- (D) Allocation permit number.

* * * * *

[FR Doc. 2023-07017 Filed 4-4-23; 8:45 am]

BILLING CODE 3510-22-P

This section of the FEDERAL REGISTER contains documents other than rules or proposed rules that are applicable to the public. Notices of hearings and investigations, committee meetings, agency decisions and rulings, delegations of authority, filing of petitions and applications and agency statements of organization and functions are examples of documents appearing in this section.

AGENCY FOR INTERNATIONAL DEVELOPMENT

Senior Executive Service: Membership of Performance Review Board

ACTION: Notice.

SUMMARY: This notice provides a list of approved candidates who comprise a standing roster for service on the Agency's 2023 SES Performance Review Board. The Agency will use this roster to select SES Performance Review Board members.

FOR FURTHER INFORMATION CONTACT: Lena Travers at 202-712-5636 or ltravers@usaid.gov.

SUPPLEMENTARY INFORMATION: The standing roster is as follows:

Bader, Harry
Ball, Kimberly
Beers, Mia
Bertram, Robert
Broderick, Deborah
Brown, Erin
Buckley, Ruth
Davis, Thomas
Detherage, Maria Price
Faraj, Shereen
Feinstein, Barbara
Girod, Gayle
Gray, Jason
Jenkins, Robert
Jin, Jun
Johnson, Mark
Knudsen, Ciara
Korde, Sonali
Kuyumjian, Kent
Lucas, Rachel
Martinez, Ismael
McGill, Brian
Mitchell, Reginald
Napoli, Roman
Nims, Matthew
Ohlweiler, John
Pryor, Jeanne
Pustejovsky, Brandon
Schulz, Laura
Singh, Sukhvinder
Sokolowski, Alexander
Taylor, Margaret
Vega, Dennis
Voorhees, John
Wallace, Julia

Walther, Mark
Walton, David
Willis, Lindsey

Lena Travers,

Acting Director, Center for Performance Excellence.

[FR Doc. 2023-07001 Filed 4-4-23; 8:45 am]

BILLING CODE 6116-01-P

DEPARTMENT OF AGRICULTURE

Forest Service

Notice of Intent To Publish Proposed Permanent Recreational Shooting Order in the Laramie Ranger District of the Medicine Bow-Routt National Forests

AGENCY: Forest Service, Agriculture (USDA).

ACTION: Notice.

SUMMARY: The Forest Service, U.S. Department of Agriculture, is giving notice of its intent to publish for public comment a proposed permanent order prohibiting recreational shooting in the Pole Mountain Area of the Laramie Ranger District of the Medicine Bow-Routt National Forests, which covers approximately 55,000 acres in Albany County, Wyoming, from March 31 to September 10. At the end of the advance notice period, the Forest Service will seek public comments, as specified in this notice, on the proposed permanent seasonal recreational shooting order.

DATES: Advance notice of the opportunity to provide public comment on the proposed permanent seasonal recreational shooting order is being provided until April 12, 2023. Beginning on April 12, 2023, the Forest Service will accept comments on the proposed permanent seasonal recreational shooting order for 60 days. The notice of opportunity for public comment will be posted on the Medicine Bow-Routt National Forests and Thunder Basin National Grassland's web page at <https://www.fs.usda.gov/alerts/mbr/alerts-notice>.

ADDRESSES: The proposed permanent seasonal recreational shooting order, map and the justification for the proposed permanent order are posted on the Forest Service's Regulations and Policies web page at www.fs.usda.gov/about-agency/regulations-policies.

FOR FURTHER INFORMATION CONTACT:

Frank Romero, Laramie District Ranger, 307-745-2337 or frank.e.romero@usda.gov. Individuals who use telecommunication devices for the hearing-impaired may call the Federal Relay Service at 800-877-8339, 24 hours a day, every day of the year, including holidays.

SUPPLEMENTARY INFORMATION:

Advance Notice and Public Comment Procedures

Section 4103 of the John D. Dingell, Jr. Conservation, Management, and Recreation Act of 2019 (Pub. L. 116-9, Title IV (Sportsmen's Access and Related Matters)), hereinafter "the Dingell Act," requires the Forest Service to provide advance notice and opportunity for public comment before temporarily or permanently closing any National Forest System lands to hunting, fishing, or recreational shooting. Section 4103 of the Dingell Act applies to the proposed permanent order prohibiting recreational shooting in the Pole Mountain Area of the Laramie Ranger District in the Medicine Bow-Routt National Forests from March 31 to September 10. The public notice and comment process in section 4103(b)(2) of the Dingell Act requires the Forest Service to publish a notice of intent in the **Federal Register** of the proposed permanent order in advance of the public comment period for the proposed permanent order. This notice meets the requirement to publish a notice of intent in the **Federal Register** in advance of the public comment period.

Following the notice of intent, section 4103(b)(2) of the Dingell Act requires an opportunity for public comment on proposed temporary or permanent hunting, fishing, or recreational shooting orders. Because the proposed order would permanently prohibit recreational shooting in the Pole Mountain Area of the Laramie Ranger District of the Medicine Bow-Routt National Forests from March 31 to September 10, the public comment period must be at least 60 days. Beginning on April 12, 2023, the Forest Service will accept public comments on the proposed permanent order for 60 days. The notice of opportunity for public comment will be posted on the Medicine Bow-Routt National Forests and Thunder Basin National Grassland's

web page at <https://www.fs.usda.gov/alerts/mbr/alerts-notices>.

Section 4103(b)(2) of the Dingell Act requires the Forest Service to respond to public comments received on the proposed permanent order before issuing a final permanent order, including an explanation of how any significant issues raised by the comments were resolved and, if applicable, how resolution of those issues affected the proposed permanent order or the justification for the proposed permanent order. The final permanent order, the justification for the final permanent order, and the response to comments on the proposed permanent order will be posted on the Medicine Bow-Routt National Forests and Thunder Basin National Grassland's web page at <https://www.fs.usda.gov/alerts/mbr/alerts-notices>.

Background and Need

The proposed permanent order would implement a requirement of the 2008 Allotment Management Plan Revisions for the Pole Mountain Grazing Allotments and Limiting Firearm Use Within the Pole Mountain Area Environmental Assessment (EA) and 2010 Decision Notice and Finding of No Significant Impact—Limiting Firearm Use Within the Pole Mountain Area. The proposed permanent order would prohibit discharging a firearm, air rifle, or gas gun in the Pole Mountain Area of the Laramie Ranger District of the Medicine Bow-Routt National Forests from March 31 to September 10 to address public safety and natural resource concerns. Land management plan direction does not limit recreational shooting in any other locations of the Medicine Bow-Routt National Forests.

The proposed permanent order and the justification for the proposed permanent order are posted on the Forest Service's Regulations and Policies web page at www.fs.usda.gov/about-agency/regulations-policies.

Dated: March 29, 2023.

Gregory Smith,

Associate Deputy Chief, National Forest System.

[FR Doc. 2023-06908 Filed 4-4-23; 8:45 am]

BILLING CODE 3411-15-P

DEPARTMENT OF AGRICULTURE

Forest Service

Notice of Issuance of Final Permanent Seasonal Hunting Order in the Douglas Ranger District of the Thunder Basin National Grassland

AGENCY: Forest Service, Agriculture (USDA).

ACTION: Notice.

SUMMARY: The Forest Service (Forest Service or Agency), United States Department of Agriculture, is issuing a final permanent seasonal order prohibiting prairie dog hunting annually from February 1 to August 15 in Management Area 3.67 of the Douglas Ranger District in the Thunder Basin National Grassland, which covers approximately 42,000 acres in Campbell, Converse, and Weston Counties, Wyoming.

ADDRESSES: The final permanent seasonal order, map, response to comments on the proposed permanent seasonal order, justification for the final permanent seasonal order, and regulatory certifications for the final permanent seasonal order are posted on the Medicine Bow-Routt National Forests and Thunder Basin National Grassland's web page at <https://www.fs.usda.gov/alerts/mbr/alerts-notices>.

FOR FURTHER INFORMATION CONTACT: Rob Robertson, Douglas District Ranger, 307-358-4690 or robert.robertson@usda.gov. Individuals who use telecommunication devices for the hearing-impaired may call the Federal Relay Service at 800-877-8339, 24 hours a day, every day of the year, including holidays.

SUPPLEMENTARY INFORMATION: Section 4103 of the John D. Dingell, Jr. Conservation, Management, and Recreation Act of 2019 (Pub. L. 116-9, Title IV (Sportsmen's Access and Related Matters)), hereinafter "the Dingell Act," requires the Forest Service to provide advance notice and opportunity for public comment before temporarily or permanently closing any National Forest System lands to hunting, fishing, or recreational shooting.

The final permanent seasonal order prohibiting prairie dog hunting annually from February 1 to August 15 in Management Area 3.67 of the Douglas Ranger District in the Thunder Basin National Grassland has completed the public notice and comment process required under the Dingell Act. The Forest Service is issuing the final permanent seasonal hunting order. The

final permanent seasonal order, map, response to comments on the proposed permanent seasonal order, justification for the final permanent seasonal order, and regulatory certifications for the final permanent seasonal order are posted on the Medicine Bow-Routt National Forests and Thunder Basin National Grassland's web page at <https://www.fs.usda.gov/alerts/mbr/alerts-notices>.

Dated: March 29, 2023.

Gregory Smith,

Associate Deputy Chief, National Forest System.

[FR Doc. 2023-06909 Filed 4-4-23; 8:45 am]

BILLING CODE 3411-15-P

DEPARTMENT OF COMMERCE

Foreign-Trade Zones Board

[B-56-2022]

Foreign-Trade Zone (FTZ) 219; Authorization of Production Activity; Barco Stamping Co. Inc.; (Stamped Metal Products); Yuma, Arizona; Correction

The Federal Register notice published on March 27, 2023 (88 FR 18115), for the authorization of production activity for Barco Stamping Co. Inc., located in Yuma, Arizona, is corrected as follows:

In the first paragraph, the location identified as "Subzone 219B" should read "FTZ 219".

For further information, contact Juanita Chen at juanita.chen@trade.gov.

Dated: March 27, 2023.

Elizabeth Whiteman,

Acting Executive Secretary.

[FR Doc. 2023-07046 Filed 4-4-23; 8:45 am]

BILLING CODE 3510-DS-P

DEPARTMENT OF COMMERCE

Bureau of Industry and Security

Agency Information Collection Activities; Submission to the Office of Management and Budget (OMB) for Review and Approval; Comment Request; Five-Year Records Retention Requirement for Export Transactions and Boycott Actions

AGENCY: Bureau of Industry and Security, Department of Commerce.

ACTION: Notice of Information Collection, request for comment.

SUMMARY: The Department of Commerce, in accordance with the Paperwork Reduction Act of 1995 (PRA), invites the general public and

other Federal agencies to comment on proposed, and continuing information collections, which helps us assess the impact of our information collection requirements and minimize the public's reporting burden. The purpose of this notice is to allow for 60 days of public comment preceding submission of the collection to OMB.

DATES: To ensure consideration, comments regarding this proposed information collection must be received on or before June 5, 2023.

ADDRESSES: Interested persons are invited to submit comments by email to Mark Crace, IC Liaison, Bureau of Industry and Security, at mark.crace@bis.doc.gov or to PRAcomments@doc.gov. Please reference OMB Control Number 0694-0096 in the subject line of your comments. Do not submit Confidential Business Information or otherwise sensitive or protected information.

FOR FURTHER INFORMATION CONTACT: Requests for additional information or specific questions related to collection activities should be directed to Mark Crace, IC Liaison, Bureau of Industry and Security, phone 202-482-8093 or by email at mark.crace@bis.doc.gov.

SUPPLEMENTARY INFORMATION:

I. Abstract

This collection is necessary under Sections 760 and 762.6(a) of the Export Administration Regulations (EAR). The five-year retention requirement corresponds with the statute of limitations for violations and is necessary to preserve potential evidence for investigations. All parties involved in the export, reexport, transshipment or diversion of items subject to the EAR and the U.S. party involved in the export transaction involving a reportable boycott request are required to maintain records of these activities for a period of five years. The frequency depends upon how often each entity is involved in an export transaction or one involving a reportable boycott request.

II. Method of Collection

Paper or Electronic.

III. Data

OMB Control Number: 0694-0096.
Form Number(s): None.

Type of Review: Extension of a current information collection.

Affected Public: Business or other for-profit organizations.

Estimated Number of Respondents: 100,000.

Estimated Time per Response: 1 to 60 seconds.

Estimated Total Annual Burden Hours: 258.

Estimated Total Annual Cost to Public: 0.

Respondent's Obligation: Voluntary.

Legal Authority: 760 and 762.6(a) of the Export Administration Regulations (EAR).

IV. Request for Comments

We are soliciting public comments to permit the Department/Bureau to: (a) Evaluate whether the proposed information collection is necessary for the proper functions of the Department, including whether the information will have practical utility; (b) Evaluate the accuracy of our estimate of the time and cost burden for this proposed collection, including the validity of the methodology and assumptions used; (c) Evaluate ways to enhance the quality, utility, and clarity of the information to be collected; and (d) Minimize the reporting burden on those who are to respond, including the use of automated collection techniques or other forms of information technology.

Comments that you submit in response to this notice are a matter of public record. We will include or summarize each comment in our request to OMB to approve this ICR. Before including your address, phone number, email address, or other personal identifying information in your comment, you should be aware that your entire comment—including your personal identifying information—may be made publicly available at any time. While you may ask us in your comment to withhold your personal identifying information from public review, we cannot guarantee that we will be able to do so.

Sheleen Dumas,

Department PRA Clearance Officer, Office of the Under Secretary for Economic Affairs, Commerce Department.

[FR Doc. 2023-07018 Filed 4-4-23; 8:45 am]

BILLING CODE 3510-33-P

DEPARTMENT OF COMMERCE

International Trade Administration

[C-570-971]

Multilayered Wood Flooring From the People's Republic of China: Final Results of Expedited Second Sunset Review of the Countervailing Duty Order

AGENCY: Enforcement and Compliance, International Trade Administration, Department of Commerce.

SUMMARY: As a result of this expedited second sunset review, the Department of Commerce (Commerce) finds that

revocation of the countervailing duty (CVD) order on multilayered wood flooring (MLWF) from the People's Republic of China (China) would likely lead to continuation or recurrence of a countervailable subsidy at the levels indicated in the "Final Results of Review" section of this notice.

DATES: Applicable April 5, 2023.

FOR FURTHER INFORMATION CONTACT: Dennis McClure or Jonathan Schueler, AD/CVD Operations, Office VIII, Enforcement and Compliance, International Trade Administration, U.S. Department of Commerce, 1401 Constitution Ave. NW, Washington, DC 20230; telephone: (202) 482-5973 or (202) 482-9175, respectively.

SUPPLEMENTARY INFORMATION:

Background

On December 8, 2011, Commerce published the CVD order on MLWF from China.¹ On November 1, 2022, Commerce initiated the second sunset review of the *Order* pursuant to section 751(c) of the Tariff Act of 1930, as amended (the Act) and 19 CFR 351.218(c).² Commerce received a notice of intent to participate in the review on behalf of the American Manufacturers of Multilayered Wood Flooring (AMMWF), a domestic interested party, within the deadline specified in 19 CFR 351.218(d)(1)(i).³ AMMWF's members include AHF Product, LLC, Cahaba Veneer, Mohawk Industries, Inc., and Mullican Flooring, L.P. AMMWF claimed interested party status under section 771(9)(F) of the Act, as an association comprised of domestic producers of the domestic like product.

Commerce received an adequate substantive response from AMMWF within the 30-day deadline specified in 19 CFR 351.218(d)(3)(i).⁴ Commerce did not receive a substantive response from the Government of China or any other respondent interested party to the proceeding, and no hearing was requested.

On January 25, 2023, Commerce notified the U.S. International Trade

¹ See *Multilayered Wood Flooring from the People's Republic of China: Countervailing Duty Order*, 76 FR 76693 (December 8, 2011); see also *Multilayered Wood Flooring from the People's Republic of China: Amended Antidumping and Countervailing Duty Orders*, 77 FR 5484 (February 3, 2012), wherein the scope of the *Order* was modified (collectively, *Order*).

² See *Initiation of Five-Year ("Sunset") Reviews*, 87 FR 73757 (December 1, 2022).

³ See AMMWF's Letter, "Notice of Intent to Participate in Sunset Review," dated December 13, 2022.

⁴ See AMMWF's Letter, "Substantive Response to Notice of Initiation of Sunset Review" dated January 3, 2023.

Commission that it did not receive an adequate substantive response from respondent interested parties.⁵ As a result, pursuant to section 751(c)(3)(B) of the Act and 19 CFR 351.218(e)(1)(ii)(C)(2), Commerce conducted an expedited (120-day) sunset review of this *Order*.

Scope of the Order

The products covered by this order are certain multilayered wood flooring which are composed of an assembly of two or more layers or plies of wood veneer(s)⁶ in combination with a core.

For a full description of the scope, see the Issues and Decision Memorandum.⁷

Analysis of Comments Received

All issues raised in this sunset review are addressed in the Issues and Decision Memorandum. A list of topics discussed in the Issues and Decision Memorandum is included as an appendix to this notice. The Issues and Decision Memorandum is a public document and is on file electronically via Enforcement and Compliance’s Antidumping and Countervailing Duty Centralized Electronic Service System (ACCESS). ACCESS is available to

registered users at <https://access.trade.gov>. In addition, a complete version of the Issues and Decision Memorandum can be accessed directly at <https://access.trade.gov/public/FRNotices/ListLayout.aspx>.

Final Results of Sunset Review

Pursuant to sections 751(c)(1) and 752(b)(1) of the Act, we determine that revocation of the CVD order on MLWF from China would be likely to lead to continuation or recurrence of countervailable subsidies at the rates listed below:

Producer/exporter	Net countervailable subsidy rate (percent)
Fine Furniture (Shanghai) Ltd.; Great Wood (Tonghua) Ltd.; Fine Furniture Plantation (Shishou) Ltd	1.90
All-Others	18.87
124 Non-Cooperating Companies ⁸	43.96

Notification Regarding Administrative Protective Order

This notice serves as the only reminder to parties subject to administrative protective order (APO) of their responsibility concerning the return or destruction of proprietary information disclosed under APO in accordance with 19 CFR 351.305. Timely notification of return/destruction of APO materials or conversion to judicial protective order is hereby requested. Failure to comply with the regulations and the terms of an APO is a violation which is subject to sanction.

Notification to Interested Parties

Commerce is issuing and publishing these final results and notice in accordance with sections 751(c), 752(b), and 777(i)(1) of the Act and 19 CFR 351.218.

Dated: March 27, 2023.

Lisa W. Wang,

Assistant Secretary for Enforcement and Compliance.

Appendix

List of Topics Discussed in the Issues and Decision Memorandum

I. Summary

⁵ See Commerce’s Letter, “Sunset Reviews Initiated on December 1, 2022,” dated January 25, 2022.

⁶ A “veneer” is a thin slice of wood, rotary cut, sliced or sawed from a log, bolt or flitch. Veneer is referred to as a ply when assembled.

⁷ See Memorandum, “Issues and Decision Memorandum for the Final Results of the Expedited Second Sunset Review of the Countervailing Duty Order on Multilayered Wood Flooring from the People’s Republic of China,” (Issues and Decision

- II. Background
- III. Scope of the *Order*
- IV. History of the *Order*
- V. Legal Framework
- VI. Discussion of the Issues
 - a. Likelihood of Continuation or Recurrence of a Countervailable Subsidy
 - b. Net Countervailable Subsidy Rates Likely to Prevail
 - c. Nature of the Subsidies
- VII. Final Results of Sunset Review
- VIII. Recommendation

[FR Doc. 2023–07085 Filed 4–4–23; 8:45 am]

BILLING CODE 3510–DS–P

DEPARTMENT OF COMMERCE

International Trade Administration

[A–570–051]

Certain Hardwood Plywood Products From the People’s Republic of China: Final Results of the Expedited Sunset Review of the Antidumping Duty Order

AGENCY: Enforcement and Compliance, International Trade Administration, Department of Commerce.

SUMMARY: As a result of this expedited sunset review, the U.S. Department of Commerce (Commerce) finds that revocation of the antidumping duty (AD) order on certain hardwood

Memorandum) dated concurrently with, and hereby adopted by, this notice.

⁸ Commerce assigned a rate based on facts available with an adverse inference (AFA) to 124 non-cooperating companies in the investigation. For the full list of these companies, see *Multilayered Wood Flooring from the People’s Republic of China: Final Affirmative Countervailing Duty Determination*, 76 FR 64313 (October 18, 2011).

¹ See *Certain Hardwood Plywood Products from the People’s Republic of China: Amended Final*

plywood products (hardwood plywood) from the People’s Republic of China (China) would be likely to lead to continuation or recurrence of dumping at the levels indicated in the “Final Results of Review” section of this notice.

DATES: Applicable April 5, 2023.

FOR FURTHER INFORMATION CONTACT:

Kabir Archuletta, AD/CVD Operations, Office V, Enforcement and Compliance, International Trade Administration, U.S. Department of Commerce, 1401 Constitution Avenue NW, Washington, DC 20230; telephone: (202) 482–2593.

SUPPLEMENTARY INFORMATION:

Background

On January 4, 2018, Commerce issued the AD order on hardwood plywood from China.¹ On December 1, 2022, Commerce published the *Notice of Initiation* of the first sunset review of the *Order* pursuant to section 751(c) of the Tariff Act of 1930, as amended (the Act).² On December 13, 2022, Commerce received a notice of intent to participate from the Coalition for Fair Trade in Hardwood Plywood,³ a coalition of domestic producers of hardwood plywood products and the petitioner in the underlying

Determination of Sales at Less than Fair Value, and Antidumping Duty Order, 83 FR 504 (January 4, 2018) (*Order*).

² See *Initiation of Five-Year (Sunset) Reviews*, 87 FR 73757 (December 1, 2022) (*Notice of Initiation*).

³ The Coalition for Fair Trade in Hardwood Plywood’s members are Columbia Forest Products, Commonwealth Plywood Co., Ltd., Manthei Wood Products, States Industries LLC, and Timber Products Company.

investigation, within the deadline specified in 19 CFR 351.218(d)(1)(i).⁴ The petitioner claimed domestic interested party status under section 771(9)(F) of the Act and 19 CFR 351.102(b)(29)(viii), as an association whose members are manufacturers of the domestic like product in the United States.⁵ On January 3, 2023, the petitioner filed its timely substantive response within the 30-day deadline specified in 19 CFR 351.218(d)(3)(i).⁶ Commerce received no substantive responses from any other interested parties with respect to the *Order*, nor was a hearing requested. Commerce received comments on the adequacy of responses only from the domestic interested party in this sunset review.⁷ On January 25, 2023, Commerce notified the U.S. International Trade Commission that it did not receive an adequate substantive response from respondent interested parties in this sunset review.⁸ As a result, pursuant to section 751(c)(3)(B) of the Act and 19 CFR 351.218(e)(1)(ii)(C)(2), Commerce is conducting an expedited (120-day) sunset review of the *Order*.

Scope of the Order

The merchandise subject to this *Order* is hardwood and decorative plywood, and certain veneered panels as described below. For purposes of this proceeding, hardwood and decorative plywood is defined as a generally flat, multilayered plywood or other veneered panel, consisting of two or more layers or plies of wood veneers and a core, with the face and/or back veneer made of non-coniferous wood (hardwood) or bamboo. The veneers, along with the core may be glued or otherwise bonded together. Hardwood and decorative plywood may include products that meet the American National Standard for Hardwood and Decorative Plywood, ANSI/HPVA HP-1-2016 (including any revisions to that standard). A full description of the scope of the *Order* is contained in the Issues and Decision Memorandum.⁹

⁴ See Petitioner's Letter, "Notice of Intent to Participate in Sunset Review," dated December 13, 2022.

⁵ *Id.*

⁶ See Petitioner's Letter, "Substantive Response to Notice of Initiation," dated January 3, 2023.

⁷ See Petitioner's Letter, "Comments on Adequacy of Response," dated January 20, 2023.

⁸ See Commerce's Letter, "Sunset Reviews for December 2022," dated January 25, 2023.

⁹ See Memorandum, "Issues and Decisions Memorandum for the Expedited Sunset Review of the Antidumping Duty Order on Certain Hardwood Plywood Products from the People's Republic of China" dated concurrently with, and hereby adopted by, this notice (Issues and Decisions Memorandum).

Analysis of Comments Received

All issues raised in this review are addressed in the Issues and Decision Memorandum. The issues discussed in the Issues and Decision Memorandum include the likelihood of continuation or recurrence of dumping and the magnitude of the margins of dumping likely to prevail if the *Order* were revoked. A list of topics discussed in the Issues and Decision Memorandum is included as an appendix to this notice. The Issues and Decision Memorandum is a public document and is on file electronically via Enforcement and Compliance's Antidumping and Countervailing Duty Centralized Electronic Service System (ACCESS). ACCESS is available to registered users at <https://access.trade.gov>. In addition, a complete version of the Issues and Decision Memorandum can be accessed directly at <https://access.trade.gov/public/FRNoticesListLayout.aspx>.

Final Results of Sunset Review

Pursuant to sections 751(c)(1) and 752(c)(1) and (3) of the Act, Commerce determines that revocation of the *Order* would be likely to lead to continuation or recurrence of dumping, and that the margins of dumping likely to prevail would be weighted-average margins of up to 183.36 percent.

Administrative Protective Order

This notice serves as the only reminder to parties subject to an administrative protective order (APO) of their responsibility concerning the destruction of proprietary information disclosed under APO in accordance with 19 CFR 351.305(a). Timely notification of the destruction of APO materials or conversion to judicial protective orders is hereby requested. Failure to comply with the regulations and terms of an APO is a violation which is subject to sanction.

Notifications to Interested Parties

We are issuing and publishing these final results in accordance with sections 751(c), 752(c), and 777(i)(1) of the Act, and 19 CFR 351.218(e)(1)(ii)(C)(2) and 19 CFR 351.221(c)(5)(ii).

Dated: March 30, 2023.

Abdelali Elouaradia,

Deputy Assistant Secretary for Enforcement and Compliance.

Appendix—List of Topics Discussed in the Issues and Decision Memorandum

- I. Summary
- II. Background
- III. Scope of the *Order*
- IV. History of the *Order*
- V. Legal Framework
- VI. Discussion of the Issues

1. Likelihood of Continuation or Recurrence of Dumping
2. Magnitude of the Margins of Dumping Likely to Prevail
- VII. Final Results of Sunset Review
- VIII. Recommendation

[FR Doc. 2023-07043 Filed 4-4-23; 8:45 am]

BILLING CODE 3510-DS-P

DEPARTMENT OF COMMERCE

International Trade Administration

[A-580-899]

Acetone From the Republic of Korea: Preliminary Results of Antidumping Duty Administrative Review; 2021-2022

AGENCY: Enforcement and Compliance, International Trade Administration, Department of Commerce.

SUMMARY: The U.S. Department of Commerce (Commerce) preliminarily finds that Kumho P&B Chemicals, Inc. (KPB) and LG Chem, Ltd. (LG Chem), did not make sales of subject merchandise at less than normal value during the period of review (POR) March 1, 2021, through February 28, 2022. Interested parties are invited to comment on these preliminary results.

DATES: Applicable April 5, 2023.

FOR FURTHER INFORMATION CONTACT: Sean Carey, AD/CVD Operations, Office VII, Enforcement and Compliance, International Trade Administration, U.S. Department of Commerce, 1401 Constitution Avenue NW, Washington, DC 20230; telephone: (202) 482-3964.

SUPPLEMENTARY INFORMATION:

Background

On April 27, 2021, Commerce published the antidumping duty order on acetone from Belgium, the Republic of South Africa, and the Republic of Korea (Korea).¹ In accordance with section 751(a)(1) of the Tariff Act of 1930, as amended (the Act), Commerce is conducting an administrative review of the *Order*. On May 13, 2022, in accordance with 19 CFR 251.221(c)(1)(i), we initiated the administrative review of the *Order* covering KPB and LG Chem.² For a complete description of the events between the initiation of this review and these preliminary results, see the Preliminary Decision Memorandum.³

¹ See *Acetone from Belgium, the Republic of South Africa, and the Republic of Korea: Antidumping Duty Orders*, 85 FR 17866 (March 31, 2020) (*Order*).

² See *Initiation of Antidumping and Countervailing Duty Administrative Reviews*, 87 FR 29280 (May 13, 2022).

³ See Memorandum, "Acetone from the Republic of Korea: Decision Memorandum for the

Scope of the Order

The merchandise subject to the *Order* is acetone from Korea. For a complete description of the scope of the *Order*, see the Preliminary Decision Memorandum.⁴

Methodology

Commerce is conducting this review in accordance with section 751(a) of the Act. We calculated export price in accordance with section 772(a) of the Act. We calculated normal value in accordance with section 773 of the Act.

For a full description of the methodology underlying these preliminary results, see the Preliminary Decision Memorandum. A list of topics discussed in the Preliminary Decision Memorandum is attached as an appendix to this notice. The Preliminary Decision Memorandum is a public document and is available to the public via Enforcement and Compliance's Antidumping and Countervailing Duty Centralized Electronic Service System (ACCESS). ACCESS is available to registered users at <https://access.trade.gov>. In addition, the signed Preliminary Decision Memorandum can be accessed directly at <https://access.trade.gov/public/FRNoticesListLayout.aspx>.

Preliminary Results of the Review

We preliminarily determine the following weighted-average dumping margins for the period March 1, 2021, through February 28, 2022.

Exporter or producer	Weight-average dumping margin (percent)
Kumho P&B Chemicals, Inc	0.00
LG Chem, Ltd	0.00

Disclosure and Public Comment

Commerce intends to disclose the calculations performed for these preliminary results of review to interested parties within five days of the date of publication of this notice in accordance with 19 CFR 351.224(b). Interested parties may submit case briefs to Commerce no later than 30 days after the date of publication of this notice.⁵ Rebuttal briefs, limited to issues raised in the case briefs, may be filed not later than seven days after the date for filing

Preliminary Results of the Antidumping Duty Administrative Review; 2021–2022,” dated concurrently with, and hereby adopted by, this notice (Preliminary Decision Memorandum).

⁴ *Id.* at “Scope of the Order.”

⁵ See 19 CFR 351.309(c)(1)(ii).

case briefs.⁶ Pursuant to 19 CFR 351.309(c)(2) and (d)(2), parties who submit case briefs or rebuttal briefs in this proceeding are encouraged to submit with each argument: (1) a statement of the issue; (2) a brief summary of the argument; and (3) a table of authorities.⁷

Pursuant to 19 CFR 351.310(c), interested parties who wish to request a hearing must submit a written request to the Assistant Secretary for Enforcement and Compliance, filed electronically via ACCESS. An electronically-filed document must be received successfully in its entirety by ACCESS by 5 p.m. Eastern Standard Time within 30 days after the date of publication of this notice. Requests should contain: (1) the party's name, address, and telephone number; (2) the number of participants; (3) whether any participant is a foreign national; and (4) a list of issues the party intends to discuss. Issues raised in the hearing will be limited to those raised in the respective case and rebuttal briefs. If a request for a hearing is made, Commerce intends to hold the hearing at a date and time to be determined.⁸

All submissions should be filed using ACCESS,⁹ and must be served on interested parties.¹⁰ Commerce has temporarily modified certain of its requirements for serving documents containing business proprietary information, until further notice.¹¹

Final Results of Review

Unless otherwise extended, Commerce intends to issue the final results of this administrative review, including the results of its analysis of the issues raised in any written briefs, not later than 120 days after the date of publication of this notice, pursuant to section 751(a)(3)(A) of the Act and 19 CFR 351.213(h)(1).

Assessment Rates

Pursuant to section 751(a)(2)(A) of the Act and 19 CFR 351.212(b)(1), Commerce will determine, and U.S. Customs and Border Protection (CBP) shall assess, antidumping duties on all appropriate entries of subject merchandise in accordance with the final results of this review. Commerce intends to issue assessment instructions

to CBP no earlier than 35 days after the date of publication of the final results of this administrative review in the **Federal Register**. If a timely summons is filed at the U.S. Court of International Trade, the assessment instructions will direct CBP not to liquidate relevant entries until the time for parties to file a request for a statutory injunction has expired (*i.e.*, within 90 days of publication).

If KBP's or LG Chem's weighted-average dumping margin is not zero or *de minimis* (*i.e.*, less than 0.50 percent), upon completion of the final results, Commerce intends to calculate importer-specific assessment rates on the basis of the ratio of the total amount of dumping calculated for each importer's examined sales to the total entered value of those sales. Where we do not have entered values for all U.S. sales to a particular importer, we will calculate an importer-specific, per-unit assessment rate on the basis of the ratio of the total amount of dumping calculated for the importer's examined sales to the total quantity of those sales.¹² To determine whether an importer-specific, per-unit assessment rate is *de minimis*, in accordance with 19 CFR 351.106(c)(2), we also will calculate an importer-specific *ad valorem* ratio based on estimated entered values. Where either KBP's and LG Chem's weighted-average dumping margin is zero or *de minimis*, or an importer-specific *ad valorem* assessment rate is zero or *de minimis*, we will instruct CBP to liquidate appropriate entries without regard to antidumping duties.¹³

For entries of subject merchandise during the POR produced by either KBP or LG Chem for which it did not know that the merchandise it sold to the intermediary (*e.g.*, reseller, trading company, or exporter) was destined for the United States, we will instruct CBP to liquidate such entries at the all-others rate¹⁴ if there is no rate for the intermediate company(ies) involved in the transaction.¹⁵ The final results of this review shall be the basis for the assessment of antidumping duties on entries of merchandise covered by the final results of this review and for future

¹² See 19 CFR 351.212(b)(1).

¹³ See 19 CFR 352.106(c)(2); see also *Antidumping Proceeding: Calculation of the Weighted-Average Dumping Margin and Assessment Rate in Certain Antidumping Proceedings; Final Modification*, 77 FR 8101, 8103 (February 14, 2012).

¹⁴ See *Order*.

¹⁵ For a full discussion of this practice, see *Antidumping and Countervailing Duty Proceedings: Assessment of Antidumping Duties*, 68 FR 23954 (May 6, 2003).

⁶ See 19 CFR 351.309(d)(1) and (2); see also *Temporary Rule Modifying AD/CVD Service Requirements Due to COVID-19*, 85 FR 17006, 17007 (March 26, 2020).

⁷ See 19 CFR 351.309(c)(2) and (d)(2).

⁸ See 19 CFR 351.310(c).

⁹ See 19 CFR 351.303.

¹⁰ See 19 CFR 351.303(f).

¹¹ See *Temporary Rule Modifying AD/CVD Service Requirements Due to COVID-19; Extension of Effective Period*, 85 FR 41363 (July 10, 2020).

deposits of estimated antidumping duties, where applicable.¹⁶

Cash Deposit Requirements

The following cash deposit requirements will be effective for all shipments of subject merchandise entered, or withdrawn from warehouse, for consumption on or after the date of publication of the final results of this administrative review, as provided for by section 751(a)(2)(C) of the Act: (1) the company-specific cash deposit rate for KBP and LG Chem will be equal to the weighted-average dumping margin established in the final results of this review for each respondent (except, if that rate is *de minimis*, then the cash deposit rate will be zero); (2) for producers or exporters not covered in this review but covered in a prior segment of the proceeding, the cash deposit rate will continue to be the company-specific rate published for the most recently-completed segment of this proceeding in which they were reviewed; (3) if the exporter is not a firm covered in this review or a prior segment of the proceeding but the producer is, then the cash deposit rate will be the rate established for the most recently completed segment of this proceeding for the producer of the merchandise; and (4) the cash deposit rate for all other producers or exporters will continue to be 33.10 percent, the all-others rate established in the less-than-fair-value investigation.¹⁷ These cash deposit requirements, when imposed, shall remain in effect until further notice.

Notification to Importers

This notice serves as a preliminary reminder to importers of their responsibility under 19 CFR 351.402(f)(2) to file a certificate regarding the reimbursement of antidumping duties prior to liquidation of the relevant entries during this review period. Failure to comply with this requirement could result in Commerce's presumption that reimbursement of antidumping duties occurred and the subsequent assessment of double antidumping duties.

Notification to Interested Parties

We are issuing and publishing these preliminary results in accordance with sections 751(a)(1) and 777(i) of the Act, and 19 CFR 351.213(h) and 351.221(b)(4).

Dated: March 29, 2023.

Abdelali Elouaradia,

Deputy Assistant Secretary for Enforcement and Compliance.

Appendix

List of Topics Discussed in the Preliminary Decision Memorandum

- I. Summary
- II. Background
- III. Scope of the Order
- IV. Affiliation
- V. Discussion of the Methodology
- VI. Product Comparisons
- VII. Export Price
- VIII. Normal Value
- IX. Currency Conversion
- X. Recommendation

[FR Doc. 2023-07044 Filed 4-4-23; 8:45 am]

BILLING CODE 3510-DS-P

DEPARTMENT OF COMMERCE

International Trade Administration

[A-570-049, C-570-050]

Ammonium Sulfate From the People's Republic of China: Continuation of Antidumping and Countervailing Duty Orders

AGENCY: Enforcement and Compliance, International Trade Administration, Department of Commerce.

SUMMARY: The U.S. Department of Commerce (Commerce) and the U.S. International Trade Commission (ITC) have determined that revocation of the antidumping duty (AD) and countervailing duty (CVD) orders on ammonium sulfate from the People's Republic of China (China) would be likely to lead to the continuation or recurrence of dumping, net countervailable subsidies, and material injury to an industry in the United States. Therefore, Commerce is publishing a notice of continuation of these AD and CVD orders.

DATES: Applicable April 5, 2023.

FOR FURTHER INFORMATION CONTACT: Thomas Martin, AD/CVD Operations, Office IV, Enforcement and Compliance, International Trade Administration, U.S. Department of Commerce, 1401 Constitution Avenue NW, Washington, DC 20230; telephone: (202) 482-3936.

SUPPLEMENTARY INFORMATION:

Background

On May 9, 2017, Commerce published the AD and CVD orders on ammonium sulfate from China.¹ On February 1, 2022, Commerce published the notice of

¹ See *Ammonium Sulfate from the People's Republic of China: Antidumping Duty and Countervailing Duty Orders*, 82 FR 13094 (March 9, 2017) (*Orders*).

initiation of the first sunset reviews of the *Orders*, pursuant to section 751(c) of the Tariff Act of 1930, as amended (the Act).² As a result of its reviews, Commerce determined that revocation of the AD order would likely lead to the continuation or recurrence of dumping and that revocation of the CVD order would likely lead to the continuation or recurrence of countervailable subsidies.³ Therefore, Commerce notified the ITC of the magnitude of the dumping margins and net countervailable subsidy rates likely to prevail should the *Orders* be revoked, pursuant to sections 752(b) and (c) of the Act. On February 14, 2023, the ITC published its determination, pursuant to section 751(c) of the Act, that revocation of the *Orders* would likely lead to continuation or recurrence of material injury to an industry in the United States within a reasonably foreseeable time.⁴

Scope of the Orders

The merchandise covered by the *Orders* is ammonium sulfate in all physical forms, with or without additives such as anti-caking agents. Ammonium sulfate, which may also be spelled as ammonium sulphate, has the chemical formula (NH₄)₂SO₄.

The scope includes ammonium sulfate that is combined with other products, including by, for example, blending (*i.e.*, mixing granules of ammonium sulfate with granules of one or more other products), compounding (*i.e.*, when ammonium sulfate is compacted with one or more other products under high pressure), or granulating (incorporating multiple products into granules through, *e.g.*, a slurry process). For such combined products, only the ammonium sulfate component is covered by the scope of the *Orders*.

Ammonium sulfate that has been combined with other products is included within the scope regardless of whether the combining occurs in countries other than China.

Ammonium sulfate that is otherwise subject to the *Orders* is not excluded when commingled (*i.e.*, mixed or

² See *Initiation of Five-Year (Sunset) Reviews*, 87 FR 5467 (February 1, 2022).

³ See *Ammonium Sulfate from the People's Republic of China: Final Results of the Expedited First Sunset Review of the Antidumping Duty Order*, 87 FR 34841 (June 8, 2022), and accompanying Issues and Decision Memorandum (IDM); see also *Ammonium Sulfate from the People's Republic of China: Final Results of the Expedited First Sunset Review of the Countervailing Duty Order*, 87 FR 34848 (June 8, 2022), and accompanying IDM.

⁴ See *Ammonium Sulfate from China; Investigation Nos. 701-TA-562 and 731-TA-1329 (Review)*, 88 FR 9540 (February 14, 2023).

¹⁶ See section 751(a)(2)(C) of the Act.

¹⁷ See *Order*, 85 FR at 17866.

combined) with ammonium sulfate from sources not subject to the *Orders*. Only the subject component of such commingled products is covered by the scope of the *Orders*.

The Chemical Abstracts Service (CAS) registry number for ammonium sulfate is 7783-20-2.

The merchandise covered by the *Orders* is currently classifiable under Harmonized Tariff Schedule of the United States (HTSUS) subheading 3102.21.0000. Although this HTSUS subheading and CAS registry number are provided for convenience and customs purposes, the written description of the scope of the *Orders* is dispositive.

Continuation of the *Orders*

As a result of the determinations by Commerce and the ITC that revocation of the *Orders* would likely lead to the continuation or recurrence of dumping, countervailable subsidies, and material injury to an industry in the United States, pursuant to section 751(d)(2) of the Act and 19 CFR 351.218(a), Commerce hereby orders the continuation of the *Orders*. U.S. Customs and Border Protection will continue to collect AD and CVD cash deposits at the rates in effect at the time of entry for all imports of subject merchandise.

The effective date of continuation of these *Orders* will be the date of publication in the **Federal Register** of this notice of continuation. Pursuant to section 751(c)(2) of the Act, Commerce intends to initiate the next five-year reviews of the *Orders* not later than 30 days prior to the fifth anniversary of the effective date of continuation.

Administrative Protective Order (APO)

This notice also serves as the only reminder to parties subject to an APO of their responsibility concerning the return or destruction of proprietary information disclosed under APO in accordance with 19 CFR 351.305(a)(3). Timely written notification of the return or destruction of APO materials, or conversion to judicial protective order, is hereby requested. Failure to comply with the regulations and terms of an APO is a violation which is subject to sanction.

Notification to Interested Parties

These five-year (sunset) reviews and this notice are in accordance with sections 751(c) and 751(d)(2) of the Act and published in accordance with section 777(i) of the Act, and 19 CFR 351.218(f)(4).

Dated: February 16, 2023.

Lisa W. Wang,

Assistant Secretary for Enforcement and Compliance.

[FR Doc. 2023-07042 Filed 4-4-23; 8:45 am]

BILLING CODE 3510-DS-P

DEPARTMENT OF COMMERCE

International Trade Administration

[C-533-870]

Certain New Pneumatic Off-the-Road Tires From India: Preliminary Results of Countervailing Duty Administrative Review; 2021

AGENCY: Enforcement and Compliance, International Trade Administration, Department of Commerce.

SUMMARY: The U.S. Department of Commerce (Commerce) preliminarily determines that countervailable subsidies were provided to producers and/or exporters of certain new pneumatic off-the-road tires (OTR tires) from India, during the period of review (POR) January 1, 2021, through December 31, 2021. Interested parties are invited to comment on these preliminary results.

DATES: Applicable April 5, 2023.

FOR FURTHER INFORMATION CONTACT: Mark Hoadley, AD/CVD Operations, Office VII, Enforcement and Compliance, International Trade Administration, U.S. Department of Commerce, 1401 Constitution Avenue NW, Washington, DC 20230; telephone: (202) 482-3148.

SUPPLEMENTARY INFORMATION:

Background

On May 9, 2022, Commerce initiated this administrative review of the countervailing duty order on OTR tires from India.¹ The mandatory company respondents are ATC Tires Private Limited (ATC) and Balkrishna Industries Ltd. (BKT). On November 21, 2022, Commerce extended the time limit for these preliminary results to March 31, 2023.²

For a complete description of the events that followed the initiation of the review, see the Preliminary Decision Memorandum.³ A list of topics

¹ See *Initiation of Antidumping and Countervailing Duty Administrative Reviews*, 87 FR 29280 (May 13, 2022).

² See Memorandum, "Extension of Deadline for Preliminary Results of Review," dated November 21, 2022.

³ See Memorandum, "Decision Memorandum for the Preliminary Results of the Countervailing Duty Administrative Review, Off-the-Road Tires from India; 2021," dated concurrently with, and hereby adopted by, this notice (Preliminary Decision Memorandum).

discussed in the Preliminary Decision Memorandum is included as Appendix I to this notice. The Preliminary Decision Memorandum is a public document and is on file electronically via Enforcement and Compliance's Antidumping and Countervailing Duty Centralized Electronic System (ACCESS). ACCESS is available to registered users at <https://access.trade.gov>. In addition, a complete version of the Preliminary Decision Memorandum can be accessed directly at <https://access.trade.gov/public/FRNoticesListLayout.aspx>.

Scope of the Order

The merchandise covered by the order is OTR tires. OTR tires are tires with an off road tire size designation. The tires included in the scope may be either tube-type or tubeless, radial, or non-radial, regardless of whether for original equipment manufacturers or the replacement market. For a complete description of the scope of this order, see the Preliminary Decision Memorandum.

Methodology

Commerce is conducting this administrative review in accordance with section 751(a)(1)(A) of the Tariff Act of 1930, as amended (the Act). For each of the subsidy programs preliminarily found to be countervailable, Commerce preliminarily determines that there is a subsidy, *i.e.*, a financial contribution from an authority that gives rise to a benefit to the recipient and that the subsidy is specific.⁴ For a full description of the methodology underlying Commerce's preliminary conclusions, see the Preliminary Decision Memorandum.

Companies Not Selected for Individual Examination

The Act and Commerce's regulations do not directly address the subsidy rate to be applied to companies not selected for individual examination where Commerce limits its examination in an administrative review pursuant to section 777A(e)(2) of the Act. However, Commerce normally determines the rates for non-selected companies in reviews in a manner that is consistent with section 705(c)(5) of the Act, which provides instructions for calculating the all-others rate in an investigation. Section 777A(e)(2) of the Act provides that "the individual countervailable subsidy rates determined under

⁴ See sections 771(5)(B) and (D) of the Act regarding financial contribution; section 771(5)(E) of the Act regarding benefit; and section 771(5A) of the Act regarding specificity.

subparagraph (A) shall be used to determine the all-others rate under section 705(c)(5) {of the Act}.” Section 705(c)(5)(A) of the Act states that for companies not investigated, in general, we will determine an all-others rate by weight averaging the countervailable subsidy rates established for each of the companies individually investigated, excluding zero and de minimis rates or any rates based solely on the facts available.

Accordingly, to determine the rate for companies not selected for individual examination, Commerce’s practice is to weight average the net subsidy rates for the selected mandatory respondents, excluding rates that are zero, *de minimis*, or based entirely on facts available.⁵ We preliminarily determine that ATC and BKT received countervailable subsidies that are above *de minimis* and are not based entirely on facts available. Therefore, we preliminarily determine to apply the weighted average of the net subsidy rates calculated for ATC and BKT using publicly ranged sales data submitted by those respondents to the non-selected companies.⁶ The companies for which a review was requested, and which were not selected as mandatory respondents or found to be cross-owned with a mandatory respondent, are listed in Appendix II.

Preliminary Results of Review

Commerce preliminarily determines the net countervailable subsidy rates exist for the period January 1, 2021, through December 31, 2021:

Company	Subsidy rate (percent <i>ad valorem</i>)
ATC Tires Private Limited ⁷ ..	1.57
Balkrishna Industries Ltd	1.00
Companies Not Selected for Individual Review	1.29

Assessment Rates

In accordance with 19 CFR 351.221(b)(4)(i), Commerce preliminarily assigned a subsidy rate in the amount for the producer/exporter shown above. Upon completion of the administrative review, consistent with section 751(a)(1) of the Act and 19 CFR 351.212(b)(2), Commerce shall determine, and U.S. Customs and

⁵ See, e.g., *Certain Pasta from Italy: Final Results of the 13th (2008) Countervailing Duty Administrative Review*, 75 FR 37386, 37387 (June 29, 2010).

⁶ See Memorandum, “Calculation of Subsidy Rate for Non-Selected Companies Under Review,” dated concurrently with this memorandum.

⁷ This rate applies to ATC and ATC Tires AP Private Ltd.

Border Protection (CBP) shall assess, countervailing duties on all appropriate entries covered by this review. Commerce intends to issue assessment instructions to CBP no earlier than 35 days after the date of publication of the final results of this review in the **Federal Register**. If a timely summons is filed at the U.S. Court of International Trade, the assessment instructions will direct CBP not to liquidate relevant entries until the time for parties to file a request for a statutory injunction has expired (*i.e.*, within 90 days of publication).

Cash Deposit Rates

Pursuant to section 751(a)(1) of the Act, Commerce intends to instruct CBP to collect cash deposits in the amounts indicated for the producer/exporter listed above with regard to shipments of subject merchandise entered or withdrawn from warehouse, for consumption on or after the date of publication of the final results of this review. For all non-reviewed firms, CBP will continue to collect cash deposits of estimated countervailable duties at the all-others rate or the most recent company-specific rate applicable to the company, as appropriate. These cash deposit requirements, when imposed, shall remain in effect until further notice.

Disclosure

Commerce intends to disclose its calculations and analysis performed in reaching the preliminary results within five days of publication of these preliminary results, in accordance with 19 CFR 351.224(b).

Public Comment

Case briefs or other written documents may be submitted to the Assistant Secretary for Enforcement and Compliance.⁸ A timeline for the submission of case and rebuttal briefs and written comments will be provided to interested parties at a later date.

Pursuant to 19 CFR 351.301(c) and (d)(2), parties who wish to submit case or rebuttal briefs in this review are requested to submit for each argument: (1) a statement of the issue; (2) a brief summary of the argument; and (3) a table of authorities. All briefs must be filed electronically using ACCESS. Note that Commerce has modified certain of its requirements for serving documents containing business proprietary information, until further notice.⁹

⁸ See 19 CFR 351.309(c) and (d).

⁹ See *Temporary Rule Modifying AD/CVD Service Requirements Due to COVID-19; Extension of Effective Period*, 85 FR 41363 (July 10, 2020).

Pursuant to 19 CFR 351.310(c), interested parties who wish to request a hearing, limited to issues raised in the case and rebuttal briefs, must do so within 30 days after the date of publication of this notice by submitting a written request to the Assistant Secretary for Enforcement and Compliance.¹⁰ Requests should contain: (1) the party’s name, address, and telephone number; (2) the number of participants and whether a participant is a foreign national; and (3) a list of the issues to be discussed. If a hearing request is made, Commerce intends to hold the hearing at a time and date to be determined. Parties should confirm by telephone the date, time, and location of the hearing two days before the scheduled date.

Unless the deadline is extended, Commerce intends to issue the final results of this administrative review, which will include the results of Commerce’s analysis of the issues raised in the case briefs, within 120 days after the date of the preliminary results, pursuant to section 751(a)(3)(A) of the Act and 19 CFR 351.213(h)(1).

Notification to Interested Parties

These preliminary results are issued and published pursuant to sections 751(a)(1) and 777(i)(1) of the Act, and 19 CFR 351.221(b)(4).

Dated: March 30, 2023.

Abdelali Elouaradia,

Deputy Assistant Secretary for Enforcement and Compliance.

Appendix I

List of Topics Discussed in the Preliminary Decision Memorandum

- I. Summary
- II. Background
- III. Period of Review
- IV. Scope of the *Order*
- V. Rate for Non-Examined Companies
- VI. Subsidies Valuation
- VII. Interest Rate Benchmarks, Discount Rates, and Benchmarks for Measuring the Adequacy of Remuneration
- VIII. Analysis of Programs
- IX. Recommendation

Appendix II

List of Companies Not Selected for Individual Review

Apollo Tyres Ltd.
Asian Tire Factory Ltd.
Cavendish Industries Ltd.
CEAT Ltd.
Celite Tyre Corporation
Emerald Resilient Tyre Manufacturer
HRI Tyres India
Innovative Tyres & Tubes Limited
JK Tyres and Industries Ltd.
K.R.M. Tyres

¹⁰ See 19 CFR 351.310(c).

M/S. Caroline Furnishers Pvt Ltd.
MRF Limited
MRL Tyres Limited (Malhotra Rubbers Ltd.)
OTR Laminated Tyres (I) Pvt. Ltd.
Rubberman Enterprises Pvt. Ltd.
Sheetla Polymers
Speedways Rubber Company
Sun Tyres & Wheel Systems
Sundaram Industries Private Limited
Superking Manufacturers (Tyre) Pvt., Ltd.
TVS Srichakra Limited

[FR Doc. 2023-07086 Filed 4-4-23; 8:45 am]

BILLING CODE 3510-DS-P

DEPARTMENT OF COMMERCE

International Trade Administration

[C-489-832]

Carbon and Alloy Steel Wire Rod From the Republic of Turkey: Final Results of the Expedited First Sunset Review of the Countervailing Duty Order

AGENCY: Enforcement and Compliance, International Trade Administration, Department of Commerce.

SUMMARY: The U.S. Department of Commerce (Commerce) finds that revocation of the countervailing duty (CVD) order on carbon and alloy steel wire rod (wire rod) from the Republic of Turkey (Turkey) would be likely to lead to continuation or recurrence of countervailing subsidies at the levels indicated in the “Final Results of Sunset Review” section of this notice.

DATES: Applicable April 5, 2023.

FOR FURTHER INFORMATION CONTACT:

Kabir Archuletta, AD/CVD Operations, Office V, Enforcement and Compliance, International Trade Administration, U.S. Department of Commerce, 14th Street and Constitution Avenue NW, Washington, DC 20230; telephone: (202) 482-2593.

SUPPLEMENTARY INFORMATION:

Background

On May 21, 2018, Commerce published in the *Federal Register* the CVD order on wire rod from Turkey.¹ On December 1, 2022, Commerce published the notice of initiation of the first sunset review of the *Order*, pursuant to section 751(c) of the Tariff Act of 1930, as amended (the Act).² On December 14, 2022, Commerce received a timely-filed notice of intent to participate from Charter Steel, Commercial Metals Company, Liberty

¹ See *Carbon and Alloy Steel Wire Rod from Italy and the Republic of Turkey: Amended Final Affirmative Countervailing Duty Determination for the Republic of Turkey and Countervailing Duty Orders for Italy and the Republic of Turkey*, 83 FR 23420 (May 21, 2018) (*Order*).

² See *Initiation of Five-Year (Sunset) Reviews*, 87 FR 73757 (December 1, 2022) (*Initiation Notice*).

Steel USA, Nucor Corporation, and Optimus Steel LLC (collectively, the domestic interested parties), within the deadline specified in 19 CFR 351.218(d)(1)(i).³ The domestic interested parties claimed interested party status under section 771(9)(C) of the Act as producers of the domestic like product in the United States.

On December 30, 2022, Commerce received an adequate substantive response to the *Initiation Notice* from the domestic interested parties within the 30-day deadline specified in 19 CFR 351.218(d)(3)(i).⁴ We received no substantive responses from any other interested parties, including the Government of Turkey, nor was a hearing requested. On January 25, 2023, Commerce notified the U.S. International Trade Commission that it did not receive an adequate substantive response from respondent interested parties.⁵ As a result, pursuant to section 751(c)(3)(B) of the Act and 19 CFR 351.218(e)(1)(ii)(B)(2) and (C)(2), Commerce conducted an expedited (120-day) sunset review of the *Order*.

Scope of the Order

The merchandise covered by this *Order* is certain hot-rolled products of carbon steel and alloy steel, in coils, of approximately round cross section, less than 19.00 mm in actual solid cross-sectional diameter. For a full description of the scope, see the Issues and Decision Memorandum.⁶

Analysis of Comments Received

All issues raised in this sunset review are addressed in the accompanying Issues and Decision Memorandum.⁷ A list of topics discussed in the Issues and Decision Memorandum is included as an appendix to this notice. The Issues and Decision Memorandum is a public document and is on file electronically via Enforcement and Compliance’s Antidumping and Countervailing Duty Centralized Electronic Service System (ACCESS). ACCESS is available to registered users at <https://access.trade.gov>. In addition, a complete

³ See Domestic Interested Parties’ Letter, “Domestic Interested Parties’ Notice of Intent to Participate,” dated December 14, 2022.

⁴ See Domestic Interested Parties’ Letter, “Domestic Interested Parties’ Substantive Response,” dated December 30, 2022.

⁵ See Commerce’s Letter, “Sunset Reviews Initiated on December 1, 2022,” dated January 25, 2023.

⁶ See Memorandum, “Issues and Decision Memorandum for the Final Results of the Expedited First Sunset Review of the Countervailing Duty Order on Carbon and Alloy Steel Wire Rod from the Republic of Turkey,” dated concurrently with, and hereby adopted by, this notice (Issues and Decision Memorandum).

⁷ *Id.*

version of the Issues and Decision Memorandum can be accessed directly on the internet at <https://access.trade.gov/public/FRNoticesListLayout.aspx>.

Final Results of Sunset Review

Pursuant to sections 751(c)(1) and 752(b) of the Act, Commerce determines that revocation of the *Order* would likely lead to continuation or recurrence of countervailable subsidies at the rates listed below.

Exporter/producer	Net subsidy rate (percent <i>ad valorem</i>)
Habas Sinai Ve Tibbi Gazlar Istih (Habas)	6.09
Icdas Celik Eberji Tersane Ve Ulasim San (Icdas)	3.81
All Others	4.95

Administrative Protective Order (APO)

This notice serves as the only reminder to interested parties subject to an APO of their responsibility concerning the return or destruction of proprietary information disclosed under APO in accordance with 19 CFR 351.305. Timely notification of the return or destruction of APO materials or conversion to judicial protective order is hereby requested. Failure to comply with the regulations and terms of an APO is a violation which is subject to sanction.

Notification to Interested Parties

We are issuing and publishing these final results and notice in accordance with sections 751(c), 752(b), and 777(i)(1) of the Act and 19 CFR 351.218.

Dated: March 30, 2023.

Abdelali Elouaradia,

Deputy Assistant Secretary for Enforcement and Compliance.

Appendix

List of Topics Discussed in the Issues and Decision Memorandum

- I. Summary
- II. Background
- III. Scope of the *Order*
- IV. History of the *Order*
- V. Legal Framework
- VI. Discussion of the Issues
 1. Likelihood of Continuation or Recurrence of a Countervailable Subsidy
 2. Net Countervailable Subsidy Rate Likely to Prevail
 3. Nature of the Subsidies
- VII. Final Results of Sunset Review
- VIII. Recommendation

[FR Doc. 2023-07039 Filed 4-4-23; 8:45 am]

BILLING CODE 3510-DS-P

DEPARTMENT OF COMMERCE

International Trade Administration

[A-580-881]

Certain Cold-Rolled Steel Flat Products From the Republic of Korea: Final Results of Antidumping Duty Administrative Review; 2020–2021

AGENCY: Enforcement and Compliance, International Trade Administration, Department of Commerce.

SUMMARY: The U.S. Department of Commerce (Commerce) determines that certain cold-rolled steel flat products (cold-rolled steel) from the Republic of Korea (Korea) were not sold in the United States at less than normal value during the period of review (POR) September 1, 2020, through August 31, 2021.

DATES: Applicable April 5, 2023.

FOR FURTHER INFORMATION CONTACT: Preston Cox or Fred Baker, AD/CVD Operations, Office VI, Enforcement and Compliance, International Trade Administration, U.S. Department of Commerce, 1401 Constitution Avenue NW, Washington, DC 20230; telephone: (202) 482-5041 or (202) 482-2924, respectively.

SUPPLEMENTARY INFORMATION:

Background

On September 20, 2016, Commerce published in the *Federal Register* the antidumping duty order on cold-rolled steel from Korea.¹ On October 7, 2022, Commerce published the *Preliminary Results* of this administrative review in the *Federal Register*.² This administrative review covers four producers and/or exporters of the subject merchandise.³ Commerce selected Hyundai and POSCO/PIC (collectively, POSCO/PIC)⁴ for

¹ See *Certain Cold Rolled Steel Flat Products from Brazil, India, the Republic of Korea, and the United Kingdom: Amended Final Affirmative Antidumping Determinations for Brazil and the United Kingdom and Antidumping Duty Orders*, 81 FR 64432 (September 20, 2016) (*Order*).

² See *Certain Cold-Rolled Steel Flat Products from the Republic of Korea: Preliminary Results of Antidumping Duty Administrative Review; 2020–2021*, 87 FR 60989 (October 7, 2022) (*Preliminary Results*), and accompanying Preliminary Decision Memorandum (PDM).

³ See *Initiation of Antidumping and Countervailing Duty Administrative Reviews*, 86 FR 61121 (November 5, 2021). The four companies included in this review are Hyundai Steel Company (Hyundai), KG Dongbu Steel Co., Ltd. (Dongbu), POSCO, and POSCO International Corporation (PIC).

⁴ Commerce continues to treat POSCO and POSCO International Corporation as a collapsed single entity for the final results of this administrative review. See *Preliminary Results PDM* at 1.

individual examination.⁵ On January 18, 2023, we extended the deadline for these final results to no later than April 5, 2023.⁶ During November 2022 and January 2023, Commerce conducted on-site sales verifications of the questionnaire responses submitted by Hyundai and POSCO/PIC.⁷ Following the verifications, Commerce invited interested parties to submit case and rebuttal briefs.⁸ We received no comments from interested parties. Accordingly, no decision memorandum accompanies this *Federal Register* notice. Commerce conducted this administrative review in accordance with section 751 of the Tariff Act of 1930, as amended (the Act).

Scope of the Order

The merchandise covered by the *Order* is cold-rolled steel. For a complete description of the scope of the *Order*, see Appendix.

Verification

Pursuant to 782(i)(3) of the Act and 19 CFR 351.307(b)(1)(v), we conducted verification of the questionnaire responses submitted by Hyundai and POSCO/PIC.⁹

Changes Since the Preliminary Results

Based on a review of the record, including the results of verification, Commerce made certain changes to the preliminary weighted-average dumping margin calculation for POSCO/PIC. For detailed information, see POSCO/PIC's Final Analysis Memorandum.¹⁰

⁵ See *Preliminary Results PDM* at 2.

⁶ See Memorandum, “Extension of Final Results of Antidumping Duty Administrative Review; 2021–2021,” dated January 18, 2023.

⁷ See Memoranda, “Sales Verification Report for Hyundai Steel Company,” dated March 6, 2023; “Sales Verification Report for POSCO and POSCO International Corporation,” dated March 6, 2023; “Constructed Export Price Sales Verification Report for Hyundai Steel America,” dated March 6, 2023; and “Sales Verification Report for POSCO International America Corporation, POSCO America Corporation, and POSCO America Alabama Processing Center Co., Ltd.,” dated March 6, 2023.

⁸ See Memorandum, “Briefing Schedule,” dated March 8, 2023.

⁹ See Memoranda, “Sales Verification Report for Hyundai Steel Company,” dated March 6, 2023; “Sales Verification Report for POSCO and POSCO International Corporation,” dated March 6, 2023; “Constructed Export Price Sales Verification Report for Hyundai Steel America,” dated March 6, 2023; and “Sales Verification Report for POSCO International America Corporation, POSCO America Corporation, and POSCO America Alabama Processing Center Co., Ltd.,” dated March 6, 2023.

¹⁰ See Memorandum, “Final Analysis Memorandum for POSCO/PIC,” dated concurrently with this notice (POSCO/PIC's Final Analysis Memorandum).

Rate for Non-Selected Respondent

The Act and Commerce's regulations do not address the establishment of a rate to be applied to companies not selected for individual examination when Commerce limits its examination in an administrative review pursuant to section 777A(c)(2) of the Act. Generally, Commerce looks to section 735(c)(5) of the Act, which provides instructions for calculating the all-others rate in a market economy investigation, for guidance when calculating the rate for companies which were not selected for individual examination in an administrative review. Under section 735(c)(5)(A) of the Act, the all-others rate is normally “an amount equal to the weighted average of the estimated weighted average dumping margins established for exporters and producers individually investigated, excluding any zero or *de minimis* margins, and any margins determined entirely {on the basis of facts available}.”

For these final results, we have calculated weighted-average dumping margins for Hyundai and POSCO/PIC that are zero or *de minimis*, and we have not calculated any margins which are not zero, *de minimis*, or determined entirely on the basis of facts available. Therefore, consistent with our practice, we are applying to Dongbu, the company not selected for individual examination in this review, a margin of zero percent.¹¹

Final Results of Administrative Review

For these final results, we determine that the following weighted-average dumping margins exist for the period September 1, 2020, through August 31, 2021:

Producer/exporter	Weighted-average dumping margin (percent)
Hyundai Steel Company	0.00
POSCO/POSCO International Corporation	0.00
KG Dongbu Steel Co., Ltd ¹²	0.00

Disclosure

Commerce intends to disclose the calculations performed for POSCO/PIC for these final results to parties in this proceeding within five days of the date of publication of this notice in the *Federal Register*, in accordance with 19 CFR 351.224(b). Because we have made no changes from the *Preliminary Results*

¹¹ See *Albamarle Corp. v. United States*, 821 F.3d 1345 (Fed. Cir. 2016).

¹² This company is the only non-examined company in this review.

to the weighted-average dumping margin calculation for Hyundai, there are no calculations to disclose for the final results.

Assessment Rates

Pursuant to section 751(a)(2)(C) of the Act and 19 CFR 351.212(b)(1), Commerce has determined, and U.S. Customs and Border Protection (CBP) shall assess, antidumping duties on all appropriate entries of subject merchandise in accordance with the final results of this review. Because we calculated weighted-average dumping margins for Hyundai and POSCO/PIC which are zero or *de minimis* in the final results of this review, we intend to instruct CBP to liquidate the appropriate entries without regard to antidumping duties. For Dongbu, the company that was not selected for individual examination in this review, we will instruct CBP to liquidate entries at the rate established in these final results of review (*i.e.*, to liquidate entries without regard to antidumping duties).

For entries of subject merchandise during the POR produced by the above-referenced respondents for which they did not know its merchandise was destined for the United States, we will instruct CBP to liquidate unreviewed entries at the all-others rate in the less-than-fair-value investigation if there is no rate for the intermediate company(ies) involved in the transaction.¹³

Commerce intends to issue assessment instructions to CBP no earlier than 35 days after the date of publication of the final results of this review in the **Federal Register**. If a timely summons is filed at the U.S. Court of International Trade, the assessment instructions will direct CBP not to liquidate relevant entries until the time for parties to file a request for a statutory injunction has expired (*i.e.*, within 90 days of publication). The final results of this administrative review shall be the basis for the assessment of antidumping duties on entries of merchandise under review and for future cash deposits of estimated antidumping duties, where applicable.

Cash Deposit Requirements

The following cash deposit requirements will be effective upon publication in the **Federal Register** of these final results of administrative review for all shipments of the subject merchandise entered, or withdrawn from warehouse, for consumption on or

after the publication date, as provided by section 751(a)(2)(C) of the Act: (1) the cash deposit rate for companies subject to this review will be equal to the zero margin established in the final results of this administrative review; (2) for merchandise exported by a company not covered in this review but covered in a prior segment of the proceeding, the cash deposit rate will continue to be the company-specific rate published in the completed segment for the most recent period; (3) if the exporter is not a firm covered in this review, a prior review, or the less-than-fair-value investigation, but the producer is, then the cash deposit rate will be the rate established in the most recently completed segment of the proceeding for the producer of the merchandise; and (4) the cash deposit rate for all other producers or exporters will continue to be 20.33 percent, the all-others rate established in the less-than-fair-value investigation.¹⁴ These cash deposit requirements, when imposed, shall remain in effect until further notice.

Notification to Importers

This notice serves as a final reminder to importers of their responsibility under 19 CFR 351.402(f)(2) to file a certificate regarding the reimbursement of antidumping duties prior to liquidation of the relevant entries during this review period. Failure to comply with this requirement could result in Commerce's presumption that reimbursement of antidumping duties occurred and the subsequent assessment of double antidumping duties.

Administrative Protective Order

This notice also serves as a reminder to parties subject to an administrative protective order (APO) of their responsibility concerning the return or destruction of proprietary information disclosed under APO in accordance with 19 CFR 351.305(a)(3), which continues to govern business proprietary information in this segment of the proceeding. Timely written notification of the return or destruction of APO materials, or conversion to judicial protective order, is hereby requested. Failure to comply with the regulations and the terms of an APO is a sanctionable violation.

Notification to Interested Parties

These final results of review are issued and published in accordance with sections 751(a)(1) and 777(i)(1) of the Act, and 19 CFR 351.221(b)(5).

Dated: March 29, 2023.

Abdelali Elouaradia,

Deputy Assistant Secretary for Enforcement and Compliance.

Appendix

Scope of the Order

The products covered by the *Order* are certain cold-rolled (cold-reduced), flat-rolled steel products, whether or not annealed, painted, varnished, or coated with plastics or other non-metallic substances. The products covered do not include those that are clad, plated, or coated with metal. The products covered include coils that have a width or other lateral measurement ("width") of 12.7 mm or greater, regardless of form of coil (*e.g.*, in successively superimposed layers, spirally oscillating, *etc.*). The products covered also include products not in coils (*e.g.*, in straight lengths) of a thickness less than 4.75 mm and a width that is 12.7 mm or greater and that measures at least 10 times the thickness. The products covered also include products not in coils (*e.g.*, in straight lengths) of a thickness of 4.75 mm or more and a width exceeding 150 mm and measuring at least twice the thickness. The products described above may be rectangular, square, circular, or other shape and include products of either rectangular or non-rectangular cross-section where such cross-section is achieved subsequent to the rolling process, *i.e.*, products which have been "worked after rolling" (*e.g.*, products which have been beveled or rounded at the edges). For purposes of the width and thickness requirements referenced above:

(1) where the nominal and actual measurements vary, a product is within the scope if application of either the nominal or actual measurement would place it within the scope based on the definitions set forth above, and

(2) where the width and thickness vary for a specific product (*e.g.*, the thickness of certain products with non-rectangular cross-section, the width of certain products with non-rectangular shape, *etc.*), the measurement at its greatest width or thickness applies.

Steel products included in the scope of the *Order* are products in which: (1) iron predominates, by weight, over each of the other contained elements; (2) the carbon content is 2 percent or less, by weight; and (3) none of the elements listed below exceeds the quantity, by weight, respectively indicated:

- 2.50 percent of manganese, or
- 3.30 percent of silicon, or
- 1.50 percent of copper, or
- 1.50 percent of aluminum, or
- 1.25 percent of chromium, or
- 0.30 percent of cobalt, or
- 0.40 percent of lead, or
- 2.00 percent of nickel, or
- 0.30 percent of tungsten (also called wolfram), or
- 0.80 percent of molybdenum, or
- 0.10 percent of niobium (also called columbium), or
- 0.30 percent of vanadium, or
- 0.30 percent of zirconium

¹³ See *Antidumping and Countervailing Duty Proceedings: Assessment of Antidumping Duties*, 68 FR 23954 (May 6, 2003).

¹⁴ See *Order*, 81 FR at 64434.

Unless specifically excluded, products are included in this scope regardless of levels of boron and titanium.

For example, specifically included in this scope are vacuum degassed, fully stabilized (commonly referred to as interstitial-free (IF)) steels, high strength low alloy (HSLA) steels, motor lamination steels, Advanced High Strength Steels (AHSS), and Ultra High Strength Steels (UHSS). IF steels are recognized as low carbon steels with micro-alloying levels of elements such as titanium and/or niobium added to stabilize carbon and nitrogen elements. HSLA steels are recognized as steels with micro-alloying levels of elements such as chromium, copper, niobium, titanium, vanadium, and molybdenum. Motor lamination steels contain micro-alloying levels of elements such as silicon and aluminum. AHSS and UHSS are considered high tensile strength and high elongation steels, although AHSS and UHSS are covered whether or not they are high tensile strength or high elongation steels.

Subject merchandise includes cold-rolled steel that has been further processed in a third country, including but not limited to annealing, tempering, painting, varnishing, trimming, cutting, punching, and/or slitting, or any other processing that would not otherwise remove the merchandise from the scope of the *Order* if performed in the country of manufacture of the cold-rolled steel.

All products that meet the written physical description, and in which the chemistry quantities do not exceed any one of the noted element levels listed above, are within the scope of the order unless specifically excluded. The following products are outside of and/or specifically excluded from the scope of the *Order*:

- Ball bearing steels;¹⁵
- Tool steels;¹⁶
- Silico-manganese steel;¹⁷

¹⁵ Ball bearing steels are defined as steels which contain, in addition to iron, each of the following elements by weight in the amount specified: (i) not less than 0.95 nor more than 1.13 percent of carbon; (ii) not less than 0.22 nor more than 0.48 percent of manganese; (iii) none, or not more than 0.03 percent of sulfur; (iv) none, or not more than 0.03 percent of phosphorus; (v) not less than 0.18 nor more than 0.37 percent of silicon; (vi) not less than 1.25 nor more than 1.65 percent of chromium; (vii) none, or not more than 0.28 percent of nickel; (viii) none, or not more than 0.38 percent of copper; and (ix) none, or not more than 0.09 percent of molybdenum.

¹⁶ Tool steels are defined as steels which contain the following combinations of elements in the quantity by weight respectively indicated: (i) more than 1.2 percent carbon and more than 10.5 percent chromium; or (ii) not less than 0.3 percent carbon and 1.25 percent or more but less than 10.5 percent chromium; or (iii) not less than 0.85 percent carbon and 1 percent to 1.8 percent, inclusive, manganese; or (iv) 0.9 percent to 1.2 percent, inclusive, chromium and 0.9 percent to 1.4 percent, inclusive, molybdenum; or (v) not less than 0.5 percent carbon and not less than 3.5 percent molybdenum; or (vi) not less than 0.5 percent carbon and not less than 5.5 percent tungsten.

¹⁷ Silico-manganese steel is defined as steels containing by weight: (i) not more than 0.7 percent of carbon; (ii) 0.5 percent or more but not more than 1.9 percent of manganese, and (iii) 0.6 percent or more but not more than 2.3 percent of silicon.

• Grain-oriented electrical steels (GOES) as defined in the final determination of the U.S. Department of Commerce in Grain-Oriented Electrical Steel from Germany, Japan, and Poland.¹⁸

• Non-Oriented Electrical Steels (NOES), as defined in the antidumping orders issued by the U.S. Department of Commerce in Non-Oriented Electrical Steel from the People's Republic of China, Germany, Japan, the Republic of Korea, Sweden, and Taiwan.¹⁹

The products subject to the *Order* are currently classified in the Harmonized Tariff Schedule of the United States (HTSUS) under item numbers: 7209.15.0000, 7209.16.0030, 7209.16.0040, 7209.16.0045, 7209.16.0060, 7209.16.0070, 7209.16.0091, 7209.17.0030, 7209.17.0040, 7209.17.0045, 7209.17.0060, 7209.17.0070, 7209.17.0091, 7209.18.1530, 7209.18.1560, 7209.18.2510, 7209.18.2520, 7209.18.2580, 7209.18.2585, 7209.18.6020, 7209.18.6090, 7209.25.0000, 7209.26.0000, 7209.27.0000, 7209.28.0000, 7209.90.0000, 7210.70.3000, 7211.23.1500, 7211.23.2000, 7211.23.3000, 7211.23.4500, 7211.23.6030, 7211.23.6060, 7211.23.6090, 7211.29.2030, 7211.29.2090, 7211.29.4500, 7211.29.6030, 7211.29.6080, 7211.90.0000, 7212.40.1000, 7212.40.5000, 7225.50.6000, 7225.50.8080, 7225.99.0090, 7226.92.5000, 7226.92.7050, and 7226.92.8050.

The products subject to the *Order* may also enter under the following HTSUS numbers: 7210.90.9000, 7212.50.0000, 7215.10.0010, 7215.10.0080, 7215.50.0016, 7215.50.0018, 7215.50.0020, 7215.50.0061, 7215.50.0063, 7215.50.0065, 7215.50.0090, 7215.90.5000, 7217.10.1000, 7217.10.2000, 7217.10.3000, 7217.10.7000, 7217.90.1000, 7217.90.5030, 7217.90.5060, 7217.90.5090, 7225.19.0000, 7226.19.1000, 7226.19.9000, 7226.99.0180, 7228.50.5015, 7228.50.5040, 7228.50.5070, 7228.60.8000, and 7229.90.1000.

¹⁸ See *Grain-Oriented Electrical Steel from Germany, Japan, and Poland: Final Determinations of Sales at Less Than Fair Value and Certain Final Affirmative Determination of Critical Circumstances*, 79 FR 42501, 42503 (July 22, 2014). This determination defines grain-oriented electrical steel as “a flat-rolled alloy steel product containing by weight at least 0.6 percent but not more than 6 percent of silicon, not more than 0.08 percent of carbon, not more than 1.0 percent of aluminum, and no other element in an amount that would give the steel the characteristics of another alloy steel, in coils or in straight lengths.”

¹⁹ See *Non-Oriented Electrical Steel from the People's Republic of China, Germany, Japan, the Republic of Korea, Sweden, and Taiwan: Antidumping Duty Orders*, 79 FR 71741, 71741–42 (December 3, 2014). The orders define NOES as “cold-rolled, flat-rolled, alloy steel products, whether or not in coils, regardless of width, having an actual thickness of 0.20 mm or more, in which the core loss is substantially equal in any direction of magnetization in the plane of the material. The term ‘substantially equal’ means that the cross grain direction of core loss is no more than 1.5 times the straight grain direction (*i.e.*, the rolling direction) of core loss. NOES has a magnetic permeability that does not exceed 1.65 Tesla when tested at a field of 800 A/m (equivalent to 10 Oersteds) along (*i.e.*, parallel to) the rolling direction of the sheet (*i.e.*, B800 value). NOES contains by weight more than 1.00 percent of silicon but less than 3.5 percent of silicon, not more than 0.08 percent of carbon, and not more than 1.5 percent of aluminum. NOES has a surface oxide coating, to which an insulation coating may be applied.”

The HTSUS subheadings above are provided for convenience and U.S. Customs purposes only. The written description of the scope of the order is dispositive.

[FR Doc. 2023–07041 Filed 4–4–23; 8:45 am]

BILLING CODE 3510-DS-P

DEPARTMENT OF COMMERCE

International Trade Administration

[C–357–821, C–560–831]

Biodiesel From Argentina and Indonesia: Final Results of Expedited First Sunset Reviews of the Countervailing Duty Orders

AGENCY: Enforcement and Compliance, International Trade Administration, Department of Commerce.

SUMMARY: As a result of these expedited sunset reviews, the U.S. Department of Commerce (Commerce) finds that revocation of the countervailing duty (CVD) orders on biodiesel from Argentina and Indonesia would be likely to lead to continuation or recurrence of countervailable subsidies at the levels indicated in the “Final Results of Sunset Review” section of this notice.

DATES: Applicable April 5, 2023.

FOR FURTHER INFORMATION CONTACT: Mark Hoadley, AD/CVD Operations, Office VII, Enforcement and Compliance, International Trade Administration, U.S. Department of Commerce, 1401 Constitution Avenue NW, Washington, DC 20230; telephone: (202) 482–3148.

SUPPLEMENTARY INFORMATION:

Background

On January 4, 2018, Commerce published the CVD orders on biodiesel from Argentina and Indonesia.¹ On March 1, 2022, Commerce published the notice of initiation of the first sunset reviews of the *Orders*, pursuant to section 751(c) of the Tariff Act of 1930, as amended (the Act).² Commerce received a timely notice of intent to participate from Clean Fuels Alliance Fair Trade Coalition³ (Coalition) (the

¹ See *Biodiesel from the Republic of Argentina and the Republic of Indonesia: Countervailing Duty Orders*, 83 FR 522 (January 4, 2018) (*Orders*).

² See *Initiation of Five-Year (Sunset) Reviews*, 87 FR 11416 (March 1, 2022).

³ The Coalition members are: Clean Fuels Alliance America; Ag Processing Inc. a cooperative; Kolmar Americas, Inc.; Archer Daniels Midland Company; Cape Cod Biofuels; Crimson Renewable Energy LP; Minnesota Soybean Processors; Seaboard Energy, Inc.; Iowa Renewable Energy, LLC; Lake Erie Biofuels dba HERO BX; Renewable Biofuels, LLC; Renewable Energy Group, Inc.; Western Dubuque Biodiesel, LLC; Western Iowa Energy, LLC; World Energy, LLC; and Thumb BioEnergy LLC.

domestic interested party) within the deadline specified in 19 CFR 351.218(d)(1)(i).⁴ The domestic interested party claimed interested party status under section 771(9)(F) of the Act, as an association, a majority of whose members are manufacturers, producers, or wholesalers of a domestic like product in the United States.

Commerce received a substantive response from the domestic interested party within the 30-day deadline specified in 19 CFR 351.218(d)(3)(i).⁵ Commerce received no substantive response from any other interested parties in these proceedings. On January 25, 2023, Commerce notified the U.S. International Trade Commission that it did not receive adequate substantive responses from any respondent interested party in these proceedings.⁶ As a result, pursuant to section 751(c)(3)(B) of the Act and 19 CFR 351.218(e)(1)(ii)(C)(2), Commerce determined that the respondent interested party did not provide an adequate response to the notice of initiation and, therefore, Commerce conducted an expedited (120-day) sunset review of the *Orders*.

Scope of the Orders

The product covered by the *Orders* is biodiesel from Argentina and Indonesia. For a complete description of the scope of the *Orders*, see the Issues and Decision Memoranda.⁷

⁴ See Domestic Interested Party’s Letter, “Five-Year (“Sunset”) Review of Antidumping and Countervailing Duty Orders on Biodiesel from Argentina: Notice of Intent to Participate,” dated December 16, 2022; see also Domestic Interested Party’s Letter, “Five-Year (“Sunset”) Review of Antidumping and Countervailing Duty Orders on Biodiesel from Indonesia: Notice of Intent to Participate,” dated December 16, 2022.

⁵ See Domestic Interested Party’s Letters, “Biodiesel from Argentina: Substantive Response of the Clean Fuels Alliance Fair Trade Coalition to Commerce’s Notice of Initiation of the First Five Year (“Sunset”) Review of the Countervailing Duty Order,” dated January 3, 2023 (Domestic Interested Party’s Argentina Substantive Response); and “Biodiesel from Indonesia: Substantive Response of the Clean Fuels Alliance Fair Trade Coalition to Commerce’s Notice of Initiation of the First Five Year (“Sunset”) Review of the Countervailing Duty Order,” dated January 3, 2023 (Domestic Interested Party’s Indonesia Substantive Response).

⁶ See Commerce’s Letter, “Sunset Reviews Initiated December 1, 2022,” dated January 25, 2023.

⁷ See Memorandum, “Issues and Decision Memorandum for the Expedited First Sunset Review of the Countervailing Duty Order on Biodiesel from Argentina,” dated concurrently with, and hereby adopted by, this notice; see also Issues and Decision Memorandum for the Expedited First Sunset Review of the Countervailing Duty Order on Biodiesel from Indonesia,” dated concurrently with, and hereby adopted by, this notice (collectively, Issues and Decision Memoranda).

Analysis of Comments Received

All issues raised in these sunset reviews are addressed in the Issues and Decision Memoranda. A list of topics discussed in each Issues and Decision Memoranda is included as the appendix to this notice. The Issues and Decision Memoranda are public documents and are on file electronically via the Enforcement and Compliance’s Antidumping and Countervailing Duty Centralized Electronic Service System (ACCESS). ACCESS is available to registered users at <https://access.trade.gov>. In addition, complete versions of the Issues and Decision Memoranda can be accessed directly at <https://access.trade.gov/public/FRNoticesListLayout.aspx>.

Final Results of Sunset Reviews

Pursuant to sections 751(c)(1) and 752(b) of the Act, Commerce determines that revocation of the CVD order on biodiesel from Argentina would be likely to lead to continuation or recurrence of countervailable subsidies at the following rates:

Company	Subsidy rate (percent <i>ad valorem</i>)
LDC Argentina S.A. ⁸	72.28
Vicentin S.A.I.C. ⁹	71.45
All Others	71.87

Pursuant to sections 751(c)(1) and 752(b) of the Act, Commerce determines that revocation of the CVD order on biodiesel from Indonesia would be likely to lead to continuation or recurrence of countervailable subsidies at the following rates:

Company	Subsidy rate (percent <i>ad valorem</i>)
Wilmar Trading Co., Ltd	34.45
PT Musim Mas	64.73
All Others	38.95

Administrative Protective Order (APO)

This notice also serves as the only reminder to parties subject to an APO of their responsibility concerning the return or destruction of proprietary information disclosed under APO in accordance with 19 CFR 351.305. Timely notification of the return or

⁸ In the final determination of the CVD investigation, Commerce found the following companies to be cross-owned with LDC Argentina S.A.: LDC Semillas S.A. and Semillas del Rosario S.A. See *Orders*, 83 FR at 522.

⁹ In the final determination of the CVD investigation, Commerce found the following companies to be cross-owned with Vicentin S.A.I.C.: Oleaginosa San Lorenzo S.A. and Los Amores S.A. See *Orders*, 83 FR at 522.

destruction of APO materials or conversion to judicial protective order is hereby requested. Failure to comply with the regulations and terms of an APO is a violation which is subject to sanction.

Notification to Interested Parties

Commerce is issuing and publishing the final results and this notice in accordance with sections 751(c), 752(b), and 777(i)(1) of the Act, and 19 CFR 351.218(e)(1)(ii)(C)(2).

Dated: March 29, 2023.

Abdelali Elouaradia,
Deputy Assistant Secretary for Enforcement and Compliance.

Appendix

List of Topics Discussed in the Issues and Decision Memoranda

- I. Summary
- II. Background
- III. Scope of the *Order*
- IV. History of the *Order*
- V. Legal Framework
- VI. Discussion of the Issues
 - 1. Likelihood of Continuation or Recurrence of Countervailable Subsidies
 - 2. Net Countervailable Subsidy Rates Likely to Prevail
 - 3. Nature of the Subsidies
- VII. Final Results of Sunset Review
- VIII. Recommendation

[FR Doc. 2023–07040 Filed 4–4–23; 8:45 am]

BILLING CODE 3510–DS–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

Notice of Intent To Conduct Scoping and To Prepare a Draft Environmental Impact Statement for the Proposed Atchafalaya National Estuarine Research Reserve

AGENCY: Office for Coastal Management, National Ocean Service (NOS), National Oceanic and Atmospheric Administration (NOAA), U.S. Department of Commerce.

ACTION: Notice of Intent to prepare a draft environmental impact statement and hold public scoping meetings; request for comments.

SUMMARY: In accordance with Section 315 of the Coastal Zone Management Act of 1972, as amended, and the National Environmental Policy Act of 1969, as amended, NOAA and the State of Louisiana (the State) intend to prepare a Draft Environmental Impact Statement (DEIS) and Draft Management Plan (DMP) for the proposed Atchafalaya National Estuarine Research Reserve (NERR). NOAA and the State

also announce two public scoping meetings to solicit comments on significant issues related to the development of a DEIS for the proposed Atchafalaya NERR.

DATES: An in-person meeting will be held on Thursday, April 20, 2023 at 5 p.m. Central Daylight Time (CDT). A virtual meeting will be held on Tuesday, April 25, 2023 at 12 p.m. CDT. Written comments provided electronically must be submitted no later than Monday, May 15, 2023; written comments submitted by mail must be postmarked by Monday, May 15, 2023.

ADDRESSES: The public scoping meeting on Thursday, April 20, 2023 will be conducted at the Morgan City Municipal Auditorium; 728 Myrtle Street, Morgan City, Louisiana 70380 at 5 p.m. CDT. This meeting will be in-person only and not broadcast. The public scoping meeting on Tuesday, April 25, 2023 will be held virtually at the following link: <https://www.youtube.com/@louisianacpra5300/streams> at 12 p.m. CDT. Participants will be able to provide written comments during the virtual meeting. Meeting documents will be available on the Coastal Protection and Restoration Authority's NERR website: <https://coastal.la.gov/our-work/key-initiatives/atchafalaya-national-estuarine-research-reserve/>, as well as on the Federal eRulemaking Portal: <https://www.regulations.gov/docket/NOAA-NOS-2023-0050>. Written comments may be submitted by:

- **Electronic Submission:** Submit all electronic public comments via the Federal eRulemaking Portal. Go to <https://www.regulations.gov/docket/NOAA-NOS-2023-0050>, click the "Comment Now!" button, complete the required fields, and enter or attach your comments. Written comments must be submitted no later than 11:59 p.m. Eastern Daylight Time on Monday, May 15, 2023.

- **Mail:** Submit written comments to Kristin Ransom, Stewardship Division, Office for Coastal Management, NOS, NOAA, 1021 Balch Boulevard, Stennis Space Center, Mississippi, 39529; ATTN: Atchafalaya NERR. Comments must be postmarked no later than Monday, May 15, 2023.

Instructions: All comments received are part of the public record and will be posted for public viewing on <https://www.regulations.gov/docket/NOAA-NOS-2023-0050> with no changes. All personally identifiable information (e.g., name, address, etc.), confidential business information, or otherwise sensitive information submitted voluntarily by the commenter will be publicly accessible and maintained by

NOAA as part of the public record. NOAA will accept anonymous comments; on the eRulemaking Portal, enter "N/A" in the required fields if you wish to remain anonymous. If you would like to submit an anonymous comment during the in-person meeting, a comment box along with paper and writing implements will be provided. Multimedia submissions (i.e., audio, video, etc.) must be accompanied by a written comment. The written comment is considered the official comment and should include discussion of all points you wish to make. NOAA will generally not consider comments, or comment contents, located outside of the primary submission sites or addresses (i.e., those posted on the web, cloud, or other file-sharing system). Please note that no public comments will be audio or video recorded by NOAA or the State.

Closed captioning will be provided for those who attend the virtual public meeting through the meeting link:

<https://www.youtube.com/@louisianacpra5300/streams>.

FOR FURTHER INFORMATION CONTACT: Kristin Ransom, Stewardship Division, Office for Coastal Management, NOS, NOAA, 1021 Balch Boulevard, Stennis Space Center, Mississippi, 39529; ATTN: LA NERR. Phone: 601-568-1091-; or Email: kristin.ransom@noaa.gov.

SUPPLEMENTARY INFORMATION: In accordance with Section 315 of the Coastal Zone Management Act of 1972, as amended, and its implementing regulations (15 CFR part 921), and the National Environmental Policy Act of 1969, as amended, and its implementing regulations (40 CFR part 1500), NOAA and the State intend to prepare a DEIS for the proposed Atchafalaya NERR. Early in the development of the DEIS, NOAA and the State are required to hold a scoping meeting to solicit public and government comments on significant issues related to this proposed action. (15 CFR 921.13(c)).

NOAA received the State's nomination of the proposed site on June 29, 2022. NOAA evaluated the nomination package and found that the proposed site met the NERR System requirements. NOAA informed the State on March 22, 2023 that it was accepting the nomination and that the next step would be to prepare a DEIS and DMP. The DEIS will assess the potential impact of designating the State's recommended site as a National Estuarine Research Reserve site, and identify boundary alternatives. The DMP will set a course for operating the Atchafalaya NERR if approved and will include plans for administration,

research, education, and facilities of the proposed site. (See 15 CFR 921.13.)

The proposed site consists of the following State-owned properties: Lake Fausse Pointe State Park, Attakapas Island Wildlife Management Area, Atchafalaya Delta Wildlife Management Area, and Marsh Island Wildlife Refuge; public trust waters including portions of the Atchafalaya River, Atchafalaya Bay, East and West Cote Blanche Bays, and Vermilion Bay.

The proposed site resulted from a comprehensive evaluation process that sought the views of the public, affected landowners, and other interested parties. The state held informal, widely-publicized town hall meetings statewide in February 2022 to describe the NERR system, explain the rationale for establishing a reserve in Louisiana, and outline a process for selecting and nominating a site to NOAA. The state assembled a Site Development Committee composed of State agency representatives, academia, non-governmental organizations, members of the public, and federal agencies. The team conducted preliminary screening, detailed screening, and scoring of potential sites that led to the preferred site. The State and NOAA held public hearings on November 2 and 3, 2022 to solicit comments on the proposed site. For more detailed information on the site selection process and the proposed site, see the Louisiana Coastal Protection and Restoration Authority's NERR website: <https://coastal.la.gov/our-work/key-initiatives/atchafalaya-national-estuarine-research-reserve/>. Federal Domestic Assistance Catalog Number 11.420, (Coastal Zone Management) Research Reserves.

Authority: 16 U.S.C. 1461.

Keelin Kuipers,

Deputy Director, Office for Coastal Management, National Ocean Service, National Oceanic and Atmospheric Administration.

[FR Doc. 2023-07056 Filed 4-4-23; 8:45 am]

BILLING CODE 3510-08-P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

Agency Information Collection Activities; Submission to the Office of Management and Budget (OMB) for Review and Approval; Comment Request; NOAA Space-Based Data Collection System (DCS) Agreements

The Department of Commerce will submit the following information collection request to the Office of

Management and Budget (OMB) for review and clearance in accordance with the Paperwork Reduction Act of 1995, on or after the date of publication of this notice. We invite the general public and other Federal agencies to comment on proposed, and continuing information collections, which helps us assess the impact of our information collection requirements and minimize the public's reporting burden. Public comments were previously requested via the **Federal Register** on January 20, 2023 during a 60-day comment period. This notice allows for an additional 30 days for public comments.

Agency: National Oceanic and Atmospheric Administration (NOAA), Commerce.

Title: NOAA Space-Based Data Collection System (DCS) Agreements.

OMB Control Number: 0648–0157.

Form Number(s): None.

Type of Request: Regular submission (extension of a current information collection).

Number of Respondents: 225.

Average Hours per Response: GOES DCS Use Agreement and Argos DCS Use Agreement—0.5 hours.

Total Annual Burden Hours: 113.

Needs and Uses: The National Oceanic and Atmospheric Administration (NOAA) operates two space-based data collection systems (DCS) per 15 CFR part 911: the Geostationary Operational Environmental Satellite (GOES) DCS and the Polar-Orbiting Operational Environmental Satellite (POES) DCS, also known as the Argos system. Both the GOES DCS and the Argos DCS are operated to support environmental applications, *e.g.*, meteorology, oceanography, hydrology, ecology, and remote sensing of Earth resources. In addition, the Argos DCS currently supports applications related to protection of the environment, *e.g.*, hazardous material tracking, fishing vessel tracking for treaty enforcement, and animal tracking. Presently, the majority of users of these systems are government agencies and researchers and much of the data collected by both the GOES DCS and the Argos DCS are provided to the World Meteorological Organization via the Global Telecommunication System for inclusion in the World Weather Watch Program.

Current loading on both of the systems does not use the entire capacity of that system, so NOAA is able to make its excess capacity available to other users who meet certain criteria. Applications are made in response to the requirements in 15 CFR 911 (under the authority of 15 U.S.C. 313, Duties of

the Secretary of Commerce and others), using system use agreement (SUA) forms. The application information received is used to determine if the applicant meets the criteria for use of the system. The system use agreements contain the following information: (1) the period of time the agreement is valid and procedures for its termination, (2) the authorized use(s) of the DCS, and its priorities for use, (3) the extent of the availability of commercial services which met the user's requirements and the reasons for choosing the government system, (4) any applicable government interest in the data, (5) required equipment standards, (6) standards of operation, (7) conformance with applicable International Telecommunication Union (ITU) and Federal Communications Commission (FCC) agreements and regulations, (8) reporting time and frequencies, (9) data formats, (10) data delivery systems and schedules and (11) user-borne costs.

Accepted applicants use the NOAA DCS to collect environmental data and in limited cases, non-environmental data via the Argos DCS, to support other governmental and non-governmental research or operational requirements, such as for law enforcement purposes. The applicants must submit information to ensure that they meet these criteria. NOAA does not approve agreements where there is a commercial service available to fulfill the user requirements (per 15 CFR part 911).

Affected Public: Not-for-profit institutions; Federal Government; State, local, or Tribal government; business or other for-profit organizations.

Frequency: Annual, every 3 years, every 5 years (per regulations).

Respondent's Obligation: Required to obtain or maintain benefits.

Legal Authority: 15 CFR 911.

This information collection request may be viewed at www.reginfo.gov. Follow the instructions to view the Department of Commerce collections currently under review by OMB.

Written comments and recommendations for the proposed information collection should be submitted within 30 days of the publication of this notice on the following website www.reginfo.gov/public/do/PRAMain. Find this particular information collection by selecting "Currently under 30-day Review—Open for Public Comments" or by using the search function and

entering either the title of the collection or the OMB Control Number 0648–0157.

Sheleen Dumas,

Department PRA Clearance Officer, Office of the Under Secretary for Economic Affairs, Commerce Department.

[FR Doc. 2023–07083 Filed 4–4–23; 8:45 am]

BILLING CODE 3510–HR–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

[RTID 0648–XC878]

Takes of Marine Mammals Incidental To Specified Activities; Taking Marine Mammals Incidental to the Replacement of Pier 3 at Naval Station Norfolk in Norfolk, Virginia

AGENCY: National Marine Fisheries Service (NMFS), National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Notice; issuance of renewal incidental harassment authorization (IHA).

SUMMARY: In accordance with the regulations implementing the Marine Mammal Protection Act (MMPA), as amended, notification is hereby given that NMFS has issued a renewal IHA to the U.S. Navy to harass marine mammals incidental to construction activities associated with the replacement of Pier 3 at Naval Station Norfolk in Norfolk, Virginia.

DATES: This renewal IHA is effective from April 1, 2023 through March 21, 2024.

FOR FURTHER INFORMATION CONTACT: Jessica Taylor, Office of Protected Resources, NMFS, (301) 427–8401. Electronic copies of the original application, renewal request, and supporting documents (including NMFS **Federal Register** notices of the original proposed and final authorizations, and the previous IHA), as well as a list of the references cited in this document, may be obtained online at: <https://www.fisheries.noaa.gov/permit/incidental-take-authorizations-under-marine-mammal-protection-act>. In case of problems accessing these documents, please call the contact listed above.

SUPPLEMENTARY INFORMATION:

Background

The Marine Mammal Protection Act (MMPA) prohibits the "take" of marine mammals, with certain exceptions. Sections 101(a)(5)(A) and (D) of the MMPA (16 U.S.C. 1361 *et seq.*) direct the Secretary of Commerce (as delegated

to NMFS) to allow, upon request, the incidental, but not intentional, taking of small numbers of marine mammals by U.S. citizens who engage in a specified activity (other than commercial fishing) within a specified geographical region if certain findings are made and either regulations are issued or, if the taking is limited to harassment, an incidental harassment authorization is issued.

Authorization for incidental takings shall be granted if NMFS finds that the taking will have a negligible impact on the species or stock(s) and will not have an unmitigable adverse impact on the availability of the species or stock(s) for taking for subsistence uses (where relevant). Further, NMFS must prescribe the permissible methods of taking and other “means of effecting the least practicable adverse impact” on the affected species or stocks and their habitat, paying particular attention to rookeries, mating grounds, and areas of similar significance, and on the availability of such species or stocks for taking for certain subsistence uses (referred to here as “mitigation measures”). Monitoring and reporting of such takings are also required. The meaning of key terms such as “take,” “harassment,” and “negligible impact” can be found in section 3 of the MMPA (16 U.S.C. 1362) and the agency’s regulations at 50 CFR 216.103.

NMFS’ regulations implementing the MMPA at 50 CFR 216.107(e) indicate that IHAs may be renewed for additional periods of time not to exceed 1 year for each reauthorization. In the notice of proposed IHA for the initial authorization, NMFS described the circumstances under which we would consider issuing a renewal for this activity, and requested public comment on a potential renewal under those circumstances. Specifically, on a case-by-case basis, NMFS may issue a one-time 1-year renewal IHA following notice to the public providing an additional 15 days for public comments when (1) up to another year of identical, or nearly identical, activities as described in the Detailed Description of Specified Activities section of the initial IHA issuance notice is planned or (2) the activities as described in the Description of the Specified Activities and Anticipated Impacts section of the initial IHA issuance notice would not be completed by the time the initial IHA expires and a renewal would allow for completion of the activities beyond that described in the **DATES** section of the notice of issuance of the initial IHA, provided all of the following conditions are met:

1. A request for renewal is received no later than 60 days prior to the needed

renewal IHA effective date (recognizing that the renewal IHA expiration date cannot extend beyond 1 year from expiration of the initial IHA).

2. The request for renewal must include the following:

- An explanation that the activities to be conducted under the requested renewal IHA are identical to the activities analyzed under the initial IHA, are a subset of the activities, or include changes so minor (e.g., reduction in pile size) that the changes do not affect the previous analyses, mitigation and monitoring requirements, or take estimates (with the exception of reducing the type or amount of take).

- A preliminary monitoring report showing the results of the required monitoring to date and an explanation showing that the monitoring results do not indicate impacts of a scale or nature not previously analyzed or authorized.

3. Upon review of the request for renewal, the status of the affected species or stocks, and any other pertinent information, NMFS determines that there are no more than minor changes in the activities, the mitigation and monitoring measures will remain the same and appropriate, and the findings in the initial IHA remain valid.

An additional public comment period of 15 days (for a total of 45 days), with direct notice by email, phone, or postal service to commenters on the initial IHA, is provided to allow for any additional comments on the proposed renewal. A description of the renewal process may be found on our website at: www.fisheries.noaa.gov/national/marine-mammal-protection/incidental-harassment-authorization-renewals.

History of Request

On March 15, 2022, NMFS issued an IHA to the United States Navy (Navy) to take marine mammals incidental to the replacement of Pier 3 at Naval Station Norfolk in Norfolk, Virginia (87 FR 15945), effective from April 1, 2022 through March 31, 2023. On July 29, 2022, NMFS received a request from the Navy for a modification to the Pier 3 replacement project IHA due to a change in the construction contractor’s plan to include concurrent pile driving and drilling activities, and a modified IHA was issued to the Navy on January 18, 2023 (88 FR 2880). Hereafter, any references to the initial IHA (as modified) refer to the modified IHA issued on January 18, 2023, while the 2022 IHA will be referred to as the 2022 initial IHA. On February 23, 2023, NMFS received a request for the renewal of the initial IHA (as modified).

After discussion with the Navy, NMFS received a final revised request to renew the initial IHA (as modified) on March 7, 2023. As described in that request, the activities for which incidental take is authorized consist of a subset of the identical activities covered in the initial authorization (as modified). As required, the applicant also provided a preliminary monitoring report (available at <https://www.fisheries.noaa.gov/action/incidental-take-authorization-replacement-pier-3-naval-station-norfolk-norfolk-virginia>) which confirms that the applicant has implemented the required mitigation and monitoring, and which also shows that no impacts of a scale or nature not previously analyzed or authorized have occurred as a result of the activities conducted. There are no changes from the proposed authorization to the final authorization.

Description of the Specified Activities and Anticipated Impacts

The Navy is replacing Pier 3 at Naval Station (NAVSTA) Norfolk in Norfolk, VA. The existing Pier 3 is being demolished and a new Pier 3 will be constructed immediately north of the existing location (see Figure 1 in the **Federal Register** notice for the proposed 2022 initial IHA; 87 FR 3976, January 26, 2022). Work at Pier 4, Pier 3T, and the bulkheads associated with Pier 3 and 3T is necessary to support the Pier 3 replacement. Pier 3 has been in a deteriorated state and does not provide minimum operation requirements for NAVSTA Norfolk. In-water work associated with Pier 4, including timber pile removal and concrete pile installation, has been completed under the 2022 initial IHA. In addition, concrete pile removal at Pier 3T will be completed by the expiration of the initial IHA. However, in-water work associated with construction of the CEP-176 and CEP-175 bulkheads, the CEP-102 bulkhead and relieving platform, and the new Pier 3, as well as installation of piles necessary for Pier 3T, will not be completed by the expiration date of the initial IHA (as modified). During the renewal period, the activities that will occur are the same as previously analyzed under the initial IHA (as modified). These activities include the installation of 42-inch (1.07 meters (m)) steel pipe piles, 28-inch (0.71 m) steel sheet piles, 13-inch (0.33 m) polymeric piles, and 24-inch (0.61 m) precast concrete piles. Pre-drilling may be used to set the piles to depth. The remaining in-water construction associated with these activities is planned to occur from April 1, 2023 through June 30, 2023.

Under the 2022 initial IHA, Level A and Level B harassment resulting from pile driving and drilling activities was authorized for harbor seals (*Phoca vitulina*), gray seals (*Halichoerus grypus*), and harbor porpoises (*Phocoena phocoena*). Level B harassment only resulting from pile driving and drilling activities was authorized for bottlenose dolphins (*Tursiops truncatus*) and humpback whales (*Megaptera novaeangliae*). Neither the Navy nor NMFS expects serious injury or mortality to result from this activity and, therefore, a renewal IHA is appropriate.

The following documents are referenced in this notification and include important supporting information:

- 2023 final initial IHA (as modified) (88 FR 2880, January 18, 2023);
- 2023 proposed initial IHA (as modified) (87 FR 75600, December 9, 2022);
- 2022 final initial IHA (87 FR 15945, March 21, 2022); and
- 2022 proposed initial IHA (87 FR 3976, January 26, 2022).

The 2022 initial IHA application, IHA modification request, 2022 initial IHA, initial IHA (as modified), and references are available at <https://www.fisheries.noaa.gov/action/incidental-take-authorization-replacement-pier-3-naval-station-norfolk-norfolk-virginia>.

Detailed Description of the Activity

A detailed description of the construction activities may be found in the **Federal Register** notice associated with the issuance of the 2022 initial IHA (87 FR 3976, January 26, 2022). A description of the concurrent pile driving activities associated with the initial IHA (as modified) may be found in the **Federal Register** notice of issuance of the initial IHA (as modified) (88 FR 2880, January 18, 2023). The location, timing, and nature of the activities, including the types of equipment planned for use, are identical to those described in the previous notices.

At the time of the renewal request, the following individual activities have been completed for the following structures:

- Pier 4
 - Vibratory removal of 36 14-inch timber piles; and
 - Pre-drilling and impact installation of 36 24-inch precast concrete square piles.

- Pier 3T
 - Vibratory removal of 87 14-inch timber piles; and
 - Vibratory removal of 196 18-inch precast concrete square piles.

At the time of the renewal request, the following concurrent activities have been completed for the following structures:
- Pier 3T and Pier 4
 - Vibratory removal of 14-inch timber and 18-inch concrete piles and impact installation of 24-inch concrete piles; and
 - Vibratory removal of 14-inch timber and 18-inch concrete piles and rotary drill of 24-inch concrete piles, with 90 concrete piles remaining as noted about for Pier 3T.

- Pier 3T and Pier 3
 - Vibratory removal of 14-inch timber and 18-inch concrete piles and impact installation of 24-inch concrete piles, with four concrete piles remaining to be installed.

A detailed description of the planned in-water individual activities and concurrent activities is provided in the **Federal Register** notice for the proposed renewal IHA (88 FR 15675, March 14, 2023). Since that time, no changes have been made to the planned in-water construction activities. Therefore, a detailed description is not provided here. Please refer to that **Federal Register** notice for the description of the specific activities.

Description of Marine Mammals

A description of the marine mammals in the area of the activities for which take is authorized, including information on abundance, status, distribution, and hearing, may be found in the notice of the proposed IHA for the initial authorization (87 FR 3976, January 26, 2022). NMFS has reviewed the monitoring data from the initial IHA (as modified), recent draft Stock Assessment Reports, information on relevant Unusual Mortality Events, and other scientific literature, and determined that neither this nor any other new information affects which species or stocks have the potential to be affected or the pertinent information in the Description of the Marine Mammals in the Area of Specified Activities contained in the supporting documents for the 2022 initial IHA. The only changes indicated in the draft 2022 SARs are that the Potential Biological Removal value for the gray seal Western North Atlantic stock increased from 1,389 to 1,458, annual mortality and serious injury of the harbor porpoise Gulf of Maine/Bay of Fundy stock

decreased from 217 to 164, and humpback whale Gulf of Maine stock is no longer considered a strategic stock.

Potential Effects on Marine Mammals and Their Habitat

A description of the potential effects of the specified activity on marine mammals and their habitat for the activities for which take is authorized may be found in the notices of the proposed IHA for the 2022 initial authorization. NMFS has reviewed the monitoring data from the initial IHA (as modified), recent draft Stock Assessment Reports, information on relevant Unusual Mortality Events, and other scientific literature, and determined that neither this nor any other new information affects our initial analysis of impacts on marine mammals and their habitat.

Estimated Take

A detailed description of the methods and inputs used to estimate take for the specified individual activity are found in the notices of the proposed and final IHAs for the initial authorization (87 FR 3976, January 26, 2022; 87 FR 15945, March 21, 2022) and for the specified concurrent activities, in the notices of the proposed and final initial IHAs (as modified) (87 FR 75600, December 9, 2022; 88 FR 2880, January 18, 2023). Activities authorized under the renewal IHA are subject to the same sound propagation boundaries as those analyzed for the 2022 initial IHA and initial IHA (as modified). The analysis of sound source level and sound pressure level (SPL) propagation provided in the 2022 initial IHA and initial IHA (as modified) remain applicable to the activities covered in this renewal IHA. Marine mammal density/occurrence data applicable to this authorization remain unchanged from the 2022 initial IHA.

Similarly, the stocks taken, methods of take, and types of take remain unchanged from the previously issued initial IHA. The take calculation method also remains the same, with the exception of fewer days of activity than what was described in the initial IHA. The approximate total number of operational days for this renewal IHA is 90 days as compared to the 280 days required for the project under the initial IHA. The number of takes authorized through the renewal IHA are indicated below in Table 1.

The total take number for bottlenose dolphins was estimated using inshore seasonal densities provided in Engelhaupt *et al.* (2016) from vessel line-transect surveys near NAVSTA Norfolk and adjacent areas near Virginia

Beach, Virginia from August 2012 through August 2015. This density includes sightings inshore of the Chesapeake Bay from NAVSTA Norfolk west to the Thimble Shoals Bridge, and is the most representative density for the project area. NMFS multiplied the density of 1.38 dolphins per square kilometer by the Level B harassment zone area for each activity for the project, and then by the number of days associated with that activity (see Table 1). The Level B harassment zones increased as a result of concurrent pile driving activities; therefore, calculated Level B harassment exposure estimates also increased as a result. As described in the notice of the initial proposed and issued IHA, there is insufficient information on relative abundance to apportion the takes precisely to each of the three stocks in the area. Therefore, the same approach as used in previous projects (e.g., Hampton Roads Bridge

Tunnel project (86 FR 17458, April 2, 2021), and the U.S. Navy Norfolk Maintenance Rule (86 FR 24340, May 6, 2021)) was used to estimate the appointment of takes to each of the three bottlenose dolphin stocks that may be present in the area. Given that most of the Northern North Carolina Estuarine Stock (NNCES) are found in the Pamlico Sound Estuary, over 160 kilometers from Norfolk, we conservatively estimated that no more than 200 of the authorized takes will be from this stock. Since members of the northern migratory coastal and southern migratory coastal stocks are thought to occur in or near the Bay in greater numbers, we conservatively assume that no more than half of the remaining takes will accrue to either of these stocks. Additionally, a subset of these takes would likely be comprised of the Chesapeake Bay resident dolphins,

although the size of that population is unknown.

Based upon the methodology for estimating take for the initial IHA (as modified) (88 FR 2880, January 18, 2023), the Navy calculated potential exposure to Level A harassment for gray seals by assuming 20 percent of potential take events would be by Level A harassment. As only one take is estimated to occur under the renewal IHA, we assume that individual take will be by Level B harassment only. Therefore, the Navy did not request, and NMFS has not authorized, take by Level A harassment for gray seals.

The total taking by Level B harassment of all species is predicted to be the same or lower with concurrent activity scenarios due to a lower number of construction days for concurrent activities; therefore, the authorized take from individual activities represents the most conservative take estimate.

TABLE 1—AUTHORIZED TAKE AND PERCENT OF STOCK AUTHORIZED FOR TAKE

Species	Stock	Individual activities		Concurrent activities		Percent of stock ¹
		Level A	Level B	Level A	Level B	
Bottlenose dolphin	Western North Atlantic Coastal, Northern Migratory.	0	1,281	0	486	² 19.3
	Western North Atlantic Coastal, Southern Migratory.	0	1,280	0	485	² 34.1
	Northern North Carolina Estuarine	0	200	0	200	² 24.3
Harbor seal	Western North Atlantic	57	759	53	478	1.33
Gray seal	Western North Atlantic	0	1	0	1	0.004
Harbor porpoise ...	Gulf of Maine/Bay of Fundy	2	2	0	2	0.004
Humpback whale	Gulf of Maine	0	4	0	2	0.29

¹ Percent of stock calculation based upon the largest take calculation from either individual or concurrent activities.

² Assumes multiple repeated takes of same individuals from a portion of each stock representing small numbers.

Description of Mitigation, Monitoring, and Reporting Measures

The mitigation, monitoring, and reporting measures included as requirements in this authorization are identical to those included in the FR notice announcing the issuance of the 2022 initial IHA (87 FR 15945, March 21, 2022) for individual activities and the FR notice announcing the issuance of the initial IHA (as modified) (88 FR 2880, January 18, 2023) for concurrent activities, and the discussion of the least practicable adverse impact included in that document remains accurate. The same measures are included for this renewal and are summarized here:

- The Navy must implement shutdown zones for all pile driving and removal and drilling activities. Shutdown zones would vary based upon the activity type and marine mammal hearing group, as shown in Table 2 for individual activities and Table 3 for concurrent activities. The

Navy must shut down if any marine mammals come within hearing group-specific shutdown zones;

- The Navy must implement impact pile driving soft-starts at the beginning of each day’s impact pile driving and at any time following cessation of impact pile driving for a period of 30 minutes or more. To implement soft-start, contractors will be required to provide an initial set of three strikes from the hammer at reduced energy, followed by a 30-second waiting period, then two subsequent reduced energy strike sets;

- Protected Species Observers (PSOs) must monitor the entirety of all shutdown zones as well as Level B harassment zones to the extent practicable during all pile driving and removal and drilling activities. Monitoring must be conducted by a minimum of two PSOs for impact driving, and a minimum of three PSOs for vibratory and drilling activities;
- Pre-activity monitoring must begin prior to the start of daily in-water

construction activities or whenever a break in pile driving/removal of 30 minutes or longer occurs. Pre-activity and post-activity monitoring must take place for a period of 30 minutes prior to beginning construction activities and after construction activities are complete for the day;

- Acoustic monitoring shall include two underwater positions as well as be conducted in accordance with NMFS guidance for 10 percent of each type of activity that has not previously been monitored at NAVSTA Norfolk (see Table 4);

- The Navy must submit draft marine mammal and acoustic monitoring reports to NMFS within 90 days after the completion of pile driving and removal and drilling activities under the renewal IHA;

- The Navy must prepare and submit final monitoring reports within 30 days following resolution of comments on the draft reports from NMFS;

- The Navy must submit all PSO datasheets and/or raw sighting data (in a separate file from the Final Report referenced immediately above); and
- The Navy must report injured or dead marine mammals.

TABLE 2—SHUTDOWN AND HARASSMENT ZONES FOR INDIVIDUAL PILE DRIVING ACTIVITIES

Pile size, type, and method	Minimum shutdown zone (m)			Harassment zone (m) ¹
	Humpback whale	Porpoises	All other species	
Impact Driving, 42-inch Steel Pipe Pile	1,005	500	200	1000
Vibratory Driving, 42-inch Steel Pipe Pile	50	120	50	15,850
Impact Driving, 28-inch Steel Sheet Piles	775	500	200	2,520
Vibratory Driving, 28-inch Steel Sheet Piles	65	65	65	13,600
Impact Driving, 13-inch Polymeric Piles	30	30	30	10
Vibratory Driving, 13-inch Polymeric Piles	30	30	30	6,310
Impact Driving, 24-inch Concrete Piles	160	500	200	120
Vibratory Driving, 24-inch Concrete Piles	10	10	10	1,850

¹ Rounded to the nearest 10 m.

TABLE 3—SHUTDOWN AND HARASSMENT ZONES FOR CONCURRENT PILE DRIVING ACTIVITIES

Pile sizes, type, and method	Minimum shutdown zone (m)			Harassment zone (m) ¹
	Humpback whale	Porpoises	All other species	
Vibratory removal 18-inch concrete piles and vibratory installation 42-inch steel pipe piles	200	200	50	18,480
Vibratory removal 18-inch concrete piles and pre-drilling for preparation of 24-in concrete pile install	45	45	30	7,360

¹ Rounded to the nearest 10 m.

TABLE 4—ACOUSTIC MONITORING SUMMARY ¹

Pile type	Count	Method of install/removal	Number monitored
13-inch polymeric	9	Vibratory	5
13-inch polymeric	9	Impact	5
13-inch polymeric	9	Drilling	5
24-inch concrete	11	Impact	10
42-inch steel pipe	103	Impact	10
42-inch steel pipe	103	Vibratory	10
28-inch steel sheet	221	Impact	10
28-inch steel sheet	221	Vibratory	10

¹ Acoustic monitoring will be conducted for activities for which measurements are needed.

Comments and Responses

A notice of NMFS’ proposal to issue a renewal IHA to the U.S. Navy was published in the **Federal Register** on March 14, 2023 (88 FR 15675). That notice either described, or referenced descriptions of, the U.S. Navy’s activity, the marine mammal species that may be affected by the activity, the anticipated effects on marine mammals and their habitat, estimated amount and manner of take, and proposed mitigation, monitoring, and reporting measures. NMFS received one comment letter from a private citizen that was not relevant to the scope of the proposed action. No other comments were received.

Determinations

The renewal request consists of a subset of activities analyzed through the initial IHA and initial IHA (as modified) described above. The methods of determining estimated take, potential effects, and required mitigation, monitoring, and reporting have not changed.

NMFS has defined negligible impact as an impact resulting from the specified activity that cannot be reasonably expected to, and is not reasonably likely to, adversely affect the species or stock through effects on annual rates of recruitment or survival (50 CFR 216.103). In analyzing the effects of the activities for the initial IHA, NMFS determined that the Navy’s activities would have a negligible

impact on the affected species or stocks and that authorized take numbers of each species or stock were small relative to the relevant stocks (e.g., less than one-third the abundance of all stocks).

NMFS has concluded that there is no new information suggesting that our analysis or findings should change from those reached for the initial IHA (as modified). Based on the information and analysis contained here and in the referenced documents, NMFS has determined the following: (1) the required mitigation measures will effect the least practicable impact on marine mammal species or stocks and their habitat; (2) the authorized takes will have a negligible impact on the affected marine mammal species or stocks; (3) the authorized takes represent small numbers of marine mammals relative to

the affected stock abundances; (4) the Navy's activities will not have an unmitigable adverse impact on taking for subsistence purposes as no relevant subsistence uses of marine mammals are implicated by this action, and; (5) appropriate monitoring and reporting requirements are included.

National Environmental Policy Act

To comply with the National Environmental Policy Act of 1969 (NEPA; 42 U.S.C. 4321 *et seq.*) and NOAA Administrative Order (NAO) 216-6A, NMFS must review our proposed action (*i.e.*, the issuance of an IHA renewal) with respect to potential impacts on the human environment.

This action is consistent with categories of activities identified in Categorical Exclusion B4 (incidental take authorizations with no anticipated serious injury or mortality) of the Companion Manual for NOAA Administrative Order 216-6A, which do not individually or cumulatively have the potential for significant impacts on the quality of the human environment and for which we have not identified any extraordinary circumstances that would preclude this categorical exclusion. Accordingly, NMFS determined that the issuance of the initial IHA qualified to be categorically excluded from further NEPA review. NMFS has determined that the application of this categorical exclusion remains appropriate for this renewal IHA.

Endangered Species Act

Section 7(a)(2) of the Endangered Species Act of 1973 (ESA; 16 U.S.C. 1531 *et seq.*) requires that each Federal agency insure that any action it authorizes, funds, or carries out is not likely to jeopardize the continued existence of any endangered or threatened species or result in the destruction or adverse modification of designated critical habitat. To ensure ESA compliance for the issuance of IHAs, NMFS consults internally whenever we propose to authorize take for endangered or threatened species.

No incidental take of ESA-listed species is authorized or expected to result from this activity. Therefore, NMFS has determined that formal consultation under section 7 of the ESA is not required for this action.

Renewal

NMFS has issued a renewal IHA to the Navy for the take of marine mammals incidental to pile driving and drilling activities at NAVSTA Norfolk in Norfolk, VA, effective through March 31, 2024.

Dated: March 30, 2023.

Catherine Marzin,

Deputy Director, Office of Protected Resources, National Marine Fisheries Service.

[FR Doc. 2023-07026 Filed 3-31-23; 4:15 pm]

BILLING CODE 3510-22-P

DEPARTMENT OF COMMERCE

Patent and Trademark Office

[Docket No. PTO-P-2023-0008]

Patent Center Electronic Office Action Program

AGENCY: United States Patent and Trademark Office, Department of Commerce.

ACTION: Notice; request for comments.

SUMMARY: The United States Patent and Trademark Office (USPTO or Office) will begin transitioning to the Patent Center Electronic Office (e-Office) Action program upon publication of this notice. The Patent Center e-Office Action program is designed to modernize the e-Office action process and further streamline the USPTO's service delivery processes. Implementation of the Patent Center e-Office Action program is another step in the USPTO's transition to Patent Center, a more modern, user-friendly system that provides improved system performance and a more intuitive user experience. Once fully implemented, the Patent Center e-Office Action program will replace the existing e-Office Action program available to users of the Private Patent Application Information Retrieval (PAIR) system. In addition, the Patent Center e-Office Action program offers a new option for users to receive courtesy postcards by email (e-postcards) as a reminder that there are available USPTO communications that have not been viewed or downloaded. The USPTO is implementing the e-postcard option based on feedback from customers, particularly to reduce paper consumption and mitigate the impact of potential postal delays. Through this notice, the USPTO seeks public comments on eliminating the postal postcard for all Patent Center e-Office Action program users in the future. As with the existing program, participation in the Patent Center e-Office Action program is optional.

DATES: Comments must be received by June 5, 2023 to ensure consideration.

ADDRESSES: For reasons of government efficiency, comments must be submitted through the Federal eRulemaking Portal at www.regulations.gov. To submit comments via the portal, enter docket

number PTO-P-2023-0008 on the homepage and click "Search." The site will provide a search results page listing all documents associated with this docket. Find a reference to this document and click on the "Comment" icon, complete the required fields, and enter or attach your comments. Attachments to electronic comments will be accepted in Adobe® portable document format (PDF) or Microsoft Word® format. Because comments will be made available for public inspection, information that the submitter does not desire to make public, such as an address or phone number, should not be included in the comments.

Visit the Federal eRulemaking Portal for additional instructions on providing comments via the portal. If electronic submission of comments is not feasible due to a lack of access to a computer and/or the internet, please contact the USPTO using the contact information below for special instructions.

FOR FURTHER INFORMATION CONTACT:

Eugenia A. Jones, Senior Legal Advisor, Office of Patent Legal Administration, at 571-272-7727; or Kristie A. Mahone, Senior Legal Advisor, Office of Patent Legal Administration, at 571-272-9016; or patent.practice@uspto.gov. For technical questions, please contact the Patent Electronic Business Center (EBC) at 1-866-217-9197 (toll-free), 571-272-4100 (local), or ebc@uspto.gov. The Patent EBC is open from 6 a.m. to midnight ET, Monday-Friday.

SUPPLEMENTARY INFORMATION: In May 2009, the USPTO implemented the e-Office Action program as an option for all users of the Private PAIR system. See Electronic Office Action, 1343 Off. Gaz. Pat. Office 45 (June 2, 2009). Under the Private PAIR e-Office Action program, the USPTO emails applicants notifications of Office communications retrievable through Private PAIR, rather than mailing the communications through the United States Postal Service (USPS), with a few exceptions. Participants in the Private PAIR e-Office Action program are also sent a courtesy postcard through the USPS as a reminder when none of the new Office communications listed in the email notification have been viewed or downloaded within seven calendar days after the date of the email notification and at least one of the listed Office communications requires the applicant's reply.

On August 1, 2022, the USPTO replaced the public view of the PAIR system (Public PAIR) with Patent Center, which offers a single interface for electronic filing and the management of patent applications. Patent Center,

once fully developed, will replace EFS-Web and the Private PAIR system. Upon publication of this notice, the USPTO will begin migrating participants in the Private PAIR e-Office Action program to the Patent Center e-Office Action program by Customer Number to modernize the e-Office Action process and continue streamlining its service and delivery processes. Current Private PAIR participants will not be required to make any changes to their Customer Number to participate in the Patent Center program.

Under the Patent Center e-Office Action program, Patent Center will send an improved, easier-to-read email notification listing retrievable Office communications to participating users. Those users may view and download the listed Office communications in Patent Center. Users will also be sent a courtesy postcard through the USPS when none of the Office communications listed in the email notification have been viewed or downloaded in Patent Center within seven calendar days after the date of the notification and at least one of the listed Office communications requires the applicant's reply.

In addition to Patent Center's enhanced user interface experience, Patent Center e-Office Action program participants may choose to receive e-postcards. Once a participant elects to receive e-postcards, the USPTO will no longer mail courtesy postcards through the USPS if none of the Office communications have been viewed or downloaded in Patent Center within seven calendar days after the date of the email notification and at least one of the Office communications requires an applicant's reply. Instead, the USPTO will send a courtesy e-postcard, as discussed in item 5 below.

The USPTO will endeavor to migrate all participants from the Private PAIR e-Office Action program to the Patent Center e-Office Action program expeditiously. The transition is expected to be complete approximately four weeks from the publication of this notice. Participation in the Patent Center e-Office Action program will be optional. Participants may withdraw by following the procedure set forth in item 7 of this notice.

The following enumerated paragraphs revise the guidance for the Private PAIR program to incorporate the technical modifications arising from the implementation of the Patent Center e-Office Action program, as well as the new e-postcard option. The USPTO seeks comments on eliminating the postal postcard default option and will evaluate whether maintaining a postal

postcard is necessary based on feedback from the public. The USPTO will provide advance notice of the changes to the Patent Center e-Office Action program detailed in this notice.

1. Who may participate in the Patent Center e-Office Action program, and how should new users register?

Any registered attorney or agent of record, or a named inventor acting pro se, in a patent application that is associated with a Customer Number is eligible to participate in the Patent Center e-Office Action program by accessing Patent Center. To access Patent Center, the participant must have a registered MyUSPTO account linked to the participant's Customer Number. For information on the creation of a MyUSPTO account and the method for accessing Patent Center, please contact the Patent EBC.

To register for the Patent Center e-Office Action program and receive email notifications of subsequent Office communications, Patent Center users must:

- a. log in to Patent Center and select "Manage/Manage customer numbers";
- b. select the Customer Number to enroll;
- c. select "Edit";
- d. select the "Receive correspondence notification via Email" option within the "Edit customer" screen; and
- e. designate at least one email address to receive email notifications for Office communications issued in the applications associated with the Customer Number.

The user may designate up to three email addresses. After registration, Office communications entered by participating USPTO business units (see item 7 below) in each application associated with the Customer Number will be processed under the Patent Center e-Office Action program.

2. How does the Patent Center e-Office Action program work?

When one of the participating business units within the USPTO enters an Office communication in an application that is associated with a registered Customer Number, the USPTO will send an email notification to the designated email addresses. The email notification will contain the following information: (a) the date and time the USPTO sends the email notification, (b) the Customer Number, and (c) information regarding each new Office communication. The Office communication information will include: (i) the application number of the application in which the Office communication is entered; (ii) the

document code associated with the Office communication; (iii) the mailroom/notification date indicated on the form PTOL-90, which accompanies the Office communication (generally, any time period for reply set forth in the Office communication will commence on the mailroom/notification date (see item 4 below)); and (iv) the attorney docket number.

The Office communication will be available and retrievable immediately through Patent Center. The USPTO will not mail a paper copy of the Office communication. Upon receipt of the email notification, the participant can download or view the new Office communication by logging in to Patent Center and using either: (a) the "Workbench/View correspondence" option, or (b) the "Application Search" option, and accessing the "Documents & Transactions" tab.

If the user has multiple applications associated with the Customer Number, a single consolidated email notification will be sent to the user, and it will list all the new Office communications entered on that day in the applications associated with the Customer Number. An abridged version of the email notification that contains only data pertinent to an individual application will be scanned into that application file as part of the official record. The abridged email notification scanned into the application file will not contain information regarding other applications.

3. How often will a participant receive the email notification?

The USPTO will send an email notification to the designated email addresses only when there is a new Office communication in the applications associated with the participant's Customer Number. If there are multiple new Office communications entered in the applications on the same day, the participant will receive a single email notification listing all the new Office communications. Therefore, participants will receive a single email notification per day for each Customer Number when there is a new Office communication.

4. When does the time period for reply start?

Generally, any time period for reply set forth in the Office communication will commence on the mailroom/notification date indicated on the form PTOL-90 accompanying the Office communication. The mailroom/notification date is treated like the mailing date of a paper communication.

More specifically, for Office actions under 35 U.S.C. 132(a), the mailroom/notification date is the date of the notice under 35 U.S.C. 133. See Electronic Office Action, 1343 Off. Gaz. Pat. Office at 46. The mailroom/notification date will also be considered the date of mailing of the correspondence for all other purposes (e.g., 37 CFR 1.71(g)(2), 1.97(b), 1.701–1.705).

However, the 63-day time period set forth in 37 CFR 90.3 for filing a notice of appeal to the U.S. Court of Appeals for the Federal Circuit, or for commencing a civil action, begins on the date of the decision of the Patent Trial and Appeal Board (PTAB). The time period is not measured from the mailroom/notification date. See also 35 U.S.C. 142. Participants may request extensions of time pursuant to 37 CFR 90.3(c).

Once the participant receives an email notification, the USPTO highly recommends that the participant log in to Patent Center to view the new Office communication as soon as possible to determine whether the communication requires a reply and when the reply is due.

5. What is a courtesy postcard?

The USPTO will send a courtesy postcard notifying the applicant if none of the Office communications listed in the email notification are viewed or downloaded through Patent Center within seven calendar days after the date of the email notification and at least one of the Office communications requires an applicant's reply. The courtesy postcard will be mailed through the USPS to the correspondence address associated with the Customer Number, unless the participant opts to receive courtesy e-postcards.

Patent Center e-Office Action participants may opt to receive courtesy e-postcards rather than courtesy postcards mailed through the USPS. To elect between receiving postal postcards and e-postcards for subsequent email notifications, a Patent Center participant must:

- a. log in to Patent Center and select "Manage/Manage customer numbers";
- b. select the Customer Number to change the postcard notification method;
- c. select "Edit";
- d. select "Receive postcard notification via Email" for the e-postcard option; or
- e. select "Receive postcard notification via Postal mail" for the postal mail option within the "Edit customer" screen.

If a participant has elected to receive e-postcards, the USPTO will no longer

mail a courtesy postcard through the USPS if none of the Office communications have been viewed or downloaded in Patent Center within seven calendar days after the date of the email notification and at least one of the Office communications requires an applicant's reply. Courtesy e-postcards will be emailed to the same email addresses assigned to the Customer Number for the correspondence address.

The mailing or sending of a courtesy postcard will not restart any time period for reply. The time period for reply will continue to run from the mailroom/notification date indicated on the form PTOL-90 accompanying the Office communication.

6. What types of applications are included in the Patent Center e-Office Action program?

The program includes provisional applications filed under 35 U.S.C. 111(b); nonprovisional applications filed under 35 U.S.C. 111(a) (including utility, plant, design, and reissue applications); and international applications that have entered the national stage under 35 U.S.C. 371. International applications that have not entered the national stage in the United States, reexamination proceedings, and PTAB trial proceedings are not included in the program.

7. Which business units at the USPTO participate in the Patent Center e-Office Action program?

Participants will receive email notifications for all Office communications prepared by the following participating business units:

- a. Technology Centers (including the examining corps), which enter Office actions and notices, including notices of allowance;
- b. The Office of Patent Application Processing, which enters application formality review notices, including notices to file missing parts;
- c. The Office of Data Management (Pre-Grant Publications and Office of Publications), which enters notices of publication and issues patents;
- d. The PTAB for ex parte appeals of rejections of claims in patent applications;
- e. The Office of Petitions; and
- f. The Office of Licensing and Review.

Since several areas of the Office have independent mailing processes, participants will continue to receive paper mailings for communications prepared by the non-participating business units, including (but not limited to):

- a. The Patent Cooperation Treaty Operations Division, International Branch;
- b. The PTAB for trial proceedings and reexamination proceedings;
- c. The Central Reexamination Unit for ex parte reexamination and inter partes reexamination proceedings;
- d. The Office of Enrollment and Discipline; and
- e. The Office of the Solicitor.

8. Can a participant withdraw from the Patent Center e-Office Action program?

Participants may opt out of the program at any time. To change back to paper delivery of any subsequent Office communications, Patent Center users must:

- a. Log in to Patent Center and select the "Manage/Manage customer numbers" screen;
- b. Select the Customer Number to opt out;
- c. Select the "Edit" button; and
- c. Select the "Receive correspondence via Postal mail" option on the "Edit customer" screen.

Any Office communications prepared after the withdrawal is recognized by the USPTO will be mailed to the correspondence address associated with the application. However, if the Office communication has been prepared before the withdrawal is recognized by the USPTO, the Office communication may be processed under the email notification procedure. This means that the USPTO may send an email notification for the communication rather than mailing a paper copy of the communication. Prior to the completion of the withdrawal process, participants may receive some Office communications on paper (those that were prepared after the withdrawal was recognized) and email notifications for those that were prepared before the withdrawal was recognized. Therefore, it is important for the participants to check their designated email addresses for email notifications and review the Office communications via Patent Center, even after withdrawing from the program. Furthermore, the participants may receive courtesy postcards in the previously elected mode (postal postcard or e-postcard) for any unviewed communication (that has a time period for reply) for which an email notification was sent.

9. Can a participant change or add email addresses?

Participants may change email addresses at any time. To change or add an email address, a participant must:

- a. Log in to Patent Center and select "Manage/Manage Customer Number";

b. Select the “Edit” button; and
 c. Change or add the email address to receive email notifications for Office communications entered in the applications associated with the Customer Number. The participant may designate up to three email addresses. The Patent Center system will send a test email to each of the new email addresses associated with the Customer Number.

10. Who should a participant contact if an email notification for an Office communication has not been received?

The participant should contact the Patent EBC if an Office communication is available in Patent Center but the participant did not receive an email notification for the Office communication. The USPTO will take appropriate corrective actions. For example, the USPTO will send the participant an email notification if an email notification was not previously sent to the designated email addresses. Any time period for reply (except for the 63-day time period under 37 CFR 90.3) set forth in the Office communication will be restarted when the USPTO sends the email notification. For more information on the time period for reply, see item 4 above.

However, if the USPTO did send an email notification to each of the email addresses designated by the user, the USPTO will not send a new email notification, and any time period for reply set forth in the Office communication will not be restarted. The time period for reply will continue to run from the original mailroom/ notification date. Therefore, it is important for the user to designate the correct email addresses when signing up for the program.

11. Who should a participant contact if an improper communication has been scanned into the application?

The participant should contact the Patent EBC if an improper communication has been scanned into the application file, so that the USPTO can take appropriate corrective actions. For example, if the improper communication belongs to another application, the USPTO will move the communication to the correct application. The USPTO will send a new email notification when a proper communication is available and retrievable through Patent Center.

Please note that the document code corresponding to an Office communication identified on the email notification is informal (unofficial) information. If there is any discrepancy between the document code

corresponding to an Office communication identified on the email notification and the document code corresponding to the image of the communication available through Patent Center, the document code corresponding to the image of the Office communication available through Patent Center is the official record. The USPTO will not send a new email notification for an incorrect document code on the email notification.

If an Office communication contains an error that affects an applicant’s ability to reply to the Office communication and this error is called to the attention of the USPTO in writing within one month of the email date, the USPTO will follow the procedure set forth in section 710.06 of the Manual of Patent Examining Procedure (MPEP) (9th ed., rev. 7.2022, February 2023).

12. Who should the participant contact if the date of the email notification is a few days later than the mailroom/ notification date?

If the Office communication (e.g., an application filing receipt or a notice of publication) does not require a reply from an applicant and it does not have a time period for reply, it is not necessary for the participant to contact the Office. However, if the Office communication requires a reply and it sets forth a time period for reply, the participant should call the Patent EBC within one month from the email date so the USPTO can reset the time period for reply (except for the 63-day period under 37 CFR 90.3) to the original email date. For more information on the time period for reply, see item 4 above.

For example, an email notification sent on October 6, 2022, could indicate that an Office action with a mailroom/ notification date of October 3, 2022, has been entered in the application. The time period for reply set forth in the Office action commences on the mailroom/notification date (October 3, 2022). If the participant contacts the Patent EBC within one month from the email date (October 6, 2022), the USPTO will reset the time period for reply to commence on October 6, 2022.

13. How can a participant identify the email notification sent from the Office?

The email notification will have the following language in the subject line: “USPTO: Patent Electronic System—Correspondence Notification for Customer Number xxx.,” where “xxx” will be the participant’s Customer Number. The sender’s address will be “noreply@uspto.gov.” Any inquiries regarding the email notification should be directed to the Patent EBC.

Participants should not reply to the “noreply” email address.

14. Does the Patent Center e-Office Action program change the policy for communications via the internet?

By registering for the Patent Center e-Office Action program, a participant is authorizing the USPTO to send email notifications of Office communications entered by the participating USPTO business units in the applications associated with the Customer Number. The Patent Center e-Office Action program does not, otherwise, change the policy for communications via the internet as set forth in section 502.03 of the MPEP.

The Patent Center e-Office Action program does not alter the USPTO’s policy prohibiting an applicant or examiner from engaging in improper email correspondence. For example, the applicant may not send a reply to an Office action to the USPTO via email, and the examiner may not send an Office action to the applicant via email. See section 502.03 of the MPEP.

Katherine K. Vidal,

Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office.

[FR Doc. 2023-07087 Filed 4-4-23; 8:45 am]

BILLING CODE 3510-16-P

COMMODITY FUTURES TRADING COMMISSION

Privacy Act of 1974; System of Records

AGENCY: Commodity Futures Trading Commission.

ACTION: Notice of a modified system of records.

SUMMARY: This system includes records relevant to investigations conducted by the Office of the Inspector General (OIG), including but not limited to information regarding individuals who are part of an investigation or allegation pertaining to fraud and abuse concerning Commodity Futures Trading Commission (CFTC or Commission) programs and operations, internal staff memoranda, copies of all subpoenas issued during the investigation, affidavits, witness statements, and transcripts of testimony.

DATES: Comments must be received on or before May 5, 2023. New routine uses will go into effect on May 5, 2023.

ADDRESSES: You may submit comments identified as pertaining to “Office of the Inspector General Investigative Files” by any of the following methods:

- *CFTC Comments Portal*: <https://comments.cftc.gov>. Select the “Submit Comments” link for this notice and follow the instructions on the Public Comment Form.

- *Mail*: Send to Christopher Kirkpatrick, Secretary of the Commission, Commodity Futures Trading Commission, Three Lafayette Centre, 1155 21st Street NW, Washington, DC 20581.

- *Hand Delivery/Courier*: Follow the same instructions as for Mail, above. Please submit your comments using only one of these methods. Submissions through the CFTC Comments Portal are encouraged.

All comments must be submitted in English, or if not, be accompanied by an English translation. Comments will be posted as received to comments.cftc.gov. You should submit only information that you wish to make available publicly.

The Commission reserves the right, but shall have no obligation, to review, pre-screen, filter, redact, refuse, or remove any or all of a submission from comments.cftc.gov that it may deem to be inappropriate for publication, such as obscene language. All submissions that have been redacted or removed that contain comments on the merits of this notice will be retained in the comment file and will be considered as required under all applicable laws, and may be accessible under the Freedom of Information Act.

FOR FURTHER INFORMATION CONTACT:

Marcela Souaya, (202) 418–5137, privacy@cftc.gov, Office of the General Counsel, Commodity Futures Trading Commission, Three Lafayette Centre, 1155 21st Street NW, Washington, DC 20581.

SUPPLEMENTARY INFORMATION: This modification updates the routine uses for this system, rescinding the inheritance of the Commission’s “blanket routine uses” last published on March 14, 2001 at 76 FR 5973 and incorporates the routine uses that apply to the records maintained in CFTC–32. This modification updates and clarifies the Privacy Act exemptions promulgated for this system, and also makes conforming changes to align with format requirements in OMB Circular A–108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*.

SYSTEM NAME AND NUMBER:

Office of the Inspector General Investigative Files; CFTC–32.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Office of the Inspector General, Commodity Futures Trading Commission, Three Lafayette Centre, 1155 21st Street NW, Washington, DC 20581. The system will be hosted on a cloud and data center computing infrastructure. Duplicate versions of some or all system information may be at satellite locations where the CFTC has granted direct access to support CFTC operations, system backup, emergency preparedness, and/or continuity of operations.

SYSTEM MANAGER(S):

Inspector General, Office of the Inspector General, Commodity Futures Trading Commission, Three Lafayette Centre, 1155 21st Street NW, Washington, DC 20581, OIG@cftc.gov.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Commodity Exchange Act, 7 U.S.C. 1 *et seq.*, and regulations, rules or orders issued thereunder; Public Law 95–452, as amended, 5 U.S.C. app. 3.

PURPOSE(S) OF THE SYSTEM:

The purpose of this system is to enable the Office of the Inspector General to effectively and efficiently intake allegations and conduct investigations relating to the programs and operations of the CFTC.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals who are part of an allegation or investigation of fraud and abuse concerning Commission programs or operations.

CATEGORIES OF RECORDS IN THE SYSTEM:

This system includes all allegations, all correspondence relevant to the investigation; all internal staff memoranda, copies of all subpoenas issued during the investigation, affidavits, statement from witnesses, transcripts of testimony taken in the investigation and accompanying exhibits; documents and records or copies obtained during the investigation; incoming allegations and allegation development, opening reports, progress reports and closing reports; records documenting allegation and investigation file status.

RECORD SOURCE CATEGORIES:

Information in these records is supplied by: Individuals including, where practicable, those to whom the information relates; witnesses, corporations and other entities; records of individuals and of the Commission; records of other entities; Federal, foreign, State or local bodies and law enforcement agencies; documents,

correspondence relating to litigation, and transcripts of testimony; miscellaneous other sources including other nongovernmental sources and open source intelligence, including web-based communities, user-generated content, social-networking sites, wikis, blogs and news sources maintained on the Surface, Deep, and Dark web. The Surface Web is what users access in their regular day-to-day activity. It is available to the general public using standard search engines and can be accessed using standard web browsers that do not require any special configuration. The Deep Web is the portion of the web that is not indexed or searchable by ordinary search engines. The Dark Web is a less accessible subset of the Deep Web that relies on connections made between trusted peers and requires specialized software, tools, or equipment to access.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

These records and information in these records may be disclosed:

1. The information may be given or shown to any person or entity during the course of an Office of the Inspector General (OIG) audit or audit activity (audit) if there is reason to believe that disclosure to the person or entity will further the audit.

2. To the Department of Justice or other federal entity, the Merit Systems Protection Board, the Office of Special Counsel, or in a proceeding before a court, adjudicative body, or other administrative body before which the agency is authorized to appear, or in the course of civil discovery, litigation, or settlement negotiations, in actions authorized under the Commodity Exchange Act and otherwise authorized, when:
 - a. The agency, or any component thereof; or
 - b. Any employee of the agency in his or her official capacity; or
 - c. Any employee of the agency in his or her personal capacity where the Department of Justice or the agency has agreed to represent the employee; or
 - d. The United States, when the litigation is likely to affect the CFTC or any of its components; is a party to litigation or has an interest in such litigation, and the use of such records by the Department of Justice or the agency is deemed to be relevant and necessary to the litigation.

3. To a federal, state, local, tribal, foreign, or international agency in response to its request for information concerning the hiring or retention of an employee; the issuance of a security

clearance; the reporting of an investigation of an employee; the letting of a contract; or the issuance of a license, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

4. To a federal, state, local, tribal, foreign, or international agency, if necessary to obtain information relevant to the CFTC's decision concerning the hiring or retention of an employee; the issuance of a security clearance; the letting of a contract; or the issuance of a license, or other benefit.

5. In any case in which records in the system, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, whether arising by general statute or particular program statute, or by regulation, rule or order issued pursuant thereto, the relevant records may be referred to the appropriate agency, whether Federal, foreign, State or local, charged with enforcing or implementing the statute, regulation, rule or order. This includes a state or federal bar association, state accountancy board, or other federal, state, local, or foreign licensing or oversight authority; or professional association or self-regulatory authority to the extent that it performs similar functions (including the Public Company Accounting Oversight Board) for investigations or possible disciplinary action, including suspension and debarment.

6. To contractors, performing or working on a contract for the Federal government when necessary to accomplish an agency function.

7. To the Office of Government Ethics to comply with agency reporting requirements under the law, including 5 CFR part 2638, subpart F.

8. To a grand jury agent pursuant either to a Federal or State grand jury subpoena, or to a prosecution request that such record be released for the purpose of its introduction to a grand jury, provided that the grand jury channels its request through the cognizant U.S. Attorney, that the U.S. Attorney has been delegated the authority to make such requests by the Attorney General, and that the U.S. Attorney actually signs the letter specifying both the information sought and the law enforcement purpose served. In the case of a State grand jury subpoena, the State equivalent of the U.S. Attorney and Attorney General shall be substituted.

9. To a Federal agency in response to a subpoena issued by the Federal agency

having the power to subpoena records of other Federal agencies, provided the subpoena is channeled through the head of the issuing agency, if the OIG determines that: (a) The head of the issuing agency signed the subpoena; (b) the subpoena specifies the information sought and the law enforcement purpose served; (c) the records are both relevant and necessary to the proceeding; and (d) such release is compatible with the purpose for which the records were collected.

10. To the Department of Justice for the purpose of obtaining its advice on an OIG investigation, or other related inquiry, including Freedom of Information or Privacy Act matters relating to information in this record system.

11. To the extent authorized or required by law, information contained in this system of records may be disclosed to complainants, witnesses, victims, and/or individuals with relevant information (including experts), to the extent that it will not interfere with the investigation.

12. To any official charged with the responsibility to conduct investigations, qualitative assessment reviews, or peer reviews of investigative operations within the Office of the Inspector General. This disclosure category includes members of the Council of the Inspectors General on Integrity and Efficiency or any successor entity and officials, designees, and administrative staff within their chain of command, as well as authorized officials of the Department of Justice and the Federal Bureau of Investigation.

13. To the news media and general public where there exists a legitimate public interest, *e.g.*, to assist in the location of fugitives, to provide notification of arrests, where necessary for protection from imminent threat of life or property, or in accordance with guidelines set out by the Department of Justice.

14. To the Department of Justice as required by law pertaining to government-wide, uniform crime reporting.

15. To appropriate agencies, entities, and persons when (1) the Commission suspects or has confirmed that there has been a breach of the system of records, (2) the Commission has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the Commission (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Commission's

efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

16. To another Federal agency or Federal entity, when the Commission determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to Individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

17. Information may be disclosed to the National Archives and Records Administration to the extent necessary to fulfill its responsibilities under the law relating to these records.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records are stored in this system electronically or on paper in secure facilities.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Investigative files are retrieved by the subject matter of the investigation, individual investigated, or by case file number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

The Office of the Inspector General temporary Investigative Files and the index to the files are destroyed 10 years after the case is closed. Investigations that involve, as subjects, the Chairman, Commissioners, Division Directors, or Office Heads; or result in substantive changes in agency policy; or draw significant public interest as reflected in widespread news media attention, Congressional interest, and/or market participant inquiries are considered permanent records and forwarded to the National Archives 15 years after the case is closed.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Administrative safeguards include restricting access to the OIG work area, and restricting relevant investigative tasks to only those competent or qualified to perform the work. In addition, all users take annual security and privacy, and records management training. Technical security measures within CFTC include restrictions on computer access to authorized individuals who have a legitimate need to know the information; required use of strong passwords; multi-factor authentication for access to some CFTC

network components; use of encryption for certain data types and transfers; firewalls and intrusion detection applications; and regular review of security procedures and best practices to enhance security. Physical safeguards include restrictions on building access to authorized individuals, 24-hour security guard service, and maintenance of records in lockable offices and filing cabinets.

RECORD ACCESS PROCEDURES:

Individuals seeking to determine whether this system of records contains information about themselves or seeking access to records about themselves in this system of records should address written inquiries to the Office of the General Counsel, Commodity Futures Trading Commission, Three Lafayette Centre, 1155 21st Street NW, Washington, DC 20581. See 17 CFR 146.3 for full details on what to include in a Privacy Act access request.

CONTESTING RECORD PROCEDURES:

Individuals contesting the content of records about themselves contained in this system of records should address written inquiries to the Office of the General Counsel, Commodity Futures Trading Commission, Three Lafayette Centre, 1155 21st Street NW, Washington, DC 20581. See 17 CFR 146.8 for full details on what to include in a Privacy Act amendment request.

NOTIFICATION PROCEDURES:

Individuals seeking notification of any records about themselves contained in this system of records should address written inquiries to the Office of the General Counsel, Commodity Futures Trading Commission, Three Lafayette Centre, 1155 21st Street NW, Washington, DC 20581. See 17 CFR 146.3 for full details on what to include in a Privacy Act notification request.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

Under 5 U.S.C. 552a(j)(2), this system of records is exempted from 5 U.S.C. 552a except subsections (b); (c)(1), and (2); (e)(4)(A) through (F); (e)(6), (7), (9), (10), and (11); and (i) to the extent the system of records pertains to the enforcement of criminal laws; and under 5 U.S.C. 552a(k)(2) is exempted from 5 U.S.C. 552a(c)(3); (d); (e)(1); (e)(4)(G), (H), and (I); and (f) to the extent the system of records consists of investigatory material compiled for law enforcement purposes, other than material within the scope of the exemption at 5 U.S.C. 552a(j)(2); provided, however, that if any individual is denied any right, privilege, or benefit that he would otherwise be

entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence. Moreover, these exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2) or (k)(2). Where compliance would not appear to interfere with or adversely affect the law enforcement process, and/or where it may be appropriate to permit individuals to contest the accuracy of the information collected, e.g., public source materials, the applicable exemption may be waived, either partially or totally, by the Office of the Inspector General (OIG). These exemptions are contained at 17 CFR 146.13.

HISTORY:

76 FR 5973.

Issued in Washington, DC, on March 30, 2023, by the Commission.

Christopher Kirkpatrick,
Secretary of the Commission.

[FR Doc. 2023-07028 Filed 4-4-23; 8:45 am]

BILLING CODE 6351-01-P

COMMODITY FUTURES TRADING COMMISSION

Privacy Act of 1974; System of Records

AGENCY: Commodity Futures Trading Commission.

ACTION: Notice of a new system of records.

SUMMARY: The Commodity Futures Trading Commission (CFTC or Commission) is establishing a new system of records, CFTC-56, Office of the Inspector General Audit Files, to account for information maintained about individuals that is included in Office of the Inspector General (OIG) audit files.

DATES: Comments must be received on or before May 5, 2023. Routine uses will go into effect on May 5, 2023.

ADDRESSES: You may submit comments by any of the following methods:

- *CFTC Comments Portal:* <https://comments.cftc.gov>. Select the "Submit Comments" link for this notice and

follow the instructions on the Public Comment Form.

- *Mail:* Send to Christopher Kirkpatrick, Secretary of the Commission, Commodity Futures Trading Commission, Three Lafayette Centre, 1155 21st Street NW, Washington, DC 20581.

- *Hand Delivery/Courier:* Follow the same instructions as for Mail, above. Please submit your comments using only one of these methods. Submissions through the CFTC Comments Portal are encouraged.

All comments must be submitted in English, or if not, be accompanied by an English translation. Comments will be posted as received to comments.cftc.gov. You should submit only information that you wish to make available publicly.

The Commission reserves the right, but shall have no obligation, to review, pre-screen, filter, redact, refuse, or remove any or all of a submission from comments.cftc.gov that it may deem to be inappropriate for publication, such as obscene language. All submissions that have been redacted or removed that contain comments on the merits of this notice will be retained in the comment file and will be considered as required under all applicable laws, and may be accessible under the Freedom of Information Act.

FOR FURTHER INFORMATION CONTACT:

Marcela Souaya, (202) 418-5137, privacy@cftc.gov, Office of the General Counsel, Commodity Futures Trading Commission, Three Lafayette Centre, 1155 21st Street NW, Washington, DC 20581.

SUPPLEMENTARY INFORMATION:

Background information is not applicable since this is a new SORN.

SYSTEM NAME AND NUMBER:

Office of the Inspector General Audit Files; CFTC-56.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Office of the Inspector General, Commodity Futures Trading Commission, Three Lafayette Centre, 1155 21st Street, NW, Washington, DC 20581. The system will be hosted on a cloud and data center computing infrastructure. Duplicate versions of some or all system information may be at satellite locations where the CFTC has granted direct access to support CFTC operations, system backup, emergency preparedness, and/or continuity of operations.

SYSTEM MANAGER(S):

Inspector General, Office of the Inspector General, Commodity Futures Trading Commission, Three Lafayette Centre, 1155 21st Street NW, Washington, DC 20581. Email is *oig@cftc.gov*.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Commodity Exchange Act, 7 U.S.C. 1 *et seq.*, and regulations, rules or orders issued thereunder; Inspector General Act of 1978, as amended, Public Law 95-452, 5 U.S.C. Appx. 3.

PURPOSE(S) OF THE SYSTEM:

The purpose of this system is to maintain a management information system for CFTC OIG audit projects (such as financial statement audits, performance audits, and other audit projects relating to the programs and operations of the CFTC); and OIG personnel (such as staff training records and conflict of interest certifications necessary for peer review purposes); and to assist in the accurate and timely conduct of audits and audit projects.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals covered consist of: (1) CFTC program participants and CFTC employees and contractors who are associated with an activity that is performed by the CFTC OIG Office of Audit as an audit or audit product included under Generally Accepted Government Auditing Standards (such as a financial audit, an attestation engagement, a review engagement, an agreed-upon procedures engagement, or a review of financial statements); (2) requesters of an OIG audit or other activity (such as a member of Congress, Congressional staff, or a CFTC Chairperson or Commissioner); and (3) persons and entities performing some other role of significance to the OIG Office of Audit efforts (such as potential witnesses, or persons who represent legal entities that are connected to an OIG audit or other activity). The system also tracks information pertaining to OIG staff handling the audit or other activity, and may contain names of relevant staff in other agencies or private sector entities.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records consist of materials compiled and/or generated in connection with audits and other activities performed by OIG staff. These materials include work papers and information regarding the planning, conduct, and resolution of audits and reviews of CFTC programs and participants in those programs, internal legal assistance requests,

information requests, responses to such requests, and reports of findings. The information consists of audit work papers and reports.

RECORD SOURCE CATEGORIES:

Information in the system is obtained from the CFTC, other federal agencies and entities, the Government Accountability Office, contractors, program participants including individuals and business entities, subject individuals, complainants, witnesses, other nongovernmental sources and open source intelligence, including web-based communities, user-generated content, social-networking sites, wikis, blogs and news sources maintained on the Surface, Deep, and Dark web. The Surface Web is what users access in their regular day-to-day activity. It is available to the general public using standard search engines and can be accessed using standard web browsers that do not require any special configuration. The Deep Web is the portion of the web that is not indexed or searchable by ordinary search engines. The Dark Web is a less accessible subset of the Deep Web that relies on connections made between trusted peers and requires specialized software, tools, or equipment to access.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

Routine uses for the Office of the Inspector General Audit Files record systems are set forth below:

1. The information may be given or shown to any person or entity during the course of an Office of the Inspector General (OIG) audit or audit activity (audit) if there is reason to believe that disclosure to the person or entity will further the audit.
2. Information may be disclosed to the Department of Justice or other federal entity, the Merit Systems Protection Board, the Office of Special Counsel, or in a proceeding before a court, adjudicative body, or other administrative body before which the agency is authorized to appear, or in the course of civil discovery, litigation, or settlement negotiations, in actions authorized under the Commodity Exchange Act and otherwise authorized, when:
 - a. The agency, or any component thereof; or
 - b. Any employee of the agency in their official capacity; or
 - c. Any employee of the agency in their personal capacity where the Department of Justice or the agency has agreed to represent the employee; or
 - d. The United States, when the litigation is likely to affect the CFTC or

any of its components; is a party to litigation or has an interest in such litigation, and the use of such records by the Department of Justice or the agency is deemed to be relevant and necessary to the litigation.

3. In any case in which records in the system, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, whether arising by general statute or particular program statute, or by regulation, rule or order issued pursuant thereto, the relevant records may be referred to the appropriate agency, whether Federal, foreign, State or local, charged with enforcing or implementing the statute, regulation, rule or order. This includes a state or federal bar association, state accountability board, or other federal, state, local, or foreign licensing or oversight authority; or professional association or self-regulatory authority to the extent that it performs similar functions (including the Public Company Accounting Oversight Board) for investigations or possible disciplinary action, including suspension and debarment.

4. Information may be disclosed to the National Archives and Records Administration to the extent necessary to fulfill its responsibilities under the law relating to these records.

5. Information may be disclosed to private and public entities, contractors, grantees, volunteers, experts, students, and others performing or working on a contract, service, grant, cooperative agreement, or job that facilitate or are necessary to accomplish an OIG audit, or to collate, aggregate or otherwise refine or dispose of data collected in the system of records. Each private or public entity, contractor, grantee, volunteer, expert, student, or other shall be required to maintain Privacy Act safeguards with respect to such information.

6. To appropriate agencies, entities, and persons when (1) CFTC's OIG suspects or has confirmed that there has been a breach of the system of records, (2) CFTC's OIG has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, CFTC's OIG (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with CFTC's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

7. To another Federal agency or Federal entity, when CFTC's OIG determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

8. A record from the system of records may be disclosed to a grand jury agent pursuant either to a Federal or State grand jury subpoena, or to a prosecution request that such record be released for the purpose of its introduction to a grand jury, provided that the grand jury channels its request through the cognizant U.S. Attorney, that the U.S. Attorney has been delegated the authority to make such requests by the Attorney General, and that the U.S. Attorney actually signs the letter specifying both the information sought and the law enforcement purpose served. In the case of a State grand jury subpoena, the State equivalent of the U.S. Attorney and Attorney General shall be substituted.

9. A record from the system of records may be disclosed in response to a subpoena issued by a Federal agency having the power to subpoena records of other Federal agencies, provided the subpoena is channeled through the head of the issuing agency, if the OIG determines that: (a) The head of the issuing agency signed the subpoena; (b) the subpoena specifies the information sought and the law enforcement purpose served; (c) the records are both relevant and necessary to the proceeding; and (d) such release is compatible with the purpose for which the records were collected.

10. A record from the system of records may be disclosed to the Department of Justice for the purpose of obtaining its advice on an OIG audit, or other related inquiry, including Freedom of Information or Privacy Act matters relating to information in this record system.

11. A record may be disclosed to any official charged with the responsibility to conduct investigations, qualitative assessment reviews, or peer reviews of audit operations within the Office of the Inspector General. This disclosure category includes members of the Council of the Inspectors General on Integrity and Efficiency or any successor entity and officials, designees, and administrative staff within their chain of command, as well as authorized

officials of the Department of Justice and the Federal Bureau of Investigation.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records are stored electronically or on paper in secure facilities.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Information in the system generally can be retrieved by OIG personnel in headquarters and working remotely. Information is generally retrieved by audit assignment number and can be retrieved by using alphanumeric queries and personal identifiers.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

The records are retained and disposed of in compliance with CFTC record disposition authorities, approved by the National Archives and Records Administration. The OIG Audit Files are destroyed 10 years after the audit is completed, unless the audit is deemed of significance sufficient to justify permanent retention. The OIG staff training and related records are destroyed six years after cut off.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Administrative safeguards include restricting access to the OIG work area, and restricting relevant audit tasks to only those competent or qualified to perform the work. Technical security measures within CFTC include restrictions on computer access to authorized individuals who have a legitimate need to know the information; use of encryption for certain data types and transfers; firewalls and intrusion detection applications (set and maintained by the CFTC); and regular review of security procedures and best practices to enhance security (performed by the CFTC). Physical safeguards include restrictions on building access to authorized individuals, 24-hour security guard service, and maintenance of records in lockable offices, desks, and filing cabinets.

RECORD ACCESS PROCEDURES:

Individuals seeking to determine whether this system of records contains information about themselves or seeking access to records about themselves in this system of records should address written inquiries to the Office of the General Counsel, Commodity Futures Trading Commission, Three Lafayette Centre, 1155 21st Street NW, Washington, DC 20581. See 17 CFR 146.3 for full details on what to include in a Privacy Act access request.

CONTESTING RECORD PROCEDURES:

Individuals contesting the content of records about themselves contained in this system of records should address written inquiries to the Office of the General Counsel, Commodity Futures Trading Commission, Three Lafayette Centre, 1155 21st Street NW, Washington, DC 20581. See 17 CFR 146.8 for full details on what to include in a Privacy Act amendment request.

NOTIFICATION PROCEDURES:

Individuals seeking notification of any records about themselves contained in this system of records should address written inquiries to the Office of the General Counsel, Commodity Futures Trading Commission, Three Lafayette Centre, 1155 21st Street NW, Washington, DC 20581. See 17 CFR 146.3 for full details on what to include in a Privacy Act notification request.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

None.

Issued in Washington, DC, on March 30, 2023, by the Commission.

Christopher Kirkpatrick,
Secretary of the Commission.

[FR Doc. 2023-07029 Filed 4-4-23; 8:45 am]

BILLING CODE 6351-01-P

COMMODITY FUTURES TRADING COMMISSION

Privacy Act of 1974; System of Records

AGENCY: Commodity Futures Trading Commission.

ACTION: Notice of a new system of records.

SUMMARY: The Commodity Futures Trading Commission (CFTC or Commission) is establishing a new system of records to cover the collection and maintenance of records pertaining to the administration of the CFTC's advisory committees and subcommittees.

DATES: In accordance with 5 U.S.C. 552a(e)(4) and (11), this notice will go into effect without further notice on April 5, 2023 unless otherwise revised pursuant to comments received. All routine uses will go into effect on May 5, 2023. Comments must be received on or before May 5, 2023.

ADDRESSES: You may submit comments, identified as pertaining to "CFTC-58 Advisory Committees," by any of the following methods:

- **CFTC Comments Portal:** <https://comments.cftc.gov>. Select the "Submit Comments" link for this notice and follow the instructions on the Public Comment Form.

- **Mail:** Send to Christopher Kirkpatrick, Secretary of the Commission, Commodity Futures Trading Commission, Three Lafayette Centre, 1155 21st Street NW, Washington, DC 20581.

- **Hand Delivery/Courier:** Follow the same instructions as for Mail, above. Please submit your comments using only one of these methods. Submissions through the CFTC Comments Portal are encouraged.

All comments must be submitted in English, or if not, be accompanied by an English translation. Comments will be posted as received to comments.cftc.gov. You should submit only information that you wish to make available publicly.

The Commission reserves the right, but shall have no obligation, to review, pre-screen, filter, redact, refuse, or remove any or all of a submission from comments.cftc.gov that it may deem to be inappropriate for publication, such as obscene language. All submissions that have been redacted or removed that contain comments on the merits of this notice will be retained in the comment file and will be considered as required under all applicable laws, and may be accessible under the Freedom of Information Act.

FOR FURTHER INFORMATION CONTACT: Marcela Souaya, (202) 418-5137, privacy@cftc.gov, Office of the General Counsel, Commodity Futures Trading Commission, Three Lafayette Centre, 1155 21st Street NW, Washington, DC 20581.

SUPPLEMENTARY INFORMATION: The CFTC's advisory committees were created to provide input and make recommendations to the Commission on a variety of regulatory and market issues that affect the integrity and competitiveness of the United States (U.S.) derivatives markets. The committees facilitate communication between the Commission and U.S. derivatives markets, trading firms, market participants, and end users. The CFTC currently has five advisory committees. The Agricultural Advisory Committee, Global Markets Advisory Committee, Market Risk Advisory Committee, and the Technology Advisory Committee are discretionary committees under the Federal Advisory Committee Act (FACA), 5 U.S.C. 1001 *et seq.* The Energy and Environmental Markets Advisory Committee was established by the Dodd-Frank Wall

Street Reform and Consumer Protection Act, Public Law 111-203, and subsequently codified in the Commodity Exchange Act, 7 U.S.C. 1 *et seq.*, at 7 U.S.C. 2(a)(15), and is not subject to the FACA. The Commission also establishes and maintains subcommittees that report to advisory committees as needed. Advisory committee and subcommittee members are generally representatives, but depending on the issues to be addressed, the Commission will appoint special government employees (SGEs) and officials from other Federal agencies from time to time. The CFTC identifies candidates for advisory committee and subcommittee membership through a variety of methods, including public requests for nominations; recommendations from existing advisory committee members; consultations with knowledgeable persons outside the CFTC (industry, consumer groups, other state or Federal government agencies, academia, etc.); requests to be represented received from individuals and organizations; and Commissioners' and CFTC staff's professional knowledge of those experienced in the derivatives and other underlying commodities markets. The CFTC collects and maintains information on CFTC advisory committee and subcommittee applicants and members, and those who make recommendations for committee or subcommittee memberships, or otherwise interact with the CFTC regarding its advisory committees and subcommittees. The records are used for the administration of the CFTC's advisory committees and subcommittees.

SYSTEM NAME AND NUMBER:

Advisory Committees CFTC 58.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

This system is located at the Commodity Futures Trading Commission, Three Lafayette Centre, 1155 21st Street NW, Washington, DC 20581. Records may also be located at the regional offices in Chicago, Illinois; Kansas City, Missouri; and New York, New York. The system will be hosted on the CFTC's cloud and data center computing infrastructure. Duplicate versions of some or all system information may be at satellite locations where the CFTC has granted direct access to support CFTC operations, system backup, emergency preparedness, and/or continuity of operations.

SYSTEM MANAGER(S):

Committee Management Officer and Deputy General Counsel for General Law, faca@cftc.gov, Office of the General Counsel, Commodity Futures Trading Commission, Three Lafayette Centre, 1155 21st Street NW, Washington, DC 20581.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

The collection of records is authorized by the Federal Advisory Committee Act, 5 U.S.C. 1001 *et seq.*, and 7 U.S.C. 2(a)(15).

PURPOSE(S) OF THE SYSTEM:

The system collects and maintains information on CFTC advisory committee and subcommittee applicants and members, and those who make recommendations for committee or subcommittee memberships, or otherwise interact with the CFTC regarding its advisory committees and subcommittees. The records are used for the administration of the CFTC's advisory committees and subcommittees. For example, as part of the member evaluation and selection process, the CFTC collects and maintains information to determine the experience and expertise of potential advisory committee and subcommittee members, ensure that the membership on a committee or subcommittee is balanced, and ensure that committee and subcommittee members are properly designated as representatives or SGEs. The records are also used to document and manage committee and subcommittee memberships, to receive public input regarding the work of the advisory committees and subcommittees, and to complete the annual mandatory FACA report to the General Services Administration (GSA).

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The categories of individuals in this system include, but are not limited to:

1. Advisory committee and subcommittee applicants;
2. Current and past advisory committee and subcommittee members;
3. Advisory committee and subcommittee experts and consultants;
4. Administrative assistants to the above-listed categories of individuals;
5. Advisory committee and subcommittee member organization point persons, designated representative members, and designated alternate representative members;
6. Advisory committee meeting panelists;
7. Individuals who make advisory committee or subcommittee member recommendations or serve as references; and,

8. Individuals who attend advisory committee or subcommittee meetings or provide public comments in conjunction with advisory committee meetings.

CATEGORIES OF RECORDS IN THE SYSTEM:

The categories of records in this system include, but are not limited to:

1. Contact information (*e.g.*, name, title, home or work address, personal or work email address, personal or work number, employer, and/or organizational affiliation) for advisory committee and subcommittee applicants and current and past members (including organizational point persons, designated representative members, and designated representative alternate members), and administrative assistants to these individuals; advisory committee and subcommittee experts and consultants; advisory committee meeting panelists; individuals who make advisory committee or subcommittee member recommendations or serve as references; and, individuals who attend advisory committee or subcommittee meetings or provide public comments in conjunction with advisory committee meetings;

2. Information that supports an applicant's experience and expertise to serve or a member's experience and expertise to continue to serve on an advisory committee or subcommittee, including letters of interest, recommendation letters, nomination letters (including self-nominations), and biographical information (*e.g.*, education, work experience, areas of expertise, professional societies, board and other committee memberships, authored publications, professional awards, etc.);

3. Information that ensures appropriate designation of an applicant or member as either a representative or SGE, membership balance (*i.e.*, represented organization and viewpoint category), or to the extent possible, helps the agency select members representing a wide ethnic, racial, gender, and age representation;

4. Federal lobbyist status and other vetting documentation; and,

5. Miscellaneous correspondence relating to the above.

RECORD SOURCE CATEGORIES:

The sources for the records maintained in this system include, but are not limited to:

1. Advisory committee and subcommittee applicants;

2. Current and past advisory committee and subcommittee members;

3. Advisory committee and subcommittee experts and consultants;

4. Administrative assistants to the above-listed categories of individuals;

5. Advisory committee and subcommittee member organization point persons, designated representative members, and designated alternate representative members;

6. Advisory committee meeting panelists;

7. Individuals who make advisory committee or subcommittee member recommendations or serve as references; and

8. Individuals who attend advisory committee or subcommittee meetings or provide public comments in conjunction with advisory committee meetings.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

These records and information in these records may be disclosed:

1. To the Chair or co-Chair of an advisory committee or subcommittee and other committee or subcommittee members to assign tasks to achieve a committee's or subcommittee's goals; to distribute information to committee or subcommittee members, their assistants, and other meeting participants for the purposes of conducting meetings and general committee or subcommittee business; and/or to prepare and review committee and subcommittee reports and/or recommendations.

2. To the public to access information about the CFTC's advisory committees and subcommittees, including its members and activities on the CFTC website (<https://www.cftc.gov>).

3. To the GSA or the Library of Congress when necessary in the administration of the CFTC's FACA committees and subcommittees, including complying with reporting obligations.

4. To the appropriate agencies, entities, and persons to the extent necessary to obtain information relevant to a determination of whether an individual is eligible to serve on a CFTC advisory committee or subcommittee, and whether the individual would serve in a representative or SGE capacity.

5. To contractors performing or working on a contract for the Federal government when necessary to accomplish an agency function.

6. To the Government Accountability Office (GAO) and other appropriate Federal legislative oversight authorities with the responsibility for reviewing agency advisory committees.

7. To the Department of Justice (DOJ) or in a proceeding before a court, adjudicative body, or other administrative body before which the agency is authorized to appear, when:

a. The Commission, or any division or office thereof;

b. Any employee of the Commission in their official capacity;

c. Any employee of the Commission in their personal capacity where the DOJ or the agency has agreed to represent the employee; or

d. The United States, when the Commission determines that litigation is likely to affect the agency or any of its divisions or offices; is a party to litigation or has an interest in such litigation, and the use of such records by the DOJ or the Commission is deemed by the agency to be relevant and necessary to the litigation provided, however, that in each case it has been determined that the disclosure is compatible with the purpose for which the records were collected.

8. To the National Archives and Records Administration pursuant to its records management and inspection authorities under 44 U.S.C. 2904 and 2906.

9. To appropriate agencies, entities, and persons when (1) the Commission suspects or has confirmed that there has been a breach of the system of records; (2) the Commission has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the Commission (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Commission's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

10. To another Federal agency or Federal entity, when the Commission determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records maintained in this system of records are stored electronically or on paper in secure facilities.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

The records are retrieved by an individual's or committee's name.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

The records maintained in this system are retained and disposed of in accordance with the National Archives and Records Administration (NARA) General Records Schedule DAA-GRS-2015-0001 (GRS 6.2) Federal Advisory Committee Records. The CFTC disposes of the paper documents by shredding. All electronic records, files, and data are destroyed either by physical destruction of the electronic storage media or by erasure of the data.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Records are protected from unauthorized access and improper use through administrative, technical, and physical security measures employed by the CFTC. Administrative safeguards include maintenance of written policies, standards, and procedures reinforced by training and periodic auditing. Technical security safeguards include restrictions on computer access to authorized individuals who have a legitimate need to know the information; required use of strong passwords that are frequently changed; multi-factor authentication for remote access and access to many network components; use of encryption for certain data types and transfers; and firewalls and intrusion detection applications. Physical safeguards include restrictions on building access to authorized individuals, use of security guard services, and video surveillance.

RECORD ACCESS PROCEDURES:

Individuals seeking to determine whether this system of records contains information about themselves or seeking access to records about themselves in this system of records should address written inquiries to the Office of the General Counsel, Commodity Futures Trading Commission, Three Lafayette Centre, 1155 21st Street NW, Washington, DC 20581. See 17 CFR 146.3 for full details on what to include in a Privacy Act access request.

CONTESTING RECORD PROCEDURES:

Individuals contesting the content of records about themselves contained in this system of records should address written inquiries to the Office of the General Counsel, Commodity Futures Trading Commission, Three Lafayette Centre, 1155 21st Street NW, Washington, DC 20581. See 17 CFR 146.8 for full details on what to include in a Privacy Act amendment request.

NOTIFICATION PROCEDURES:

Individuals seeking notification of any records about themselves contained in this system of records should address written inquiries to the Office of the General Counsel, Commodity Futures Trading Commission, Three Lafayette Centre, 1155 21st Street NW, Washington, DC 20581. See 17 CFR 146.3 for full details on what to include in a Privacy Act notification request.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

None.

Issued in Washington, DC, on March 30, 2023, by the Commission.

Christopher Kirkpatrick,
Secretary of the Commission.

[FR Doc. 2023-07030 Filed 4-4-23; 8:45 am]

BILLING CODE 6351-01-P

DEPARTMENT OF EDUCATION

[Docket No. ED-2023-SCC-0059]

Agency Information Collection Activities; Comment Request; Request for Title IV Reimbursement or Heightened Cash Monitoring 2

AGENCY: Federal Student Aid (FSA), Department of Education (ED).

ACTION: Notice.

SUMMARY: In accordance with the Paperwork Reduction Act (PRA) of 1995, the Department is proposing an extension without change of a currently approved information collection request (ICR).

DATES: Interested persons are invited to submit comments on or before June 5, 2023.

ADDRESSES: To access and review all the documents related to the information collection listed in this notice, please use <http://www.regulations.gov> by searching the Docket ID number ED-2023-SCC-0059. Comments submitted in response to this notice should be submitted electronically through the Federal eRulemaking Portal at <http://www.regulations.gov> by selecting the Docket ID number or via postal mail, commercial delivery, or hand delivery. If the www.regulations.gov site is not available to the public for any reason, the Department will temporarily accept comments at ICDocketMgr@ed.gov. Please include the docket ID number and the title of the information collection request when requesting documents or submitting comments. Please note that comments submitted after the comment period will not be

accepted. Written requests for information or comments submitted by postal mail or delivery should be addressed to the Manager of the Strategic Collections and Clearance Governance and Strategy Division, U.S. Department of Education, 400 Maryland Ave. SW, LBJ, Room 6W203, Washington, DC 20202-8240.

FOR FURTHER INFORMATION CONTACT: For specific questions related to collection activities, please contact Beth Grebeldinger, (202) 377-4018.

SUPPLEMENTARY INFORMATION: The Department, in accordance with the Paperwork Reduction Act of 1995 (PRA) (44 U.S.C. 3506(c)(2)(A)), provides the general public and Federal agencies with an opportunity to comment on proposed, revised, and continuing collections of information. This helps the Department assess the impact of its information collection requirements and minimize the public's reporting burden. It also helps the public understand the Department's information collection requirements and provide the requested data in the desired format. The Department is soliciting comments on the proposed information collection request (ICR) that is described below. The Department is especially interested in public comment addressing the following issues: (1) is this collection necessary to the proper functions of the Department; (2) will this information be processed and used in a timely manner; (3) is the estimate of burden accurate; (4) how might the Department enhance the quality, utility, and clarity of the information to be collected; and (5) how might the Department minimize the burden of this collection on the respondents, including through the use of information technology. Please note that written comments received in response to this notice will be considered public records.

Title of Collection: Request for Title IV Reimbursement or Heightened Cash Monitoring 2 (HCM2).

OMB Control Number: 1845-0089.

Type of Review: Extension without change of a currently approved ICR.

Respondents/Affected Public: Private Sector; State, Local, and Tribal Governments.

Total Estimated Number of Annual Responses: 564.

Total Estimated Number of Annual Burden Hours: 564.

Abstract: 34 CFR part 668—Student Assistance General Provisions, Subpart K—Cash Management (§ 668.162) establishes the rules and procedures for a participating institution to request, maintain, disburse, and manage the Title IV (TIV) program funds.

Institutions must complete and submit a Form 270 to request TIV program funds while participating under the Reimbursement and Heightened Cash Monitoring payment methods as explained in § 668.162(c) and (d). We are requesting an extension of the currently approved information collection. There have been no changes to the information requested or the form since its prior approval in September 2020.

Dated: March 30, 2023.

Kun Mullan,

PRA Coordinator, Strategic Collections and Clearance, Governance and Strategy Division, Office of Chief Data Officer, Office of Planning, Evaluation and Policy Development.

[FR Doc. 2023-07024 Filed 4-4-23; 8:45 am]

BILLING CODE 4000-01-P

DEPARTMENT OF EDUCATION

Applications for New Awards; Disability Innovation Fund, Pathways to Partnerships Innovative Model Demonstration Project

AGENCY: Office of Special Education and Rehabilitative Services, Department of Education.

ACTION: Notice.

SUMMARY: The U.S. Department of Education (Department) is issuing a notice inviting applications for Federal fiscal year (FFY) 2023 for the Disability Innovation Fund (DIF), Pathways to Partnerships Innovative Model Demonstration Project, Assistance Listing Number 84.421E. This notice relates to the approved information collection under OMB control number 1894-0006, Applications for New Grants under the Rehabilitation Services Administration (RSA).

DATES:

Applications Available: April 5, 2023.

Deadline for Notice of Intent to Apply: April 19, 2023.

Deadline for Transmittal of

Applications: June 5, 2023.

Date of Pre-Application Meeting: The Office of Special Education and Rehabilitative Services (OSERS) will post a PowerPoint presentation that provides general information about the Rehabilitation Services Administration's discretionary grants and a PowerPoint presentation specifically about the Disability Innovation Fund, Pathways to Partnerships Innovative Model Demonstration Project (84.421E) at <https://ncrtm.ed.gov/grant-info>. In addition to posting the PowerPoint, OSERS will conduct a pre-application meeting specific to this competition via

conference call to respond to questions. Information about the pre-application meeting will be available at <https://ncrtm.ed.gov/grant-info> prior to the date of the call. OSERS invites interested applicants to send questions to 84.421E@ed.gov in advance of the pre-application meeting. The teleconference information, including a summary of the 84.421E pre-application meeting questions and answers, will be available at <https://ncrtm.ed.gov/grant-info> within 10 business days after the pre-application meeting.

Deadline for Intergovernmental Review: August 3, 2023.

ADDRESSES: For the addresses for obtaining and submitting an application, please refer to our Common Instructions for Applicants to Department of Education Discretionary Grant Programs, published in the **Federal Register** on December 7, 2022 (87 FR 75045) and available at <https://www.federalregister.gov/documents/2022/12/07/2022-26554/common-instructions-for-applicants-to-department-of-education-discretionary-grant-programs>. Please note that these Common Instructions supersede the version published on December 27, 2021.

FOR FURTHER INFORMATION CONTACT: Cassandra P. Shoffler, U.S. Department of Education, 400 Maryland Avenue SW, Room 5065A, Potomac Center Plaza, Washington, DC 20202-2800. Telephone: (202) 245-7827. Email: 84.421E@ed.gov.

If you are deaf, hard of hearing, or have a speech disability and wish to access telecommunications relay services, please dial 7-1-1.

SUPPLEMENTARY INFORMATION:

Full Text of Announcement

I. Funding Opportunity Description

Purpose of Program: The purpose of the Disability Innovation Fund (DIF) Program, as provided by the Consolidated Appropriations Act, 2022 (Pub. L. 117-103), is to support innovative (as defined in this notice) activities aimed at increasing competitive integrated employment (CIE) as defined in section 7 of the Rehabilitation Act of 1973 (Rehabilitation Act) (29 U.S.C. 705(5)),¹

¹ This regulatory definition further clarifies the statutory definition of CIE found in the Rehabilitation Act. Competitive integrated employment means work that—

(i) Is performed on a full-time or part-time basis (including self-employment) and for which an individual is compensated at a rate that—

(A) Is not less than the higher of the rate specified in section 6(a)(1) of the Fair Labor Standards Act of 1938 (29 U.S.C. 206(a)(1)) or the rate required

for youth and other individuals with disabilities.

For FFY 2023, the Department intends to fund multiple innovative model demonstration projects focused on the creation of systemic approaches to transition services for children and youth with disabilities (as defined in this notice). Ensuring that key agents of change and required partners (as defined in this notice)—State vocational rehabilitation agencies (SVRAs), State educational agencies (SEAs), local educational agencies (LEAs), and federally funded Centers for Independent Living (CILs)—are actively collaborating to support coordinated transition processes is critical to the success of children and youth with disabilities.

Priority: We are establishing this priority for the FFY 2023 grant competition and any subsequent year in which we make awards from the list of unfunded applications from this competition, in accordance with section 437(d)(1) of the General Education Provision Act (GEPA), 20 U.S.C. 1232(d)(1).

Absolute Priority: For FFY 2023 and any subsequent year in which we make awards from the list of unfunded applications from this competition, this is an absolute priority. Under 34 CFR 75.105(c)(3), we consider only applications that meet the absolute priority.

The priority is:

under the applicable State or local minimum wage law for the place of employment;

(B) Is not less than the customary rate paid by the employer for the same or similar work performed by other employees who are not individuals with disabilities and who are similarly situated in similar occupations by the same employer and who have similar training, experience, and skills; and

(C) In the case of an individual who is self-employed, yields an income that is comparable to the income received by other individuals who are not individuals with disabilities and who are self-employed in similar occupations or on similar tasks and who have similar training, experience, and skills; and

(D) Is eligible for the level of benefits provided to other employees; and

(ii) Is at a location—

(A) Typically found in the community; and

(B) Where the employee with a disability interacts for the purpose of performing the duties of the position with other employees within the particular work unit and the entire work site, and, as appropriate to the work performed, other persons (e.g., customers and vendors), who are not individuals with disabilities (not including supervisory personnel or individuals who are providing services to such employee) to the same extent that employees who are not individuals with disabilities and who are in comparable positions interact with these persons; and

(iii) Presents, as appropriate, opportunities for advancement that are similar to those for other employees who are not individuals with disabilities and who have similar positions. (34 CFR 361.5(c)(9))

Pathways to Partnerships Innovative Model Demonstration Project.

Background:

The Americans with Disabilities Act (ADA) and the Rehabilitation Act of 1973, as amended (Rehabilitation Act) both describe the Nation's goals for people with disabilities to include achieving: equality of opportunity, full inclusion and integration in society and employment, independent living, and economic self-sufficiency (42 U.S.C. 12101(a)(7); 29 U.S.C. 701(a)(6)).

Securing an appropriate education, including transition services that lead to CIE, is one critical component that youth and adults with disabilities need to achieve the Nation's goals. As Congress found in the Rehabilitation Act, "there is a substantial need to support such students [with disabilities] as they transition from school to postsecondary life." 29 U.S.C. 701(a)(7).

Over the past several decades, States have implemented numerous federally mandated changes to improve post-school outcomes for youth with disabilities (Gingerich & Crane, 2021). For example, the changes have included greater access to the general education curriculum, which has increased the number of students with disabilities who leave high school with a standard high school diploma, and pre-employment transition services, including transition planning within the individualized education program (IEP) process beginning at age 16 (or age 14 in some States) for students with disabilities under the Individuals with Disabilities Education Act (IDEA).

However, persons with disabilities are less likely to be employed than those without disabilities. According to the U.S. Department of Labor, Office of Disability Employment Policy, in 2022 the unemployment rate for persons with disabilities ages 16–64 was 5.4 percent compared to 3.2 percent for persons without disabilities. Similarly, the unemployment rate for youth with disabilities, ages 16–19, was 19.6 percent compared to 10.4 percent for youth without a disability. An even larger disparity exists for youth with disabilities ages 20–24, with an unemployment rate of 14.5 percent compared to 6.7 percent for youth ages 20–24 without a disability. (United States Department of Labor, n.d.)² The Department intends to begin building the evidence base regarding whether early exposure to employment and career possibilities for children and youth with disabilities will lead to successful secondary or postsecondary

experiences, including employment. There are a significant number of factors contributing to disappointing transition outcomes for students with disabilities, such as limited exposure to career exploration, lack of preparation for postsecondary education, limited employment opportunities (e.g., paid internships, paid apprenticeships), and limited training for youth service professionals (as defined in this notice) (Frazier et al., 2020; Biggs & Carter, 2016; Luft, 2015; Wehman et al., 2015).

As children and youth with disabilities move through the school system, many do not have exposure to self-advocacy training, careers, and independent living opportunities until they transition from high school. It is important to support children and youth with disabilities and their support systems (as defined in this notice) to bridge the gap from school to adult life, independent living, and career. SVRAs, SEAs, LEAs, and CILs offer various transitional supports that could be more effective at achieving the Nation's goals for children and youth with disabilities expressed in the ADA and Rehabilitation Act if leveraged through innovative models. Oertle & Trach (2007) found that collaboration among educational professionals (as defined in this notice), VR professionals, youth service professionals, employers, and parents can improve interagency relationships and lead to successful outcomes for children and youth with disabilities, including increasing postsecondary education completion and securing CIE.

Through this priority, the Department seeks to support projects that foster the establishment of close ties among agencies, transforming collaboration into partnership. Each applicant is required to ensure that project partnerships are comprised of, at a minimum, each of the following entities: SVRAs, SEAs, LEAs, CILs. Each partnership will demonstrate how services might be improved in the field, by developing and piloting a cohesive service delivery model that better manages its unique resources while coordinating efforts to improve outcomes for children and youth with disabilities and their support systems and facilitating successful transitions. In addition to required partners, applicants are strongly encouraged to include additional entities that may benefit the partnership, including State, local or regional employers, chambers of commerce, institutions of higher education and non-profit or private entities that promote improved transition outcomes for children and youth with disabilities.

The required partners support transition services by providing employment services, training, career exploration, and independent living skills to children and youth with disabilities and their support systems. These entities are authorized by different laws that are administered by different Federal agencies, and each entity has an important role in supporting successful secondary or postsecondary experiences for children and youth with disabilities and their support systems.

SVRAs are authorized by the title I of the Rehabilitation Act. SVRAs provide VR services for individuals with disabilities, consistent with their strengths, resources, priorities, concerns, abilities, capabilities, interests, and informed choice, so that they may prepare for and engage in CIE or supported employment and achieve economic self-sufficiency.

The IDEA makes available a free appropriate public education to eligible children and youth with disabilities and ensures that special education and related services are available to those children and youth. SEAs, under 34 CFR 300.149, have responsibility for general supervision of LEAs under IDEA to ensure appropriate monitoring and oversight, technical assistance, and enforcement. LEAs, in turn, are responsible for the general supervision of schools within their jurisdictions. Under IDEA, LEAs must provide transition services to students at age 16 (or age 14 in some States).

Title VII of the Rehabilitation Act of 1973 authorizes the Independent Living Services and CIL programs. Administered by the Administration for Community Living, CILs are required to provide independent living core services (as defined in this notice) to individuals with significant disabilities to maximize the leadership, empowerment, independence, and productivity of individuals with disabilities, and the integration and full inclusion of individuals with disabilities into the mainstream of American society.

It is through partnerships (as defined in this notice) at the State and local levels that a seamless, comprehensive system of programs, projects, and supports can be provided in a manner that raises expectations, improves engagement, and provides empowerment opportunities for children and youth with disabilities and their support systems. Over the past three decades, research on the transition of students with significant disabilities has shown that post-school outcomes of students with disabilities increase when

² See the *Resources* section of this notice for complete citations.

educators, families, students, community members, and organizations work together in transition planning (Newman et al., 2016). These individuals each contribute a unique set of expertise to the collective group that, together, pave a clear and robust path as children and youth with disabilities transition from school to postsecondary endeavors, including CIE.

The research is clear that collaboration from all stakeholders in the transition process improves outcomes, but currently, there is a deficit in policies and practices in place to serve as models (Frazier et al., 2020). The collaboration of all stakeholders will attempt to solve common challenges associated with cross-agency communication, alignment of vision and goals, resource coordination, and trust. Partnerships will reduce organizational silos and create opportunities for a unified vision; common goals; cross-partner education and training; communication; and the identification and utilization of innovative and new approaches to collaboration among partners focused on improving transition for children and youth with disabilities and their support systems.

We encourage applicants to propose innovative models of collaboration and partnerships that coordinate funding from, and provide a seamless system of services by, required partners. Such collaboration and partnerships improve the transition for children and youth with disabilities from the education system to the vocational rehabilitation system with the goal of obtaining CIE. Innovative models have the potential to increase knowledge and access to opportunities and programs for children and youth with disabilities and their support systems, as well as to challenge the field to raise expectations and secure partnerships that result in desired employment, postsecondary education, and economic self-sufficiency outcomes for children and youth with disabilities.

Priority:

A project under this priority must develop an innovative model of collaboration and partnerships, with coordination of funding from, and a seamless system of services provided by, the required partners (SVRAs, SEAs, LEAs, and CILs). A project must include an innovative approach to the provision of seamless transition services focused on career exploration, CIE aspiration, and achievement of CIE for children and youth with disabilities, leveraging the expertise of the required partners to increase the success of the transition process. The project must include an evaluation of the training provided to—

(a) youth service professionals who are implementing the innovative model, including but not limited to service providers, aides, and other professionals who provide, for example, skills training, professional development, and cross-agency training;

(b) children and youth with disabilities (*i.e.*, in soft skills training, career exploration training, and job readiness training); and

(c) support systems of children and youth with disabilities (*i.e.*, in advocacy, financial planning, and transition planning).

The project must promote opportunities for career exposure for youth such as internships and apprenticeships. To promote transparency and provide tools for sharing best practices, the project also must establish a project-specific website geared toward actionable items, such as information for youth service professionals (*i.e.*, program descriptions and information, resources, online training opportunities, etc.) or project participant resources for children and youth with disabilities (*i.e.*, interest inventories, career exploration including virtual employer tours, job duties, educational courses that support specific careers, resources for transitioning from middle to high school or high school to post-secondary education or employment). It would also include resources, as they are being developed, that would allow for the replication of certain aspects of the project throughout the life of the project. The project must develop collaborations into partnerships that leverage resources to implement a cohesive service delivery model that supports successful postsecondary experiences for children and youth with disabilities and their support systems.

Application Requirements:

Under this priority, applicants must meet the following application requirements.

(a) *Proposed project.* Describe, in a narrative section of the application, the proposed project including a description of the defined geographic area or areas to be served by the project; how the proposed project will develop, pilot, refine, and implement, and collect and analyze data for the collaborative model that leverages the expertise of the required partners, children and youth with disabilities and their support systems, policymakers, employers, educational professionals, and youth service professionals; and other agencies and entities to assist with the proposed project. To meet this requirement, in the application, applicants must—

(1) *Develop the proposed project (In Year One).*

(i) Demonstrate that the proposed project incorporates evidence, findings, or accompanying summary reports from experts in the field, where applicable, or an existing program that has been modified to be appropriate for the proposed project;

(ii) Describe how the proposed project will develop a collaborative innovative systemic model, including ongoing professional and leadership development for youth service professionals across agencies, to assist children and youth with disabilities and their support systems;

(iii) Identify stakeholders that have experience serving children and youth with disabilities that are diverse, such as with regard to socioeconomic status, race, ethnicity, culture, language, disability, and gender, and describe how the project will include such stakeholders in project activities;

(iv) Describe how the proposed project will identify, conduct outreach to and serve children and youth with disabilities and their support systems, required partners, policy makers, employers, educational professionals, youth service professionals, and other agencies and entities that are critical to the development and implementation of the proposed project;

(v) Describe how the proposed project will identify, conduct outreach to and serve children and youth with disabilities who have been underserved by SVRAs or SEAs, such as children and youth of color, from low-income families, from rural areas or with significant disabilities.

(vi) Identify and describe the innovative services and supports that are relevant to the proposed project to promote smooth, coordinated transition services resulting in successful CIE outcomes for project participants;

(vii) Describe how the proposed project will develop and pilot (years 1 and 2), and refine and implement (years 2–5), a project website that is a centralized location for maintaining age-appropriate materials for youth participants and resources for youth service professionals to include: project details, project results, and training/resources for project participants that will be incorporated into the required partner websites at the end of the project and that will raise awareness among and facilitate engagement with other interested public entities and the business community;

(viii) Describe how the proposed project will create age-appropriate, in-person and virtual career experiences such as internships and

apprenticeships, which may include standalone models, training modules, and customized modules to meet the unique learning needs of project participants, and which may be incorporated into the proposed project website;

(ix) Describe how the proposed project will develop, refine, and implement a program that trains project participants in economic independence, including financial literacy training (as defined in this notice), and may include a standalone model or modules that may be incorporated into the proposed project website;

(x) Describe how the proposed project's required partners will collaborate on a product for use by personnel supporting the project participants and the project participants themselves, that supports and encourages career exploration and career assessment results and interests;

(xi) Describe how the proposed project will identify, and conduct outreach and information dissemination to, stakeholders, including youth and children with disabilities and their support systems, partners, and project participants;

(xii) Describe the proposed project plan to conduct local resource mapping (as defined in this notice); and

(xiii) Describe how the proposed project will identify and develop mechanisms to collect data from partners, improve data sharing among partners and stakeholders, and maintain outcome data;

(2) *Pilot the proposed project (No later than Quarter 1 of Year Two)*. Describe how the proposed project will pilot the proposed project no later than the first quarter of the second year of the proposed project period (October 1, 2024—December 30, 2024), including what services will be offered; the expected number of children and youth with disabilities served; the expected number of trainings conducted with youth service professionals, children and youth with disabilities, support systems, and other key partners and stakeholders (*i.e.*, Workforce Boards, Businesses); and data collected and evaluated during the pilot phase; and

(3) *Refine and implement the proposed project (Year Two to Five)*.

(i) Describe how the proposed project will assess the results of the pilot, including through data collection and evaluation, to determine whether components of the pilot produced the expected results as planned or will need to be altered prior to the implementation of the proposed project;

(ii) Describe how the proposed project will include a process of continuous

assessment and improvement to ensure that the proposed project activities are reviewed against the proposed project goals and objectives and are refined throughout the project period; and

(iii) Describe the plan to refine the proposed project through a process for securing feedback, through various methods (*e.g.*, in-person, phone, virtual) from project participants, partners, and stakeholders, to ensure continuous improvement and refinement of the proposed project throughout the project period; and

(4) *Collect and analyze project data (Year One to Five)*.

(i) Describe how the full implementation of the proposed project will include finalization of baseline data (first quarter of year 1); including collecting the following data elements in each year of the grant and setting appropriate targets:

(A) The number of children with disabilities who are contacted about the proposed project.

(B) The number of youth with disabilities who are contacted about the proposed project.

(C) The number of children with disabilities who are enrolled in the proposed project.

(D) The number of youth with disabilities who are enrolled in the proposed project.

(E) The number of youth with disabilities who secure competitive integrated employment.

(F) The number of youth enrolled in post-secondary education.

(G) The number of youth service professionals, broken down by program/agency (*i.e.*, SVRAs, SEAs, LEAs, CILs, and other entities) who participate in professional development training (*i.e.*, cross training) to support the development of the proposed project, increasing successful pathways to partnerships;

(ii) Describe how the assessment of baseline data will be conducted prior to the start of the proposed pilot project activities (year 1); and

(iii) Describe how data collection and assessment of feedback on the proposed project and its impact on project participants, including strengths and challenges, will be collected and analyzed during the proposed project pilot (years 1–2) and refinement (years 2–5).

(b) *Memorandum of understanding (MOU)*

(1) Submit with the application letters of intent from an authorized representative to sign a formal MOU from all required partners, identifying the general responsibilities of each partner in the proposed project.

(2) Provide an assurance in the application that if the applicant receives an award, it will, within 180 days of award date, submit to the Department a formal signed MOU between the applicant and all required partners. The MOU must include, for each required partner, a scope of work describing the portions of the application that the partner will implement. These scopes of work must contain detailed work plans and budgets that are consistent with the application, and must include—

(i) The applicant's and each partner's specific goals, activities, timelines, budgets, key personnel, and annual performance targets;

(ii) Description of a process for decision-making;

(iii) Description of a process for amending the MOU;

(iv) Identification of the fiscal agent; and

(v) Description of how the applicant and partners will communicate and exchange information.

(vi) Describe how the proposed project will establish an advisory work group or steering committee that meets at least quarterly, and includes but is not limited to, key project personnel (as defined in this notice) from the partners, with at least 10 percent of the committee members or workgroup to include children and youth with disabilities and their support systems. The advisory work group or steering committee will provide input on the development, implementation, and operationalization of partner activities that contribute to the success of project participants (as defined in this notice);

(c) *Logic model*

(1) Provide a logic model (as defined in this notice) that communicates how the proposed project will achieve its intended outcomes that depicts, at a minimum, the goals, activities, outputs, and intended outcomes of the proposed project.

(2) Demonstrate how the proposed project components (as defined in this notice) are intended to affect the proposed project outcomes. Applicants must specifically note the proposed project activities that are supported by evidence that demonstrates a rationale and are depicted in the logic model.

Note: The following website provides more information on logic models: "Logic models: A tool for designing and monitoring program evaluations" https://ies.ed.gov/ncee/edlabs/regions/pacific/pdf/rel_2014007.pdf.

(d) *Proposed project management plan*. In the narrative section of the application under "Quality of the management plan," describe how—

(1) The proposed management plan will ensure that the intended project outcomes will be achieved on time and within budget. To address this requirement, the applicant must include—

(i) Clearly defined responsibilities for key project personnel, including level of effort, consultants, and subcontractors, as applicable;

(ii) Identification of required and additional partners involved in completing the proposed project, including roles;

(iii) Timelines, milestones, and deliverables for accomplishing the project tasks;

(iv) A description of how time commitments of key project personnel and any consultants and subcontractors will be allocated and how these allocations are appropriate and adequate to achieve the intended project outcomes;

(v) The proposed management plan that ensures that the products and services provided are of high quality, relevant, and useful to recipients;

(vi) A description of how the proposed project will include a diversity of perspectives, including those of children and youth with disabilities and their support systems; the required partners; policymakers, employers, educational professionals, and youth service professionals; and other agencies and entities in its development and operation; and

(vii) A detailed description of how activities will continue to be sustained once the grant performance period is over.

(e) *Proposed project evaluation.* In the narrative section of the application under “Quality of the project evaluation,” include an evaluation plan for the proposed project as described in the following paragraphs. The evaluation plan must describe measures of progress in implementation, including the criteria for determining the extent to which the proposed project’s products and services have met the goals for reaching its target population; measures of intended outcomes or results of the proposed project activities to evaluate those activities; and how well the goals or objectives of the proposed project, as described in its logic model, have been met. Grantees must dedicate sufficient funds throughout the project period to cover the costs of developing, refining, and implementing the project evaluation plan, as well as the costs associated with collaborating throughout the period of performance with an independent evaluator

identified by RSA. The evaluation plan and process must—

(1) Identify formative and summative evaluation questions that align to the logic model;

(2) Describe how progress in and fidelity of implementation, as well as project outcomes, will be measured to answer the evaluation questions;

(3) Specify the measures and associated instruments or sources for data appropriate to the evaluation questions. Include information regarding reliability and validity of measures where appropriate;

(4) Describe strategies for analyzing data and how data collected as part of this proposed project will be used to inform and refine the logic model and evaluation plan, including subsequent data collection;

(5) Include a timeline for conducting the evaluation and include staff assignments for completing the plan. The timeline must indicate that data will be available bi-annually, for the annual performance report (October 1–March 31) and end of year performance report (October 1–September 30);

(6) Describe how the proposed project will collect data regarding the project participants, including but not limited to, demographics (e.g., gender, race, ethnic group) and regional information;

(7) Describe how the proposed project will identify and evaluate the innovative strategies that were effective for systemic change in partnerships (e.g., relationship building, resource sharing, funding mechanism for services);

(8) Describe how the proposed project will evaluate the relationship between project participants’ engagement with or use of specific practices and strategies implemented by the proposed project and key outcomes;

(9) Describe how the proposed project will make broadly available the results of any evaluations conducted of funded activities, digitally and free of charge, through formal (e.g., peer reviewed journals) or informal (e.g., newsletters) mechanisms;

(10) Describe how the proposed project will ensure that data from the grantee’s evaluation are made available to an independent evaluator identified by RSA consistent with applicable privacy requirements;

(11) Describe how the proposed project will leverage data collection, analysis, and research methodologies to result in an evaluation that can build evidence at least at the level of promising evidence (as defined in this notice); and

(12) Include an assurance that the project will cooperate on an ongoing

basis with any technical assistance provided by the Department or its contractors and comply with the requirements of any other evaluation of the program conducted by the Department, including the need to share project data.

References

- Biggs, E.E., & Carter, E.W. (2016). Quality of life for transition-age youth with autism or intellectual disability. *Journal of Autism and Developmental Disorders*, 46(1), 190–204. <https://doi.org/10.1007/s10803-015-2563-x>.
- Federal Joint Communication to State and Local Government: Resource Leveraging & Service Coordination to Increase Competitive Integrated Employment for Individuals with Disabilities. (2022, August 3). Retrieved January 26, 2023, from www.dol.gov/sites/dolgov/files/ODEP/pdf/ResourceLeveragingServiceCoordinationToIncreaseCIE8-12-22.pdf.
- Frazier, K.F., Perryman, K., & Kucharczyk, S. (2020). Transition Services: Building Successful Collaborations among School Professionals. *Journal of School-Based Counseling Policy and Evaluation*, 2(2), 131–141. <https://doi.org/10.25774/80b3-kc43>.
- Gingerich, J.A., & Crane, K. (2021). Transition Linkage Tool: A System Approach to Enhance Post-School Employment Outcomes (pp. 1–23). College Park, MD: University of Maryland.
- Luft, P. (2015). Transition services for DHH adolescents and young adults with disabilities: Challenges and theoretical frameworks. *American Annals of the Deaf*, 160(4), 395–414. <https://doi.org/10.1353/aad.2015.0028>.
- Newman, L.A., Madaus, J.W., & Javitz, H.S. (2016). Effect of transition planning on postsecondary support receipt by students with disabilities. *Exceptional Children*, 82(4), 497–514. <https://doi.org/10.1177/0014402915615884>.
- Oertle, K.M., & Trach, J.S. (2007). Interagency collaboration: The importance of rehabilitation professionals’ involvement in transition. *Journal of Rehabilitation*, 73(3).
- Disability employment statistics. United States Department of Labor. (n.d.). Disability employment statistics. Retrieved January 3, 2023, from www.dol.gov/agencies/odep/research-evaluation/statistics.
- Wehman, P., Sima, A., Ketchum, J., West, M., Chan, F., & Luecking, R. (2015). Predictors of successful transition from school to employment for youth with disabilities. *Journal of Occupational Rehabilitation*, 25(2), 323–334. <https://doi.org/10.1007/s10926-014-9541-6>.

Definitions

For the FFY 2023 grant competition and any subsequent year in which we make awards from the list of unfunded applications from this competition, in accordance with section 437(d)(1) of GEPA, we establish definitions of

“children and youth with disabilities,” “educational professional,” “financial literacy training,” “independent living core services,” “innovative,” “key project personnel,” “local resource mapping,” “partnership,” “project participants,” “promising evidence,” “required partners,” “support systems,” and “youth service professionals.” The remaining definitions are from 34 CFR 77.1. The authority for each definition is noted following the text of the definition.

“Children and youth with disabilities” means children (ages 10–13) and youth (ages 14–24) with disabilities who meets the definition of “child with a disability” in 34 CFR 300.8 or a person who (i) has a physical or mental impairment that substantially limits one or more major life activities, (ii) has a record of such an impairment, or (iii) is regarded as having such an impairment. (Section 437(d)(1) of GEPA.)

“Educational professional” means a professional providing educational services either at a school, academy, or other educational facility, or at a private facility or residence, as a teacher, professor, tutor, aide, administrator, or other education professional. (Section 437(d)(1) of GEPA.)

“Financial literacy training” means the education and understanding of knowing how money is made, spent, and saved as well as the skills and ability to use financial resources to make decisions. (Section 437(d)(1) of GEPA.)

“Independent living core services” means (i) information and referral services; (ii) independent living skills training; (iii) peer counseling (including cross-disability peer counseling); (iv) individual and systems advocacy; and (v) services that—(A) facilitate the transition of individuals with significant disabilities from nursing homes and other institutions to home and community-based residences, with the requisite supports and services; (B) provide assistance to individuals with significant disabilities who are at risk of entering institutions so that the individuals may remain in the community; and (C) facilitate the transition of youth who are individuals with significant disabilities, who were eligible for individualized education programs under section 614(d) of the IDEA (20 U.S.C. 1414(d)), and who have completed their secondary education or otherwise left school, to postsecondary life. (Section 437(d)(1) of GEPA.)

“Innovative” means featuring new methods, ideas, or approaches. (Section 437(d)(1) of GEPA.)

“Key project personnel” means, at a minimum, the project director or principal investigator with the grantee responsible for defining and identifying all other key personnel positions in their applications. (Section 437(d)(1) of GEPA.)

“Local resource mapping” means a strategy for identifying and analyzing the programs, people, services, and other resources that currently exist. (Section 437(d)(1) of GEPA.)

“Logic model” (also referred to as a theory of action) means a framework that identifies key proposed project components (as defined in 34 CFR 77.1) of the proposed project (*i.e.*, the active “ingredients” that are hypothesized to be critical to achieving the relevant outcomes (as defined in 34 CFR 77.1)) and describes the theoretical and operational relationships among the key proposed project components and relevant outcomes. (34 CFR 77.1.)

“Partnership” means an entity in which two or more co-owners contribute resources, share in success and loss, and are individually liable for the entity’s actions. (Section 437(d)(1) of GEPA.)

“Project component” means an activity, strategy, intervention, process, product, practice, or policy included in a project. Evidence may pertain to an individual project component or to a combination of project components (*e.g.*, training teachers on instructional practices for English learners and follow-on coaching for these teachers). (34 CFR 77.1.)

“Project participants” means individuals participating in the project, including but not limited to children and youth with disabilities and their support system and youth service professionals. (Section 437(d)(1) of GEPA.)

“Promising evidence” means that there is evidence of the effectiveness of a key project component in improving a relevant outcome, based on a relevant finding that includes at least one statistically significant and positive (*i.e.*, favorable) effect on a relevant outcome. (Section 437(d)(1) of GEPA.)

“Required partners” mean SVRAs, SEAs, LEAs, and CILs. (Section 437(d)(1) of GEPA.)

“Support systems” means a network of people, including family members, guardians, advocates, friends, and peers, who provide an individual with practical or emotional support. (Section 437(d)(1) of GEPA.)

“Youth service professionals” means adults, who have competencies in many fields (youth development, education, workforce development, disability, etc.) and work directly with children and

youth with disabilities, ages 10–24, in order to effectively guide youth in transition and maximize their potential. (Section 437(d)(1) of GEPA.)

Waiver of Proposed Rulemaking: Under the Administrative Procedure Act (5 U.S.C. 553), the Department generally offers interested parties the opportunity to comment on proposed priorities, selection criteria, requirements, and definitions. Section 437(d)(1) of GEPA, however, allows the Secretary to exempt from rulemaking requirements regulations governing the first grant competition under a new or substantially revised program authority. This is the first grant competition for this program under the authority given in the Consolidated Appropriations Act, 2022, and, therefore, qualifies for this exemption. In order to ensure timely grant awards, the Secretary has decided to forego public comment on the priority, requirements, definitions, and selection criteria under section 437(d)(1) of GEPA. The priority, requirements, definitions, and selection criteria will apply to the FFY 2023 grant competition and any subsequent year in which we make awards from the list of unfunded applications for this competition.

Program Authority: Consolidated Appropriations Act, 2022 (Pub. L. 117–103), 136 Stat. 49.

Note: Proposed projects will be awarded and must be operated in a manner consistent with the nondiscrimination requirements contained in Federal civil rights laws.

Applicable Regulations: (a) The Education Department General Administrative Regulations in 34 CFR parts 75, 77, 79, 81, 82, 84, 86, 97, 98, and 99. (b) The Office of Management and Budget Guidelines to Agencies on Governmentwide Debarment and Suspension (Nonprocurement) in 2 CFR part 180, as adopted and amended as regulations of the Department in 2 CFR part 3485. (c) The Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards (Uniform Guidance) in 2 CFR part 200, as adopted and amended as regulations of the Department in 2 CFR part 3474.

II. Award Information

Type of Award: Discretionary grants negotiated as cooperative agreements.

Estimated Available Funds: \$224,023,590.00.

Contingent upon the availability of funds and the quality of applications, we may make additional awards in FY 2024 from the list of unfunded applications from this competition.

Estimated Range of Awards: \$4,000,000–\$10,000,000 (frontloaded for the 60-month project period).

Estimated Average Size: \$7,000,000.

Estimated Number of Awards: 22–32.

Note: The Department is not bound by any estimates in this notice.

Project Period: Up to 60 months.

Note: The Final Performance Report must be completed and submitted by the end of the project period, September 30, 2028. Therefore, the project must complete core project activities to allow sufficient time for the evaluation and final performance report to be completed and submitted by the end of the project period on September 30, 2028.

Note: Applicants under this competition are required to provide detailed budget information for the total grant period, including detailed budget information for each of the five years of the proposed project. Applicants may not set aside more than 5 percent of the total budget to evaluate the overall effectiveness of the proposed project. Applicants are encouraged to consider the impact of implementation of the proposed project when creating a year 1 budget. Applicants are also encouraged to consider the impact of the period of performance end date, September 30, 2028, when creating the year 5 budget.

Note: Grantees are expected to complete at least monthly drawdowns of expenditures.

Note: Subgrantees are expected to report monthly invoices of expenditures to the grantee.

III. Eligibility Information

1. *Eligible Applicants:* SVRAs and SEAs.

2. a. *Cost Sharing or Matching:* This competition does not require cost sharing or matching.

b. *Indirect Cost Rate Information:* This program uses an unrestricted indirect cost rate. For more information regarding indirect costs, or to obtain a negotiated indirect cost rate, please see www2.ed.gov/about/offices/list/ocfo/intro.html.

c. *Administrative Cost Limitation:* This program does not include any program-specific limitation on administrative expenses. All administrative expenses must be reasonable and necessary and conform to the Cost Principles described in 2 CFR part 200 subpart E of the Uniform Guidance.

d. *Administrative Expenses:*

(i) All administrative expenses incurred under the DIF program must be reasonable and necessary for the administration of the DIF program and must conform to the requirements of the

Federal Cost Principles described in 2 CFR 200.403 through 200.405.

(ii) Although, in certain circumstances, proposed project participants served and services provided are the same under both the DIF programs and the SVRA programs, these programs are separate and distinct programs with separate and distinct funding streams and requirements. As such, when allocating administrative costs between the DIF programs and SVRA programs, grantees must allocate the costs in accordance with the requirements of 2 CFR 200.405. This means that both DIF program and SVRA program funds could be used to pay administrative costs associated with staff time providing services; however, with respect to those administrative activities limited to the DIF program, such as submitting progress reports, grantees must use only DIF program funds (or other allowable funds) to pay these costs. This applies to grantees and subgrantees.

(iii) SVRA program funds and non-Federal funds used for match under the VR program can only pay for allowable costs under the VR program, including administrative costs, in accordance with 2 CFR 200.403 through 200.405.

3. *Subgrantees:* Under the Consolidated Appropriations Act, 2022, a grantee under this competition may award subgrants. Under this competition, subgrants may not exceed 75 percent of the funds. Under 34 CFR 75.708(b) and (c), a grantee under this competition may award subgrants—to directly carry out project activities described in its application—to the following types of entities: public and private, nonprofit entities, SVRAs, SEAs, LEAs, and CILs. The grantee may only award subgrants to entities it has identified in an approved application. Subrecipients may not further subgrant funds received under this award.

IV. Application and Submission Information

1. *Application Submission Instructions:* Applicants are required to follow the Common Instructions for Applicants to Department of Education Discretionary Grant Programs, published in the **Federal Register** on December 7, 2022 (87 FR 75045) and available at <https://www.federalregister.gov/documents/2022/12/07/2022-26554/common-instructions-for-applicants-to-department-of-education-discretionary-grant-programs>, which contain requirements and information on how to submit an application. Please note that these Common Instructions supersede

the version published on December 27, 2021.

2. *Submission of Proprietary Information:* Given the types of proposed projects that may be proposed in applications for the DIF, your application may include business information that you consider proprietary. In 34 CFR 5.11 we define “business information” and describe the process we use in determining whether any of that information is proprietary and, thus, protected from disclosure under Exemption 4 of the Freedom of Information Act (5 U.S.C. 552, as amended).

Because we plan to make successful applications available to the public, you may wish to request confidentiality of business information.

Consistent with Executive Order 12600, please designate in your application any information that you believe is exempt from disclosure under Exemption 4. In the appropriate Appendix section of your application, under “Other Attachments Form,” please list the page number or numbers on which we can find this information. For additional information please see 34 CFR 5.11(c).

3. *Intergovernmental Review:* This competition is subject to Executive Order 12372 and the regulations in 34 CFR part 79. Information about Intergovernmental Review of Federal Programs under Executive Order 12372 is in the application package for this competition.

4. *Funding Restrictions:* We reference regulations outlining funding restrictions in the *Applicable Regulations* section of this notice.

5. *Recommended Page Limit:* The application narrative is where you, the applicant, address the selection criteria that reviewers use to evaluate your application. We recommend that you (1) limit the application narrative to no more than 45 pages and (2) use the following standards:

- A “page” is 8.5” x 11”, on one side only, with 1” margins at the top, bottom, and both sides.

- Double space (no more than three lines per vertical inch) all text in the application narrative, including titles, headings, footnotes, quotations, references, and captions, as well as all text in charts, tables, figures, and graphs.

- Use a font that is either 12 point or larger or no smaller than 10 pitch (characters per inch).

- Use one of the following fonts: Times New Roman, Courier, Courier New, or Arial.

The recommended page limit does not apply to the cover sheet; the budget

section, including the narrative budget justification; the assurances and certifications; or the one-page abstract, the resumes, the bibliography, or the letters of support. However, the recommended page limit does apply to the application narrative.

6. *Notice of Intent To Apply:* The Department will be able to review grant applications more efficiently if we know the approximate number of applicants that intend to apply. Therefore, we strongly encourage each potential applicant to notify us of their intent to submit an application. To do so, please email the program contact person listed under **FOR FURTHER INFORMATION CONTACT** with the subject line “Intent To Apply,” and include the applicant’s name and a contact person’s name and email address. Applicants that do not submit a notice of intent to apply may still apply for funding; applicants that do submit a notice of intent to apply are not bound to apply or bound by the information provided.

V. Application Review Information

1. *Selection Criteria:* The selection criteria for this competition are from 34 CFR 75.210 or are established for the FFY 2023 grant competition and any subsequent year in which we make awards from the list of unfunded applications from this competition, in accordance with section 437(d)(1) of GEPA, and are as follows:

(a) *Need for project and significance of the project (10 points)*

(1) The Secretary considers the need for the proposed project and the significance of the proposed project.

(2) In determining the need for the proposed project and the significance of the proposed project, the Secretary considers the following factors:

(i) The magnitude of the need for the services to be provided or the activities to be carried out by the proposed project.

(ii) The extent to which the proposed project is likely to build local capacity to provide, improve, or expand services that address the needs of the target population.

(b) *Quality of the project design (20 points)*

(1) The Secretary considers the quality of the design of the proposed project.

(2) In determining the quality of the design of the proposed project, the Secretary considers the following factors:

(i) The extent to which the goals, objectives, and outcomes to be achieved by the proposed project are clearly specified and measurable.

(ii) The extent to which the design of the proposed project reflects up-to-date knowledge from research and effective practice.

(iii) The extent to which the results of the proposed project are to be disseminated in ways that will enable others to use the information or strategies. (Section 437(d)(1) of GEPA.)

(iv) The extent to which the proposed project represents an exceptional innovative approach to the priority established for the competition.

(v) The extent to which performance feedback and continuous improvement are integral to the design of the proposed project.

(c) *Quality of project services (20 points)*

(1) The Secretary considers the quality of the services to be provided by the proposed project.

(2) In determining the quality of services to be provided by the proposed project, the Secretary considers the quality and sufficiency of strategies for ensuring equal access and treatment for eligible proposed project participants who are members of groups that have traditionally been underrepresented based on race, color, national origin, gender, age, or disability.

(3) In addition, the Secretary considers the following factors:

(i) The extent to which the services to be provided by the proposed project involve the collaboration of appropriate partners for maximizing the effectiveness and seamlessness of proposed project services. (Section 437(d)(1) of GEPA.)

(ii) The extent to which the services to be provided by the proposed project are appropriate to the needs of the intended recipients or beneficiaries of those services.

(iii) The likely impact of the services to be provided by the proposed project on the intended recipients of those services.

(d) *Quality of the project evaluation (20 points)*

(1) The Secretary considers the quality of the evaluation to be conducted of the proposed project.

(2) In determining the quality of the evaluation, the Secretary considers the following factors:

(i) The extent to which the methods of evaluation are thorough, feasible, and appropriate to the goals, objectives, and outcomes of the proposed project.

(ii) The extent to which the evaluation will provide performance feedback and permit periodic assessment of progress toward achieving intended outcomes.

(e) *Quality of project personnel (15 points)*

(1) The Secretary considers the quality of the personnel who will carry out the proposed project.

(2) In determining the quality of proposed project personnel, the Secretary considers the extent to which the applicant encourages applications for employment from persons who are members of groups that have traditionally been underrepresented based on race, color, national origin, gender, age, or disability.

(3) In addition, the Secretary considers the following factors:

(i) The qualifications, including relevant training and experience, of key project personnel.

(ii) The extent to which the time commitments of the project director and principal investigator and other key personnel are appropriate and adequate to meet the objectives of the proposed project. (Section 437(d)(1) of GEPA.)

(f) *Adequacy of resources (15 points)*

(1) The Secretary considers the adequacy of resources for the proposed project.

(2) In determining the adequacy of resources for the proposed project, the Secretary considers the following factors:

(i) The relevance and demonstrated commitment of each partner in the proposed project to the implementation and success of the project.

(ii) The extent to which the costs are reasonable in relation to the number of persons to be served and to the anticipated results and benefits.

(iii) The potential for the incorporation of proposed project purposes, activities, or benefits into the ongoing program of the agency or organization at the end of the Federal funding.

(iv) The adequacy of support, including facilities, equipment, supplies, and other resources, from the applicant organization.

2. *Review and Selection Process:* We remind potential applicants that in reviewing applications in any discretionary grant competition, the Secretary may consider, under 34 CFR 75.217(d)(3), the past performance of the applicant in carrying out a previous award, such as the applicant’s use of funds, achievement of proposed project objectives, and compliance with grant conditions. The Secretary may also consider whether the applicant failed to submit a timely performance report or submitted a report of unacceptable quality.

In addition, in making a competitive grant award, the Secretary requires various assurances, including those applicable to Federal civil rights laws that prohibit discrimination in programs

or activities receiving Federal financial assistance from the Department (34 CFR 100.4, 104.5, 106.4, 108.8, and 110.23).

For the FFY 2023 grant competition and any subsequent year in which we make awards from the list of unfunded applications from this competition, in accordance with section 437(d)(1) of GEPA, in selecting an application for an award under this program, we also consider the geographical distribution of projects in the DIF program throughout the country. This factor will be applied after non-Federal reviewers score the applications. The geographical distribution of projects factor will be applied to fund applications out of rank order if the top-ranked applications do not represent a geographical distribution throughout the country.

3. Risk Assessment and Specific Conditions: Consistent with 2 CFR 200.206, before awarding grants under this competition the Department conducts a review of the risks posed by applicants. Under 2 CFR 200.208, the Secretary may impose specific conditions and, under 2 CFR 3474.10, in appropriate circumstances, high-risk conditions on a grant if the applicant or grantee is not financially stable; has a history of unsatisfactory performance; has a financial or other management system that does not meet the standards in 2 CFR part 200, subpart D; has not fulfilled the conditions of a prior grant; or is otherwise not responsible.

4. Integrity and Performance System: If you are selected under this competition to receive an award that over the course of the proposed project period may exceed the simplified acquisition threshold (currently \$250,000), under 2 CFR 200.206(a)(2) we must make a judgment about your integrity, business ethics, and record of performance under Federal awards—that is, the risk posed by you as an applicant—before we make an award. In doing so, we must consider any information about you that is in the integrity and performance system (currently referred to as the Federal Awardee Performance and Integrity Information System (FAPIS)), accessible through the System for Award Management. You may review and comment on any information about yourself that a Federal agency previously entered and that is currently in FAPIS.

Please note that if the total value of your currently active grants, cooperative agreements, and procurement contracts from the Federal Government exceeds \$10,000,000, the reporting requirements in 2 CFR part 200, Appendix XII, require you to report certain integrity information to FAPIS semiannually.

Please review the requirements in 2 CFR part 200, Appendix XII, if this grant plus all the other Federal funds you receive exceed \$10,000,000.

5. In General: In accordance with the Office of Management and Budget's guidance located at 2 CFR part 200, all applicable Federal laws, and relevant Executive guidance, the Department will review and consider applications for funding pursuant to this notice inviting applications in accordance with:

(a) Selecting recipients most likely to be successful in delivering results based on the program objectives through an objective process of evaluating Federal award applications (2 CFR 200.205);

(b) Prohibiting the purchase of certain telecommunication and video surveillance services or equipment in alignment with section 889 of the National Defense Authorization Act of 2019 (Pub. L. 115–232) (2 CFR 200.216).

(c) Providing a preference, to the extent permitted by law, to maximize use of goods, products, and materials produced in the United States (2 CFR 200.322); and

(d) Terminating agreements in whole or in part to the greatest extent authorized by law if an award no longer effectuates the program goals or agency priorities (2 CFR 200.340).

VI. Award Administration Information

1. Award Notices: If your application is successful, we notify your U.S. Representative and U.S. Senators and send you a Grant Award Notification (GAN); or we may send you an email containing a link to access an electronic version of your GAN. We also may notify you informally.

If your application is not evaluated or not selected for funding, we notify you.

2. Administrative and National Policy Requirements: We identify administrative and national policy requirements in the application package and reference these and other requirements in the *Applicable Regulations* section of this notice.

We reference the regulations outlining the terms and conditions of an award in the *Applicable Regulations* section of this notice and include these and other specific conditions in the GAN. The GAN also incorporates your approved application as part of your binding commitments under the grant.

3. Open Licensing Requirements: Unless an exception applies, if you are awarded a grant under this competition, you will be required to openly license to the public grant deliverables created in whole, or in part, with Department grant funds. When the deliverable consists of modifications to pre-existing

works, the license extends only to those modifications that can be separately identified and only to the extent that open licensing is permitted under the terms of any licenses or other legal restrictions on the use of pre-existing works. Additionally, a grantee or subgrantee that is awarded competitive grant funds must have a plan to disseminate these public grant deliverables. This dissemination plan can be developed and submitted after your application has been reviewed and selected for funding. For additional information on the open licensing requirements please refer to 2 CFR 3474.20.

4. Reporting: (a) If you apply for a grant under this competition, you must ensure that you have in place the necessary processes and systems to comply with the reporting requirements in 2 CFR part 170 should you receive funding under the competition. This does not apply if you have an exception under 2 CFR 170.110(b).

(b) At the end of the project period, September 30, 2028, you must submit a final performance report, including financial information, as directed by the Secretary. If you receive a multiyear award, you must submit annual performance reports and end of year performance reports that provide the most current performance and financial expenditure information as directed by the Secretary under 34 CFR 75.118. The Secretary may also require more frequent performance reports under 34 CFR 75.720(c). For specific requirements on reporting, please go to www.ed.gov/fund/grant/apply/appforms/appforms.html.

(c) Under 34 CFR 75.250(b), the Secretary may provide a grantee with additional funding for data collection analysis and reporting. In this case, the Secretary establishes a data collection period.

5. Performance Measures: Under the absolute priority, grant recipients must develop and implement a plan to measure the innovative model demonstration project's performance and outcomes, including an evaluation of the practices and strategies implemented by the project. The performance measures will be developed in collaboration with the Department or its contracted independent evaluators during the first three months of the awards. Performance measures may, for example, assess the impact of project activities on effective collaboration and child and youth outcomes, access to resources, sustainability, and the replicability of project. The cooperative agreement, for year 1, will specify the

program measures that will be used to assess the grantees' performance in achieving the goals and objectives of the competition.

VII. Other Information

Accessible Format: On request to the program contact person listed under **FOR FURTHER INFORMATION CONTACT**, individuals with disabilities can obtain this document and a copy of the application package in an accessible format. The Department will provide the requestor with an accessible format that may include Rich Text Format (RTF) or text format (txt), a thumb drive, an MP3 file, braille, large print, audiotape, or compact disc, or other accessible format.

Electronic Access to This Document: The official version of this document is the document published in the **Federal Register**. You may access the official edition of the **Federal Register** and the Code of Federal Regulations at www.govinfo.gov. At this site you can view this document, as well as all other documents of this Department published in the **Federal Register**, in text or Portable Document Format (PDF). To use PDF, you must have Adobe Acrobat Reader, which is available free at the site.

You may also access documents of the Department published in the **Federal Register** by using the article search feature at: www.federalregister.gov. Specifically, through the advanced search feature at this site, you can limit your search to documents published by the Department.

Katherine Neas,

Deputy Assistant Secretary, Delegated the authority to perform the functions and duties of the Assistant Secretary for the Office of Special Education and Rehabilitative Services.

[FR Doc. 2023-07204 Filed 4-3-23; 4:15 pm]

BILLING CODE 4000-01-P

DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

[Project No. 15029-001]

SV Hydro, LLC; Notice of Surrender of Preliminary Permit

Take notice that SV Hydro, LLC, permittee for the proposed Itasca County Pumped Storage Project, has requested that its preliminary permit be terminated. The permit was issued on October 28, 2020, and would have expired on September 30, 2024.¹ The

project would have been located near the City of Marble, Itasca County, Minnesota.

The preliminary permit for Project No. 15029 will remain in effect until the close of business, April 28, 2023. But, if the Commission is closed on this day, then the permit remains in effect until the close of business on the next day in which the Commission is open.² New applications for this site may not be submitted until after the permit surrender is effective.

Dated: March 29, 2023.

Kimberly D. Bose,

Secretary.

[FR Doc. 2023-07016 Filed 4-4-23; 8:45 am]

BILLING CODE 6717-01-P

DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

Combined Notice of Filings

Take notice that the Commission has received the following Natural Gas & Oil Pipeline Rate and Refund Report filings:

Filings Instituting Proceedings

Docket Numbers: PR23-39-000.

Applicants: Southwest Gas Corporation.

Description: § 284.123(g) Rate Filing: Amended SOC for Blanket Certificate to be effective 4/1/2023.

Filed Date: 4/19/23.

Accession Number: 20230329-5197.

Comment Date: 5 p.m. ET 5/30/23.

Docket Numbers: RP23-607-000.

Applicants: Florida Gas Transmission Company, LLC.

Description: § 4(d) Rate Filing: New Non-Conforming Agreement—FP&L to be effective 4/1/2023.

Filed Date: 3/29/23.

Accession Number: 20230329-5203.

Comment Date: 5 p.m. ET 4/10/23.

Docket Numbers: RP23-608-000.

Applicants: Florida Gas Transmission Company, LLC.

Description: § 4(d) Rate Filing: New NRAs—OUC and Peoples and Update Non-Conf List to be effective 4/1/2023.

Filed Date: 3/29/23.

Accession Number: 20230329-5205.

Comment Date: 5 p.m. ET 4/10/23.

Docket Numbers: RP23-609-000.

Applicants: Horizon Pipeline Company, L.L.C.

Description: § 4(d) Rate Filing: NRA Filing—Natural Gas Pipeline Company of America LLC to be effective 4/1/2023.

Filed Date: 3/29/23.

Accession Number: 20230329-5209.

Comment Date: 5 p.m. ET 4/10/23.

Docket Numbers: RP23-610-000.

Applicants: Iroquois Gas

Transmission System, L.P.

Description: Iroquois Gas Transmission System, L.P. submits Fuel and Losses Retention Percentage calculations for 2022.

Filed Date: 3/29/23.

Accession Number: 20230329-5226.

Comment Date: 5 p.m. ET 4/10/23.

Docket Numbers: RP23-611-000.

Applicants: Northern Border Pipeline Company.

Description: § 4(d) Rate Filing: Negotiated Rate Agreement—Sequent TL368F/101321 to be effective 4/1/2023.

Filed Date: 3/30/23.

Accession Number: 20230330-5002.

Comment Date: 5 p.m. ET 4/11/23.

Docket Numbers: RP23-612-000.

Applicants: MountainWest Overthrust Pipeline, LLC.

Description: § 4(d) Rate Filing: Non-conforming TSA WIC 6343 to be effective 4/1/2023.

Filed Date: 3/30/23.

Accession Number: 20230330-5025.

Comment Date: 5 p.m. ET 4/11/23.

Docket Numbers: RP23-613-000.

Applicants: Equitrans, L.P.

Description: § 4(d) Rate Filing:

Amended Negotiated Rate Agreement—4/1/2023 to be effective 4/1/2023.

Filed Date: 3/30/23.

Accession Number: 20230330-5030.

Comment Date: 5 p.m. ET 4/11/23.

Docket Numbers: RP23-614-000.

Applicants: Equitrans, L.P.

Description: § 4(d) Rate Filing:

Negotiated Rate Agreements to be effective 4/1/2023.

Filed Date: 3/30/23.

Accession Number: 20230330-5031.

Comment Date: 5 p.m. ET 4/11/23.

Docket Numbers: RP23-615-000.

Applicants: Enable Gas Transmission, LLC.

Description: § 4(d) Rate Filing: Cancel SWEPCO Agreement to be effective 4/1/2023.

Filed Date: 3/30/23.

Accession Number: 20230330-5060.

Comment Date: 5 p.m. ET 4/11/23.

Docket Numbers: RP23-616-000.

Applicants: Enable Gas Transmission, LLC.

Description: § 4(d) Rate Filing: Amended NRA Filing—SWEPCO to be effective 4/1/2023.

Filed Date: 3/30/23.

Accession Number: 20230330-5061.

Comment Date: 5 p.m. ET 4/11/23.

Docket Numbers: RP23-617-000.

Applicants: Stagecoach Pipeline & Storage Company LLC.

Description: § 4(d) Rate Filing:

Stagecoach—Chesapeake, DTE, Amera &

¹ 173 FERC ¶ 62,047 (2020).

² 18 CFR 385.2007(a)(2) (2022).

KM Gas Marketing to be effective 4/1/2023.

Filed Date: 3/30/23.

Accession Number: 20230330–5065.

Comment Date: 5 p.m. ET 4/11/23.

Docket Numbers: RP23–618–000.

Applicants: El Paso Natural Gas Company, L.L.C.

Description: § 4(d) Rate Filing: Negotiated Rate Agmt Update (Conoco—Apr 23) to be effective 4/1/2023.

Filed Date: 3/30/23.

Accession Number: 20230330–5079.

Comment Date: 5 p.m. ET 4/11/23.

Any person desiring to intervene or protest in any of the above proceedings must file in accordance with Rules 211 and 214 of the Commission's Regulations (18 CFR 385.211 and 385.214) on or before 5:00 p.m. Eastern time on the specified comment date. Protests may be considered, but intervention is necessary to become a party to the proceeding.

Filings in Existing Proceedings

Docket Numbers: RP20–780–002.

Applicants: Pine Needle LNG Company, LLC.

Description: Compliance filing: Petition to Amend Settlement in Docket No. RP20–780–000 to be effective N/A.

Filed Date: 3/30/23.

Accession Number: 20230330–5108.

Comment Date: 5 p.m. ET 4/11/23.

Any person desiring to protest in any of the above proceedings must file in accordance with Rule 211 of the Commission's Regulations (18 CFR 385.211) on or before 5:00 p.m. Eastern time on the specified comment date.

The filings are accessible in the Commission's eLibrary system (<https://elibrary.ferc.gov/idmws/search/fercgensearch.asp>) by querying the docket number.

eFiling is encouraged. More detailed information relating to filing requirements, interventions, protests, service, and qualifying facilities filings can be found at: <http://www.ferc.gov/docs-filing/efiling/filing-req.pdf>. For other information, call (866) 208–3676 (toll free). For TTY, call (202) 502–8659.

Dated: March 30, 2023.

Debbie-Anne A. Reese,

Deputy Secretary.

[FR Doc. 2023–07105 Filed 4–4–23; 8:45 am]

BILLING CODE 6717–01–P

DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

[Docket No. AD20–21–000]

Notice of Availability of Revised Final Engineering Guidelines for the Evaluation of Hydropower Projects: Chapter 16—Part 12d Program

On December 16, 2021, the Federal Energy Regulatory Commission issued a Notice of Availability of Final Engineering Guidelines for the Evaluation of Hydropower Projects: Chapter 16—Part 12D Program.¹ Chapter 16 provides licensee guidance related to any Periodic Inspection or Comprehensive Assessment performed, and the report on it filed, to fulfill the requirements defined in Title 18 Code of Federal Regulations (CFR) Part 12, Subpart D. The Chapter includes an overview of the part 12D program, as well as six appendices. Appendices B, C, D, and E are outlines for the four major types of reports that must be submitted. Due to a compilation error during final preparation of the chapter, four of the included appendices were from an outdated draft version that did not incorporate all of the changes that staff made to address comments received on the draft chapter. This notice provides a revised version of Chapter 16's appendices B, C, D, and E, which were the only portions of Chapter 16 that were affected by this error.

The appendices provide the outlines and instructions for several required filings that document a Part 12D Inspection and are required by the Commission's regulations: Appendix B: the Periodic Inspection Report (PIR), Appendix C: Periodic Inspection Pre-Inspection Preparation Report (PI-PIPR), Appendix D: Comprehensive Assessment Report (CAR), and Appendix E: Comprehensive Assessment Pre-Inspection Preparation Report (CA-PIPR). These revisions to Appendices B through E ensure that the report outlines and content are consistent with the corresponding text in the body of Chapter 16. The revisions in each appendix are described below.

Chapter 16, Appendix B—Outline for the Periodic Inspection Report

- Section 1.2 Potential Failure Modes and Risk

¹ Chapter 16 is one of four new chapters of the Guidelines providing additional guidance related to 18 CFR part 12, Safety of Water Power Projects and Project Works, for which a Final Rule was also issued on December 16, 2021. Final Rule, Order No. 880, 87 FR 1490 (Jan. 11, 2022), 177 FERC ¶ 61,204 (2021).

- Listed the types of potential failure modes (PFMs) to summarize and provided an example table to document the findings.
- Section 1.3.3 Hazard Potential Classification
 - Clarified that the significant changes to the population at risk must be identified since the previous Part 12D Inspection.
- Section 1.4 Recommendations
 - Provided an example table to summarize recommendations and the suggested schedule.
- Section 2.1 Location and Purpose
 - Revised reference to Appendix C: Project Figures.
- Section 2.2 Description of Project Features
 - Clarified that the project information must not be a copy and paste from the STID.
 - Added “tunnel lining drainage holes” to the bulleted list for Water Conveyances.
- Section 3.3 Recommendations of Previous Independent Consultants
 - Revised heading text.
 - Clarified that the summary table must include recommendations from “earlier” Part 12D reports.
- Section 3.7 Previously Identified PFMs
 - Clarified that the IC Team can provide recommendations to improve the PFMA and PFMs
- Section 4 Field Inspection Observations and Interpretation of Monitoring Data
 - Revised the use of standard terms to describe the condition of project features allowing the IC Team to use consistent terminology provided the terms are identified and defined.
- Section 4.2.1 Field Inspection Observations
 - Revised reference to Appendix E: Inspection Photographs.
- Section 4.2.2 Review and Evaluation of Instrumentation Data and Surveillance
 - Revised reference to Appendix D: Instrumented Monitoring Data Plots.
- Section 5.5 Public Safety Plan
 - Inserted the requirement that the Public Safety Plan must also document the licensee's response and implementation of any required remediation measures related to project-related public safety incidents.
- Appendix B FERC Letter Approving Part 12D Inspection Plan and IC Team
 - Revised appendix title.
- Appendix C Summary of Independent Consultant's Recommendations

- Appendix deleted.
- Appendices D through H
 - Redesignated as Appendices C through G due to the removal of Appendix C.
 - Subsequent revisions listed below are for the redesignated appendix label.
- Appendix D Instrumented Monitoring Data Plots
 - Revised appendix title and text from “Instrumentation Monitoring” to “Instrumented Monitoring.”
 - Revised content to be provided in the appendix from reproductions of entire Dam Safety Surveillance and Monitoring Reports (DSSMRs) to excerpts from and citations to previous DSSMRs relevant to the review.
- Appendix E Inspection Photographs
 - Revised description of how to provide full resolution digital photographs.

Chapter 16, Appendix C—Outline for the Periodic Inspection Pre-Inspection Preparation Report (PI-PIPR)

- Changes to ensure consistency in headings and text with the above list of changes in Chapter 16, Appendix B
- Addition of placeholder sections to the outline to ensure consistent numbering between the PIR and PI-PIPR. Placeholder sections are marked with the following text: “This section is reserved as a placeholder so the numbering is consistent with the PIR. No content is required to be provided in this section of the PI-PIPR.”

Chapter 16, Appendix D—Outline for the Comprehensive Assessment Report (CAR)

- Section 1.2 Potential Failure Modes and Risk
 - Section 1.2 is redesignated as Section 1.5 Potential Failure Modes Analysis, Risk Analysis, and Dam Safety Risk Classification.
 - Revised Section 1.5 to provide separate subsections as listed below, describing the required content:
 - Section 1.5.1 Potential Failure Modes Analysis
 - Section 1.5.2 Level 2 Risk Analysis
 - Section 1.5.3 Dam Safety Risk Classification
- Sections 1.3 through 1.5
 - Redesignated as Sections 1.2 through 1.4 due to the redesignation of the above listed item.
- Section 1.6 Recommendations
 - Provided an example table to summarize recommendations and the suggested schedule.

- Section 2.2 Description of Project Features
 - Clarified that the project information must not be a copy and paste from the STID
 - Added “tunnel lining drainage holes” to the bulleted list for Water Conveyances.
- Section 3.2.1 Design Considerations
 - Revised final bullet to clarify that the current state of practice means “at the time of the Comprehensive Assessment.”
- Section 3.5
 - Revised heading text from “Powerplant” to “Powerhouse”
- Section 4: Review and Evaluation of Previous Analysis
 - Revised reference to Appendix J: Independent Calculations
- Section 4.4 Analyses of Project Features
 - Redesignated subheadings from “4.4.X” to “4.4.1” for Project Feature 1, with a further example provided as “4.4.2” for Project Feature 2 and so forth.
- Section 5.3 Recommendations of Previous Independent Consultants
 - Revised heading text.
 - Clarified that the summary table must include recommendations from “earlier” Part 12D reports.
- Section 6 Field Inspection Observations and Interpretation of Monitoring Data
 - Revised the use of standard terms to describe the condition of project features allowing the IC Team to use consistent terminology provided the terms are identified and defined.
- Section 6.2.1 Field Inspection Observations
 - Revised reference to Appendix E: Inspection Photographs.
- Section 6.2.2 Review and Evaluation of Instrumentation Data and Surveillance
 - Revised reference to Appendix D: Instrumented Monitoring Data Plots.
- Section 7.5 PFMA
 - Provided two sets of instructions depending on whether the IC Team prepared the PFMA report.
- Section 7.6 Risk Analysis and Summary
 - Revised instructions depending on whether the IC Team prepared the Risk Analysis report.
- Section 8.8 Supporting Technical Information Document and Digital Project Archive
 - Added “and Digital Project Archive” to the heading text.
 - Revised subheadings 8.8.5, 8.8.7, 8.8.8, and 8.8.9 to more closely match the STID headings provided

- in Chapter 15 of the Engineering Guidelines.
- Appendix B FERC Letter Approving Part 12D Inspection Plan and IC Team
 - Revised appendix title.
- Appendix C Summary of Independent Consultant’s Recommendations
 - Appendix deleted.
- Appendices D through H
 - Redesignated as Appendices C through J due to the removal of Appendix C.
 - Subsequent revisions listed below are for the redesignated appendix label.
- Appendix D Instrumented Monitoring Data Plots
 - Revised appendix title and text from “Instrumentation Monitoring” to “Instrumented Monitoring”
 - Revised content to be provided in the appendix from reproductions of entire Dam Safety Surveillance and Monitoring Reports (DSSMRs) to excerpts from and citations to previous DSSMRs relevant to the review.

Chapter 16, Appendix E—Outline for the Comprehensive Assessment Pre-Inspection Preparation Report (CA-PIPR)

- Changes to ensure consistency in headings and text with the above list of changes in Chapter 16, Appendix D
- Addition of placeholder sections to the outline to ensure consistent numbering between the CAR and CA-PIPR. Placeholder sections are marked with the following text: “This section is reserved as a placeholder so the numbering is consistent with the CAR. No content is required to be provided in this section of the CA-PIPR.”

All information related to “Chapter 16—Part 12D Program,” including the draft chapter, all submitted comments, the final chapter, and the revised final chapter incorporating the above listed revisions, can be found on the FERC website (www.ferc.gov) using the eLibrary link. Click on the eLibrary link, click on “General Search” and enter the docket number, excluding the last three digits in the Docket Number field (*i.e.*, AD20–21). Be sure you have selected an appropriate date range. The Commission also offers a free service called eSubscription that allows you to keep track of all formal issuances and submittals in specific dockets. This can reduce the amount of time you spend researching proceedings by automatically providing you with electronic notification of these filings and direct links to the documents. Go to

the Commission's website (www.ferc.gov), select the FERC Online option from the left-hand column, and click on eSubscription. Users must be registered in order to use eSubscription.

The revised version of Chapter 16 is also available on the Commission's Division of Dam Safety and Inspections website at: Engineering Guidelines for the Evaluation of Hydropower Projects | Federal Energy Regulatory Commission ([ferc.gov](http://www.ferc.gov)).

For assistance with any of the Commission's online systems, please contact FERC Online Support at FercOnlineSupport@ferc.gov or toll free at (866) 208-3676, or for TTY, contact (202) 502-8258.

Dated: March 29, 2023.

Kimberly D. Bose,
Secretary.

[FR Doc. 2023-07015 Filed 4-4-23; 8:45 am]

BILLING CODE 6717-01-P

DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

[Docket No. ER23-1512-000]

Westlake Natrium LLC; Supplemental Notice That Initial Market-Based Rate Filing Includes Request for Blanket Section 204 Authorization

This is a supplemental notice in the above-referenced proceeding of Westlake Natrium LLC's application for market-based rate authority, with an accompanying rate tariff, noting that such application includes a request for blanket authorization, under 18 CFR part 34, of future issuances of securities and assumptions of liability.

Any person desiring to intervene or to protest should file with the Federal Energy Regulatory Commission, 888 First Street NE, Washington, DC 20426, in accordance with Rules 211 and 214 of the Commission's Rules of Practice and Procedure (18 CFR 385.211 and 385.214). Anyone filing a motion to intervene or protest must serve a copy of that document on the Applicant.

Notice is hereby given that the deadline for filing protests with regard to the applicant's request for blanket authorization, under 18 CFR part 34, of future issuances of securities and assumptions of liability, is April 19, 2023.

The Commission encourages electronic submission of protests and interventions in lieu of paper, using the FERC Online links at <http://www.ferc.gov>. To facilitate electronic service, persons with internet access

who will eFile a document and/or be listed as a contact for an intervenor must create and validate an eRegistration account using the eRegistration link. Select the eFiling link to log on and submit the intervention or protests.

Persons unable to file electronically may mail similar pleadings to the Federal Energy Regulatory Commission, 888 First Street NE, Washington, DC 20426. Hand delivered submissions in docketed proceedings should be delivered to Health and Human Services, 12225 Wilkins Avenue, Rockville, Maryland 20852.

In addition to publishing the full text of this document in the **Federal Register**, the Commission provides all interested persons an opportunity to view and/or print the contents of this document via the internet through the Commission's Home Page (<http://www.ferc.gov>) using the "eLibrary" link. Enter the docket number excluding the last three digits in the docket number field to access the document. At this time, the Commission has suspended access to the Commission's Public Reference Room, due to the proclamation declaring a National Emergency concerning the Novel Coronavirus Disease (COVID-19), issued by the President on March 13, 2020. For assistance, contact the Federal Energy Regulatory Commission at FERCOnlineSupport@ferc.gov or call toll-free, (886) 208-3676 or TYY, (202) 502-8659.

Dated: March 30, 2023.

Debbie-Anne A. Reese,
Deputy Secretary.

[FR Doc. 2023-07104 Filed 4-4-23; 8:45 am]

BILLING CODE 6717-01-P

DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

Combined Notice of Filings #1

Take notice that the Commission received the following Complaints and Compliance filings in EL Dockets:

Docket Numbers: EL23-51-000.

Applicants: American Municipal Power, Inc., et al. v. AEP Appalachian Transmission Company Inc., et al.

Description: Joint Formal Challenge and Complaint of American Municipal Power, Inc., et al. v. AEP Appalachian Transmission Company Inc., et al.

Filed Date: 3/15/23.

Accession Number: 20230315-5231.

Comment Date: 5 p.m. ET 4/11/23.

Take notice that the Commission received the following electric rate filings:

Docket Numbers: ER21-2678-004.

Applicants: Westlands Transmission, LLC.

Description: Compliance filing: Settlement—Approved Effective Date—Solar Blue (ER21-2678-) to be effective 10/13/2021.

Filed Date: 3/30/23.

Accession Number: 20230330-5213.

Comment Date: 5 p.m. ET 4/20/23.

Docket Numbers: ER21-2679-004.

Applicants: Westlands Transmission, LLC.

Description: Compliance filing: Settlement—Approved Effective Date—Grape (ER21-2679-) to be effective 10/13/2021.

Filed Date: 3/30/23.

Accession Number: 20230330-5205.

Comment Date: 5 p.m. ET 4/20/23.

Docket Numbers: ER21-2680-004.

Applicants: Westlands Transmission, LLC.

Description: Compliance filing: Settlement—Approved Effective Date—Chestnut (ER21-2680-) to be effective 10/13/2021.

Filed Date: 3/30/23.

Accession Number: 20230330-5198.

Comment Date: 5 p.m. ET 4/20/23.

Docket Numbers: ER21-2681-004.

Applicants: Westlands Transmission, LLC.

Description: Compliance filing: Settlement—Approved Effective Date—Cherry (ER21-2681-) to be effective 10/13/2021.

Filed Date: 3/30/23.

Accession Number: 20230330-5196.

Comment Date: 5 p.m. ET 4/20/23.

Docket Numbers: ER23-1041-001.

Applicants: Florida Power & Light Company.

Description: Tariff Amendment: FPL Amendment to Attachment A Specifications for Amended TSA No. 332 to be effective 1/4/2023.

Filed Date: 3/30/23.

Accession Number: 20230330-5129.

Comment Date: 5 p.m. ET 4/20/23.

Docket Numbers: ER23-1512-000.

Applicants: Westlake Natrium LLC.

Description: Baseline eTariff Filing: Application for Market Based Rate Authority to be effective 5/29/2023.

Filed Date: 3/30/23.

Accession Number: 20230330-5000.

Comment Date: 5 p.m. ET 4/20/23.

Docket Numbers: ER23-1513-000.

Applicants: Pacific Gas and Electric Company.

Description: Tariff Amendment: Termination of High Winds, LLC (TO SA 40) to be effective 5/30/2023.

Filed Date: 3/30/23.

Accession Number: 20230330–5001.

Comment Date: 5 p.m. ET 4/20/23.

Docket Numbers: ER23–1514–000.

Applicants: PECO Energy Company, PJM Interconnection, L.L.C.

Description: § 205(d) Rate Filing: PECO Energy Company submits tariff filing per 35.13(a)(2)(iii): PECO submits revisions to Formula Rate, OATT Attachment H–7A to be effective 5/30/2023.

Filed Date: 3/30/23.

Accession Number: 20230330–5026.

Comment Date: 5 p.m. ET 4/20/23.

Docket Numbers: ER23–1515–000.

Applicants: PJM Interconnection, L.L.C.

Description: § 205(d) Rate Filing: Amendment to ISA, Service Agreement No. 5859; Queue No. AD1–081 to be effective 5/29/2023.

Filed Date: 3/30/23.

Accession Number: 20230330–5054.

Comment Date: 5 p.m. ET 4/20/23.

Docket Numbers: ER23–1516–000.

Applicants: Southwest Power Pool, Inc.

Description: § 205(d) Rate Filing: Tariff Clean-Up Filing for NorthWestern Formula Rate to be effective 9/1/2021.

Filed Date: 3/30/23.

Accession Number: 20230330–5055.

Comment Date: 5 p.m. ET 4/20/23.

Docket Numbers: ER23–1517–000.

Applicants: IP Oberon II, LLC.

Description: Baseline eTariff Filing: Application for Market Based Rate Tariff to be effective 5/30/2023.

Filed Date: 3/30/23.

Accession Number: 20230330–5147.

Comment Date: 5 p.m. ET 4/20/23.

Docket Numbers: ER23–1518–000.

Applicants: Midcontinent Independent System Operator, Inc.

Description: § 205(d) Rate Filing: 2023–03–30 SA 3006 Duke-Jordan Creek 4th Rev GIA (J515 J1470) to be effective 3/21/2023.

Filed Date: 3/30/23.

Accession Number: 20230330–5164.

Comment Date: 5 p.m. ET 4/20/23.

Docket Numbers: ER23–1519–000.

Applicants: Atlas Solar, III, LLC.

Description: Baseline eTariff Filing: Atlas Solar III MBR Application Filing to be effective 3/31/2023.

Filed Date: 3/30/23.

Accession Number: 20230330–5211.

Comment Date: 5 p.m. ET 4/20/23.

The filings are accessible in the Commission's eLibrary system (<https://elibrary.ferc.gov/idmws/search/fercensearch.asp>) by querying the docket number.

Any person desiring to intervene or protest in any of the above proceedings

must file in accordance with Rules 211 and 214 of the Commission's Regulations (18 CFR 385.211 and 385.214) on or before 5:00 p.m. Eastern time on the specified comment date. Protests may be considered, but intervention is necessary to become a party to the proceeding.

eFiling is encouraged. More detailed information relating to filing requirements, interventions, protests, service, and qualifying facilities filings can be found at: <http://www.ferc.gov/docs-filing/efiling/filing-req.pdf>. For other information, call (866) 208–3676 (toll free). For TTY, call (202) 502–8659.

Dated: March 30, 2023.

Debbie-Anne A. Reese,

Deputy Secretary.

[FR Doc. 2023–07106 Filed 4–4–23; 8:45 am]

BILLING CODE 6717–01–P

DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

[Docket No. ER23–1504–000]

Partin Solar LLC; Supplemental Notice That Initial Market-Based Rate Filing Includes Request for Blanket Section 204 Authorization

This is a supplemental notice in the above-referenced proceeding of Partin Solar LLC's application for market-based rate authority, with an accompanying rate tariff, noting that such application includes a request for blanket authorization, under 18 CFR part 34, of future issuances of securities and assumptions of liability.

Any person desiring to intervene or to protest should file with the Federal Energy Regulatory Commission, 888 First Street NE, Washington, DC 20426, in accordance with Rules 211 and 214 of the Commission's Rules of Practice and Procedure (18 CFR 385.211 and 385.214). Anyone filing a motion to intervene or protest must serve a copy of that document on the Applicant.

Notice is hereby given that the deadline for filing protests with regard to the applicant's request for blanket authorization, under 18 CFR part 34, of future issuances of securities and assumptions of liability, is April 19, 2023.

The Commission encourages electronic submission of protests and interventions in lieu of paper, using the FERC Online links at <http://www.ferc.gov>. To facilitate electronic service, persons with internet access who will eFile a document and/or be listed as a contact for an intervenor

must create and validate an eRegistration account using the eRegistration link. Select the eFiling link to log on and submit the intervention or protests.

Persons unable to file electronically may mail similar pleadings to the Federal Energy Regulatory Commission, 888 First Street NE, Washington, DC 20426. Hand delivered submissions in docketed proceedings should be delivered to Health and Human Services, 12225 Wilkins Avenue, Rockville, Maryland 20852.

In addition to publishing the full text of this document in the **Federal Register**, the Commission provides all interested persons an opportunity to view and/or print the contents of this document via the internet through the Commission's Home Page (<http://www.ferc.gov>) using the "eLibrary" link. Enter the docket number excluding the last three digits in the docket number field to access the document. At this time, the Commission has suspended access to the Commission's Public Reference Room, due to the proclamation declaring a National Emergency concerning the Novel Coronavirus Disease (COVID–19), issued by the President on March 13, 2020. For assistance, contact the Federal Energy Regulatory Commission at FERCOnlineSupport@ferc.gov or call toll-free, (866) 208–3676 or TTY, (202) 502–8659.

Dated: March 30, 2023.

Debbie-Anne A. Reese,

Deputy Secretary.

[FR Doc. 2023–07103 Filed 4–4–23; 8:45 am]

BILLING CODE 6717–01–P

DEPARTMENT OF ENERGY

Southwestern Power Administration

Integrated System Power Rates

AGENCY: Southwestern Power Administration, DOE.

ACTION: Notice of proposed change to Southwestern Power Administration Integrated System Wholesale Rates for Hydro Peaking Power Rate Schedule and opportunity for public review and comment.

SUMMARY: The Administrator, Southwestern Power Administration (Southwestern), is proposing to update the Peaking Energy Schedule Submission Time in Southwestern's existing Integrated System Wholesale Rates for Hydro Peaking Power (P–13A) Rate Schedule. Southwestern has determined that the shift in Peaking Energy Schedule Submission Time from

the current 2:30 p.m. CPT to the proposed 8:30 a.m. CPT provides Southwestern with more flexibility and greater certainty when making replacement power purchases, and better aligns with regional energy market considerations.

DATES: The consultation and comment period will begin on April 5, 2023 and will end on May 5, 2023. Written comments are due on or before May 5, 2023.

ADDRESSES: Comments should be submitted to Ms. Fritha Ohlson, Senior Vice President and Chief Operating Officer, Southwestern Power Administration, U.S. Department of Energy, 1 W 3rd St, Suite 1500, Tulsa, OK 74103.

FOR FURTHER INFORMATION CONTACT: Ms. Fritha Ohlson, Senior Vice President, Chief Operating Officer, Office of Corporate Operations, (918) 595-6684 or fritha.ohlson@swpa.gov.

SUPPLEMENTARY INFORMATION: Originally established by Order 1865, Secretary of the Interior, dated August 31, 1943 and effective September 1, 1943 (8 FR 12142 (Sept. 3, 1943)), Southwestern is authorized by Congress to market the hydroelectric power and energy from Federal dams controlled by the U.S. Army Corps of Engineers (Corps), pursuant to Section 302(a)(1) of the Department of Energy Organization Act (42 U.S.C. 7152(a)(1)), Section 5 of the Flood Control Act of 1944 (16 U.S.C. 825s), and Public Law 95-456 (16 U.S.C. 825s-3). Guidelines for preparation of power repayment studies are included in Department of Energy (DOE) Order No. RA 6120.2 (Sept. 20, 1979), entitled *Power Marketing Administration Financial Reporting*. Procedures for public participation in power and transmission rate adjustments of the Power Marketing Administrations are found at title 10, part 903, subpart A of the Code of Federal Regulations (10 CFR part 903). Procedures for the confirmation and approval of rates for the Federal Power Marketing Administrations are found at title 18, part 300, subpart L of the Code of Federal Regulations (18 CFR part 300).

Southwestern markets power from 24 multi-purpose reservoir projects with hydroelectric power facilities constructed and operated by the Corps. These projects are located in Arkansas, Missouri, Oklahoma, and Texas. Southwestern's marketing area includes these states plus Kansas and Louisiana. The costs associated with 22 of these 24 hydropower projects are repaid with revenues received under the Integrated System rates. These rates also cover the costs of Southwestern's transmission

facilities that consist of 1,381 miles of high-voltage transmission lines, 27 substations, and 46 microwave and VHF radio sites. Additionally, Southwestern markets power from two hydropower projects in southeastern Texas, Sam Rayburn Dam and Robert D. Willis. These projects are isolated hydraulically, electrically, and financially from the Integrated System, and are repaid via separate rate schedules and therefore are not addressed in this Notice.

On September 30, 2013, in Rate Order No. SWPA-66, the Deputy Secretary of Energy placed into effect Southwestern's Integrated System rate schedules (P-13, NFTS-13, and EE-13) on an interim basis for the period October 1, 2013 to September 30, 2017. The Federal Energy Regulatory Commission (FERC) confirmed and approved Southwestern's interim Integrated System rates on a final basis on January 9, 2014 for a period ending September 30, 2017.

Southwestern re-designated Integrated System rate schedule "NFTS-13" as "NFTS-13A" with no revenue adjustment. In Rate Order No. SWPA-71, the Deputy Secretary of Energy placed into effect Southwestern's rate schedule NFTS-13A on an interim basis beginning January 1, 2017. FERC confirmed and approved NFTS-13A on a final basis on March 9, 2017.

On September 13, 2017, in Rate Order No. SWPA-72, the Deputy Secretary of Energy extended all of Southwestern's Integrated System rate schedules (P-13, NTFs-13A, and EE-13) for two years, for the period of October 1, 2017 through September 30, 2019.

Southwestern re-designated Integrated System rate schedule "P-13" as "P-13A" with no revenue adjustment. In Rate Order No. SWPA-73, the Assistant Secretary for Electricity placed into effect Southwestern's rate schedule P-13A on an interim basis beginning July 1, 2019. FERC confirmed and approved P-13A on a final basis on August 29, 2019.

On September 22, 2019, in Rate Order No. SWPA-74, the Assistant Secretary for Electricity extended all of Southwestern's Integrated System rate schedules (P-13A, NTFs-13A, EE-13) for two years, for the period of October 1, 2019 through September 30, 2021.

On August 30, 2021, in Rate Order No. SWPA-77, the Administrator, Southwestern, extended all of Southwestern's Integrated System rate schedules (P-13A, NTFs-13A, EE-13) for two years, for the period of October 1, 2021 through September 30, 2023.

Decision Rationale

The proposed update to Section 4.2, Peaking Energy Schedule Submission Time, establishes the Peaking Energy Schedule Submission Time as on or before 8:30 a.m. Central Prevailing Time (CPT) of the day preceding the day for delivery of Peaking Energy. Additionally, the proposed update to Section 4.2.2, Procedure for Adjusting the Peaking Energy Schedule Submission Time, allows the Southwestern Administrator to adjust the Peaking Energy Schedule Submission Time once annually to a time no earlier than 8:00 a.m. CPT and no later than 9:00 a.m. CPT. There is no change in annual revenues associated with the proposed P-13A Rate Schedule change.

Southwestern must at times make replacement capacity and energy purchases to fulfill its contractual obligations associated with the delivery of Hydro Peaking Power as required through the majority of Power Sales Contracts that utilize Southwestern's Integrated System rate schedules. Historically, a significant portion of needed replacement power purchases were made through pre-arranged Purchase Power Agreements (PPAs), many of which were capacity and energy "call options" that allowed Southwestern to schedule the energy as needed after the Peaking Energy Schedule Submission Time of 2:00 p.m. or 2:30 p.m. In recent months, the number of PPAs available to Southwestern has decreased and the pricing of available PPAs has increased. Southwestern has also recently become a Financial-Only Market Participant of the Midcontinent Independent System Operator (MISO), which enables Southwestern to make energy purchases from the MISO Day-Ahead Market. The MISO Day-Ahead Market closes bidding at 9:30 a.m. CPT every day. In order to best utilize the MISO Day-Ahead Market as a cost-competitive option for replacement energy purchases, Southwestern must have increased certainty about its Peaking Energy obligations before 9:30 a.m. the day before the Peaking Energy will be delivered. Earlier day-ahead certainty of Peaking Energy schedules will also likely provide Southwestern with better options when seeking new PPAs. Many of Southwestern's customers have expressed support for such a change. Therefore, Southwestern determined that it would pursue shifting its Peaking Energy Schedule Submission Time from 2:30 p.m. CPT to 8:30 a.m. CPT.

The title of the P-13A Rate Schedule will be changed to P-13B to reflect

update to Section 4.2. A redlined version of the P-13A Rate Schedule, which shows the revision proposed by the P-13B Rate Schedule, will be made available upon request.

Public Review and Comment

In accordance with 10 CFR part 903, Southwestern's proposed change to its P-13A Rate Schedule is considered a minor rate adjustment, as there is no change in annual revenues. 10 CFR part 903 provides that neither a public information forum nor a public comment forum is required in conjunction with the consultation and comment period for a minor rate adjustment. Therefore, Southwestern finds that holding a public information and comment forum in conjunction with the consultation and comment period is not necessary. In accordance with 10 CFR 903.14, Southwestern is initiating a 30-day consultation and comment period (see **DATES** section) during which Southwestern will accept written comments from interested persons.

Following review and consideration of written comments, the Administrator will determine whether to confirm, approve, and place the proposed P-13B Rate Schedule into effect on an interim basis, and subsequently submit to the Federal Energy Regulatory Commission (FERC) for confirmation and approval on a final basis. The FERC will allow the public an opportunity to provide written comments on the proposed rate schedule change before making a final decision.

Legal Authority

By Delegation Order No. S1-DEL-RATES-2016, effective November 19, 2016, the Secretary of Energy delegated: (1) the authority to develop power and transmission rates to Southwestern's Administrator; (2) the authority to confirm, approve, and place such rates into effect on an interim basis to the Deputy Secretary of Energy; and (3) the authority to confirm, approve, and place into effect on a final basis, or to remand or disapprove such rates, to FERC. By Delegation Order No. S1-DEL-S3-2022-2, effective June 13, 2022, the Secretary of Energy also delegated the authority to confirm, approve, and place such rates into effect on an interim basis to the Under Secretary for Infrastructure. By Redelegation Order No. S3-DEL-SWPA1-2022, effective June 13, 2022, the Under Secretary for Infrastructure redelegated the authority to confirm, approve, and place such rates into effect on an interim basis to the Administrator, Southwestern.

Environmental Impact

Southwestern previously determined that the rate change actions, placed into effect on October 1, 2013, fit within the following class of categorically excluded actions as listed in Appendix B to Subpart D of 10 CFR part 1021, DOE's Implementing Procedures and Guidelines of the National Environmental Policy Act of 1969, as amended (42 U.S.C. 4321-4347): B4.3 (Electric power marketing rate changes). Categorically excluded actions do not require preparation of either an environmental impact statement or an environmental assessment. On March 14, 2023, Southwestern determined that categorical exclusion B4.3 applies to the current action as well.

Determination Under Executive Order 12866

Southwestern has an exemption from centralized regulatory review under Executive Order 12866; accordingly, no clearance of this notice by the Office of Management and Budget is required.

Signing Authority

This document of the Department of Energy was signed on March 27, 2023, by Mike Wech, Administrator for Southwestern Power Administration, pursuant to delegated authority from the Secretary of Energy. That document, with the original signature and date, is maintained by DOE. For administrative purposes only, and in compliance with requirements of the Office of the Federal Register, the undersigned DOE Federal Register Liaison Officer has been authorized to sign and submit the document in electronic format for publication, as an official document of DOE. This administrative process in no way alters the legal effect of this document upon publication in the **Federal Register**.

Signed in Washington, DC, on March 31, 2023.

Treena V. Garrett,

Federal Register Liaison Officer, U.S. Department of Energy.

[FR Doc. 2023-07059 Filed 4-4-23; 8:45 am]

BILLING CODE 6450-01-P

ENVIRONMENTAL PROTECTION AGENCY

[EPA-HQ-OW-2023-0095; FRL-10844-01-OW]

Proposed Information Collection Request; Comment Request; Clean Water Act Water Quality Certification

AGENCY: Environmental Protection Agency (EPA).

ACTION: Notice.

SUMMARY: The Environmental Protection Agency (EPA) is planning to submit an information collection request (ICR), "ICR Supporting Statement Information Collection Request for Clean Water Act Water Quality Certification" (EPA ICR No. 2603.07, OMB Control No. 2040-0295), to the Office of Management and Budget (OMB) for review and approval in accordance with the Paperwork Reduction Act (PRA). Before doing so, EPA is soliciting public comments on specific aspects of the proposed information collection as described below. This is a proposed extension of an ICR (OMB Control No. 2040-0295), which is currently approved through July 31, 2023. An Agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number.

DATES: Comments must be submitted on or before June 5, 2023.

ADDRESSES: Submit your comments, referencing Docket ID No. EPA-HQ-OW-2023-0095, online using www.regulations.gov (our preferred method) or by mail to: EPA Docket Center, Environmental Protection Agency, Mail Code 28221T, 1200 Pennsylvania Ave. NW, Washington, DC 20460.

EPA's policy is that all comments received will be included in the public docket without change including any personal information provided, unless the comment includes profanity, threats, information claimed to be Confidential Business Information (CBI), or other information whose disclosure is restricted by statute.

FOR FURTHER INFORMATION CONTACT: Liana Prudencio, Oceans, Wetlands, and Communities Division, Office of Wetlands, Oceans, and Watersheds, (MC 4504T), Environmental Protection Agency, 1200 Pennsylvania Ave. NW, Washington, DC 20460; telephone number: (202) 564-3351; email address: cwa401@epa.gov.

SUPPLEMENTARY INFORMATION:

Supporting documents which explain in detail the information that the EPA will be collecting are available in the public docket for this ICR. The docket can be viewed online at www.regulations.gov or in person at the EPA Docket Center, WJC West, Room 3334, 1301 Constitution Ave. NW, Washington, DC. The telephone number for the Docket Center is 202-566-1744. For additional information about EPA's public docket, visit <http://www.epa.gov/dockets>.

Pursuant to section 3506(c)(2)(A) of the PRA, the EPA is soliciting comments

and information to enable it to: (i) evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the Agency, including whether the information will have practical utility; (ii) evaluate the accuracy of the Agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used; (iii) enhance the quality, utility, and clarity of the information to be collected; and (iv) minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., electronic submission of responses. EPA will consider the comments received and amend the ICR as appropriate. EPA will then submit the final ICR package to OMB for review and approval. At that time, EPA will issue another **Federal Register** notice to announce the submission of the ICR to OMB and the opportunity to submit additional comments to OMB.

Abstract: This ICR describes the cost and burden associated with 40 CFR part 121, the regulations that implement Clean Water Act (CWA) section 401. Under section 401, a Federal agency may not issue a permit or license that may result in any discharge into waters of the United States unless the certifying authority where the discharge would originate issues a section 401 water quality certification verifying that the discharge will comply with certain water quality requirements or waives the certification requirement. Certifying authorities are states, tribes with treatment as a state (TAS) authorization, and in limited circumstances, EPA. CWA section 401 requires project proponents to submit project-specific information to certifying authorities. Certifying authorities may act on project-specific information by either granting, granting with conditions, denying, or waiving section 401 certification. To demonstrate it has acted on the certification request, the certifying authority must provide a decision document to the relevant federal licensing or permitting agency. If the certifying authority fails or refuses to act on a certification request within a reasonable period of time (which shall not exceed one year) after receipt, the requirement to obtain certification is waived. EPA is also responsible for coordinating input from certain neighboring or downstream states and tribes affected by a discharge from a

federally licensed or permitted project under section 401(a)(2). Information collected directly collected by EPA under section 401 in support of the section 402 permit program is already captured under an existing ICR (OMB Control Number 2040-0004, EPA ICR Number 0229.22) and therefore is not included in this analysis.

Form Numbers: None.

Respondents/affected entities: Project proponents, State and tribal reviewers (certifying authorities).

Respondent's obligation to respond: required to obtain 401 certification (33 U.S.C. 1341(a)(1)).

Estimated number of respondents: 154,000 responses from 77,138 respondents annually.

Frequency of response: one per Federal application.

Total estimated burden: 860,500 hours (per year). Burden is defined at 5 CFR 1320.03(b).

Total estimated cost: \$48 Million (per year), includes \$0 annualized capital or operation and maintenance costs.

Changes in Estimates: There are changes in the total estimated respondent burden, number of respondents, and number of responses compared with the ICR currently approved by OMB (OMB Control No. 2040-0295).

Brian Frazer,

Acting Director, Office of Wetlands, Oceans, and Watersheds, Office of Water.

[FR Doc. 2023-07060 Filed 4-4-23; 8:45 am]

BILLING CODE 6560-50-P

ENVIRONMENTAL PROTECTION AGENCY

[EPA-HQ-OGC-2023-0198; FRL-10838-01-OGC]

Proposed Consent Decree, Clean Air Act Citizen Suit

AGENCY: Environmental Protection Agency (EPA).

ACTION: Notice of proposed consent decree; request for public comment.

SUMMARY: In accordance with the Clean Air Act, as amended (CAA or the Act), notice is given of a proposed consent decree in *Center for Biological Diversity et al., v. Regan*, No. 3:22-cv-03309-RS (N.D. Cal.). On June 7, 2022, Plaintiffs Center for Biological Diversity and Center for Environmental Health filed a complaint in the United States District Court for the Northern District of California. On September 12, 2022, Plaintiffs filed an amended complaint. Plaintiffs alleged that the Environmental Protection Agency (EPA or the Agency)

failed to perform certain non-discretionary duties in accordance with the Act to timely respond to numerous state implementation plan (SIP) submissions from the State of North Dakota, the State of California, the State of Colorado, and the State of Pennsylvania. Plaintiffs also alleged that EPA failed to promulgate a federal implementation plan (FIP) for the State of California and the State of New Hampshire. Certain claims included in the Amended Complaint have since been rendered moot, and the proposed consent decree would establish deadlines for EPA to sign a notice of final rulemaking on the remaining claims.

DATES: Written comments on the proposed consent decree must be received by May 5, 2023.

ADDRESSES: Submit your comments, identified by Docket ID No. EPA-HQ-OGC-2023-0198, online at <https://www.regulations.gov> (EPA's preferred method). Follow the online instructions for submitting comments.

Instructions: All submissions received must include the Docket ID number for this action. Comments received may be posted without change to <https://www.regulations.gov/>, including any personal information provided. For detailed instructions on sending comments and additional information on the rulemaking process, see the "Additional Information about Commenting on the Proposed Consent Decree" heading under the **SUPPLEMENTARY INFORMATION** section of this document.

FOR FURTHER INFORMATION CONTACT: Elizabeth Pettit, Air and Radiation Law Office, Office of General Counsel, U.S. Environmental Protection Agency; telephone (202) 566-2879; email address pettit.elizabeth@epa.gov.

SUPPLEMENTARY INFORMATION:

I. Obtaining a Copy of the Proposed Consent Decree

The official public docket for this action (identified by Docket ID No. EPA-HQ-OGC-2023-0198) contains a copy of the proposed consent decree. The official public docket is available for public viewing at the Office of Environmental Information (OEI) Docket in the EPA Docket Center, EPA West, Room 3334, 1301 Constitution Ave., NW, Washington, DC. The EPA Docket Center Public Reading Room is open from 8:30 a.m. to 4:30 p.m., Monday through Friday, excluding legal holidays. The telephone number for the Public Reading Room is (202) 566-1744, and the telephone number for the OEI Docket is (202) 566-1752.

The electronic version of the public docket for this action contains a copy of the proposed consent decree, and is available through <https://www.regulations.gov>. You may use <https://www.regulations.gov> to submit or view public comments, access the index listing of the contents of the official public docket, and access those documents in the public docket that are available electronically. Once in the system, key in the appropriate docket identification number then select “search.”

II. Additional Information About the Proposed Consent Decree

The proposed consent decree would establish deadlines for EPA to take action pursuant to CAA section 110(k) on certain SIP submissions by the State of Colorado, the State of California, and the State of New Hampshire. First, on March 22, 2021, the State of Colorado made a SIP submission addressing CAA section 182(c) requirements for the Denver Metro/North Front Range Serious nonattainment area under the 2008 ozone national ambient air quality standards (NAAQS). The proposed consent decree would require EPA to sign a notice of final rulemaking by September 29, 2023.

Second, on February 3, 2017, EPA published a final rule that found that various nonattainment areas in the State of California and the State of New Hampshire failed to submit SIP revisions for various nonattainment SIP elements. The proposed consent decree would require EPA to sign a notice of final rulemaking for the nonattainment new source review (NSR) SIP element for the Los Angeles—San Bernardino Counties (West Mojave Desert), California nonattainment area by November 29, 2024. The proposed consent decree would require EPA to sign a notice of final rulemaking for various SIP elements or control techniques guidelines (CTG) for the Sacramento Metro, California nonattainment area (Sacramento Metropolitan Air Quality Management District) by March 31, 2024. The proposed consent decree would require EPA to sign a notice of final rulemaking for the reasonably available control technology (RACT) nitrogen oxides (NOx) for Major Sources SIP element for the Sacramento Metro, California nonattainment area (Sacramento Metropolitan Air Quality Management District) by September 30, 2024. The proposed consent decree would require EPA to sign a notice of final rulemaking for various SIP elements or CTG for the Sacramento Metro, California nonattainment area (Yolo-Solano Air

Quality Management District) by March 31, 2024. The proposed consent decree would require EPA to sign a notice of final rulemaking for various SIP elements or CTG for the New Hampshire portion of the ozone transport region by September 30, 2023. The proposed consent decree would require EPA to sign a notice of final rulemaking for the portion of the revision to the Placer County Air Pollution Control District portion of the California SIP concerning the minor source NSR by September 30, 2023.

Third, on December 29, 2020, the State of California made a SIP submission addressing the 2020 RACT demonstration for the 2008 ozone NAAQS for San Diego County. The proposed consent decree would require EPA to sign a notice of final rulemaking for the demonstration, except for four declarations, by October 31, 2024.

In accordance with section 113(g) of the CAA, for a period of thirty (30) days following the date of publication of this document, the Agency will accept written comments relating to the proposed consent decree. EPA or the Department of Justice may withdraw or withhold consent to the proposed consent decree if the comments disclose facts or considerations that indicate that such consent is inappropriate, improper, inadequate, or inconsistent with the requirements of the Act.

III. Additional Information About Commenting on the Proposed Consent Decree

Submit your comments, identified by Docket ID No. EPA-HQ-OGC-2023-0198, via <https://www.regulations.gov>. Once submitted, comments cannot be edited or removed from this docket. EPA may publish any comment received to its public docket. Do not submit to EPA's docket at <https://www.regulations.gov> any information you consider to be Confidential Business Information (CBI) or other information whose disclosure is restricted by statute. Multimedia submissions (audio, video, etc.) must be accompanied by a written comment. The written comment is considered the official comment and should include discussion of all points you wish to make. EPA will generally not consider comments or comment contents located outside of the primary submission (i.e. on the web, cloud, or other file sharing system). For additional submission methods, the full EPA public comment policy, information about CBI or multimedia submissions, and general guidance on making effective comments, please visit <https://www.epa.gov/dockets/commenting-epa->

dockets. For additional information about submitting information identified as CBI, please contact the person listed in the **FOR FURTHER INFORMATION CONTACT** section of this document. Note that written comments containing CBI and submitted by mail may be delayed and deliveries or couriers will be received by scheduled appointment only.

If you submit an electronic comment, EPA recommends that you include your name, mailing address, and an email address or other contact information in the body of your comment. This ensures that you can be identified as the submitter of the comment and allows EPA to contact you in case EPA cannot read your comment due to technical difficulties or needs further information on the substance of your comment. Any identifying or contact information provided in the body of a comment will be included as part of the comment that is placed in the official public docket and made available in EPA's electronic public docket. If EPA cannot read your comment due to technical difficulties and cannot contact you for clarification, EPA may not be able to consider your comment.

Use of the <https://www.regulations.gov> website to submit comments to EPA electronically is EPA's preferred method for receiving comments. The electronic public docket system is an “anonymous access” system, which means EPA will not know your identity, email address, or other contact information unless you provide it in the body of your comment.

Please ensure that your comments are submitted within the specified comment period. Comments received after the close of the comment period will be marked “late.” EPA is not required to consider these late comments.

Gautam Srinivasan,

Associate General Counsel.

[FR Doc. 2023-07061 Filed 4-4-23; 8:45 am]

BILLING CODE 6560-50-P

FEDERAL COMMUNICATIONS COMMISSION

[FR ID 134608]

Privacy Act of 1974; Matching Program

AGENCY: Federal Communications Commission.

ACTION: Notice of a new matching program.

SUMMARY: In accordance with the Privacy Act of 1974, as amended (“Privacy Act”), this document announces a new computer matching

program the Federal Communications Commission (“FCC” or “Commission” or “Agency”) and the Universal Service Administrative Company (USAC) will conduct with the Florida Department of Children and Families, Office of Economic Self Sufficiency. The purpose of this matching program is to verify the eligibility of applicants to and subscribers of Lifeline, and the Affordable Connectivity Program (ACP), both of which are administered by USAC under the direction of the FCC. More information about these programs is provided in the **SUPPLEMENTARY INFORMATION** section below.

DATES: Written comments are due on or before May 5, 2023. This computer matching program will commence on May 5, 2023, and will conclude 18 months after the effective date.

ADDRESSES: Send comments to Elliot S. Tarloff, FCC, 45 L Street NE, Washington, DC 20554, or to Privacy@fcc.gov.

FOR FURTHER INFORMATION CONTACT: Elliot S. Tarloff at 202–418–0886 or Privacy@fcc.gov.

SUPPLEMENTARY INFORMATION: The Lifeline program provides support for discounted broadband and voice services to low-income consumers. Lifeline is administered by the Universal Service Administrative Company (USAC) under FCC direction. Consumers qualify for Lifeline through proof of income or participation in a qualifying program, such as Medicaid, the Supplemental Nutritional Assistance Program (SNAP), Federal Public Housing Assistance, Supplemental Security Income (SSI), Veterans and Survivors Pension Benefit, or various Tribal-specific federal assistance programs.

In the Consolidated Appropriations Act, 2021, Pub. L. 116–260, 134 Stat. 1182, 2129–36 (2020), Congress created the Emergency Broadband Benefit Program, and directed use of the National Verifier to determine eligibility based on various criteria, including the qualifications for Lifeline (Medicaid, SNAP, etc.). EBBP provided \$3.2 billion in monthly consumer discounts for broadband service and one-time provider reimbursement for a connected device (laptop, desktop computer or tablet). In the Infrastructure Investment and Jobs Act, Pub. L. 117–58, 135 Stat. 429, 1238–44 (2021) (codified at 47 U.S.C. 1751–52), Congress modified and extended EBBP, provided an additional \$14.2 billion, and renamed it the Affordable Connectivity Program (ACP). A household may qualify for the ACP benefit under various criteria, including

an individual qualifying for the FCC’s Lifeline program.

In a Report and Order adopted on March 31, 2016, (81 FR 33026, May 24, 2016) (*2016 Lifeline Modernization Order*), the Commission ordered USAC to create a National Lifeline Eligibility Verifier (“National Verifier”), including the National Lifeline Eligibility Database (LED), that would match data about Lifeline applicants and subscribers with other data sources to verify the eligibility of an applicant or subscriber. The Commission found that the National Verifier would reduce compliance costs for Lifeline service providers, improve service for Lifeline subscribers, and reduce waste, fraud, and abuse in the program.

The Consolidated Appropriations Act of 2021 directs the FCC to leverage the National Verifier to verify applicants’ eligibility for ACP. The purpose of this matching program is to verify the eligibility of Lifeline and ACP applicants and subscribers by determining whether they receive SNAP and Medicaid benefits administered by the Florida Department of Children and Families, Office of Economic Self Sufficiency.

Participating Agencies

Florida Department of Children and Families, Office of Economic Self Sufficiency.

Authority for Conducting the Matching Program

The authority for the FCC’s ACP is Infrastructure Investment and Jobs Act, Public Law 117–58, 135 Stat. 429, 1238–44 (2021) (codified at 47 U.S.C. 1751–52); 47 CFR part 54. The authority for the FCC’s Lifeline program is 47 U.S.C. 254; 47 CFR 54.400 through 54.423; Lifeline and Link Up Reform and Modernization, *et al.*, Third Report and Order, Further Report and Order, and Order on Reconsideration, 31 FCC Rcd 3962, 4006–21, paras. 126–66 (2016) (*2016 Lifeline Modernization Order*).

Purpose(s)

The purpose of this modified matching agreement is to verify the eligibility of applicants and subscribers to Lifeline, as well as to ACP and other Federal programs that use qualification for Lifeline as an eligibility criterion. This new agreement will permit eligibility verification for the Lifeline program and ACP by checking an applicant’s/subscriber’s participation in SNAP and Medicaid in Florida. Under FCC rules, consumers receiving these benefits qualify for Lifeline discounts and also for ACP benefits.

Categories of Individuals

The categories of individuals whose information is involved in the matching program include, but are not limited to, those individuals who have applied for Lifeline and/or ACP benefits; are currently receiving Lifeline and/or ACP benefits; are individuals who enable another individual in their household to qualify for Lifeline and/or ACP benefits; are minors whose status qualifies a parent or guardian for Lifeline and/or ACP benefits; or are individuals who have received Lifeline and/or ACP benefits.

Categories of Records

The categories of records involved in the matching program include, but are not limited to, the last four digits of the applicant’s Social Security Number, date of birth, and first and last name. The National Verifier will transfer these data elements to the Florida Department of Children and Families, Office of Economic Self Sufficiency, which will respond either “yes” or “no” that the individual is enrolled in a qualifying assistance program: SNAP and Medicaid administered by the Florida Department of Children and Families, Office of Economic Self Sufficiency.

System(s) of Records

The records shared as part of this matching program reside in the Lifeline system of records, FCC/WCB–1, Lifeline, which was published in the **Federal Register** at 86 FR 11526 (Feb. 25, 2021).

The records shared as part of this matching program reside in the ACP system of records, FCC/WCB–3, Affordable Connectivity Program, which was published in the **Federal Register** at 86 FR 71494 (Dec. 16, 2021).

Federal Communications Commission.

Marlene Dortch,

Secretary.

[FR Doc. 2023–07067 Filed 4–4–23; 8:45 am]

BILLING CODE 6712–01–P

FEDERAL MARITIME COMMISSION

Notice of Agreements Filed

The Commission hereby gives notice of filing of the following agreements under the Shipping Act of 1984. Interested parties may submit comments, relevant information, or documents regarding the agreements to the Secretary by email at Secretary@fmc.gov, or by mail, Federal Maritime Commission, 800 North Capitol Street, Washington, DC 20573. Comments will be most helpful to the Commission if

received within 12 days of the date this notice appears in the **Federal Register**, and the Commission requests that comments be submitted within 7 days on agreements that request expedited review. Copies of agreements are available through the Commission's website (www.fmc.gov) or by contacting the Office of Agreements at (202) 523-5793 or tradeanalysis@fmc.gov.

Agreement No.: 201402.

Agreement Name: American Roll-On Roll-Off Carrier/Liberty Space Charter Agreement.

Parties: American Roll-On Roll-Off Carrier, LLC; Liberty Global Logistics LLC.

Filing Party: Bryant Gardner, Winston & Strawn LLP.

Synopsis: The Agreement would authorize the parties to discuss areas of potential cooperation and possibly engage in the purchasing of space on the vessels operated by one another for direct service or transshipment from ports and points in the United States, on the one hand, and ports and points in all other countries worldwide, on the other hand.

Proposed Effective Date: 5/8/2023.

Location: <https://www2.fmc.gov/FMC.Agreements.Web/Public/AgreementHistory/78502>.

Dated: March 31, 2023.

JoAnne O'Bryant,

Program Analyst.

[FR Doc. 2023-07075 Filed 4-4-23; 8:45 am]

BILLING CODE 6730-02-P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Disease Control and Prevention

[Docket No. CDC-2023-0020]

Laboratory Recommendations for Syphilis Testing in the United States

AGENCY: Centers for Disease Control and Prevention (CDC), Department of Health and Human Services (HHS).

ACTION: Notice with comment period.

SUMMARY: The Centers for Disease Control and Prevention (CDC), in the Department of Health and Human Services (HHS), announces the opening of a docket to obtain comment on the proposed Laboratory Recommendations for Syphilis Testing in the United States. The proposed recommendations for syphilis testing include laboratory-based tests, point-of-care tests, processing of samples, and reporting of test results. The recommendations are intended to aid laboratorians and

clinicians in the diagnosis of syphilis. These proposed recommendations are intended for use by clinical laboratory directors, laboratory staff, clinicians, and disease control personnel who must choose among the multiple available testing methods, establish standard operating procedures for collecting and processing specimens, interpret test results for laboratory reporting, and counsel and treat patients in the United States.

DATES: Written comments must be received on or before June 5, 2023.

ADDRESSES: You may submit comments, identified by Docket No. CDC-2023-0020 by either of the methods listed below. Do not submit comments by email. CDC does not accept comments by email.

- *Federal eRulemaking Portal:* <http://www.regulations.gov>. Follow the instructions for submitting comments.

- *Mail:* Division of STD Prevention, Centers for Disease Control and Prevention, 1600 Clifton Road NE, Mailstop US12-2, Atlanta, GA 30329, Attn: Docket No. CDC-2023-0020.

Instructions: All submissions received must include the agency name and Docket Number. All relevant comments received will be posted without change to <http://regulations.gov>, including any personal information provided. For access to the docket to read background documents or comments received, go to <http://www.regulations.gov>.

FOR FURTHER INFORMATION CONTACT: John R. Papp, Centers for Disease Control and Prevention, 1600 Clifton Road NE, Mailstop U12-3, Atlanta, GA 30329; Telephone: 404-639-8000; Email: jwp6@cdc.gov.

SUPPLEMENTARY INFORMATION: CDC's proposed Laboratory Recommendations for Syphilis Testing in the United States is available under the Supporting and Related Materials tab in the docket for this notice, Docket No. CDC-2023-0020, on <http://www.regulations.gov>.

Public Participation

Interested persons or organizations are invited to participate by submitting written views, recommendations, and data. In addition, CDC invites comments specifically on the following questions proposed in this Notice:

- Based on the evidence presented in the full recommendations document (see the Supporting and Related Materials tab in the docket), does the evidence support the proposed Laboratory Recommendations for Syphilis Testing in the United States? If not, please state the reason why and, if available, provide additional evidence for consideration.

- Are CDC's proposed Laboratory Recommendations for Syphilis Testing in the United States (see Supporting and Related Materials) clearly written? If not, what changes do you propose to make them clearer?

- If implemented as currently drafted, do you believe the proposed recommendations would result in improved laboratory testing for syphilis in the United States? If not, please provide an explanation and supporting data or evidence.

Please note that comments received, including attachments and other supporting materials, are part of the public record and are subject to public disclosure. Comments will be posted on <https://www.regulations.gov>. Therefore, do not include any information in your comment or supporting materials that you consider confidential or inappropriate for public disclosure. If you include your name, contact information, or other information that identifies you in the body of your comments, that information will be on public display. CDC will review all submissions and may choose to redact, or withhold, submissions containing private or proprietary information such as Social Security numbers, medical information, inappropriate language, or duplicate/near duplicate examples of a mass-mail campaign. Do not submit comments by email. CDC does not accept comments by email.

Background

Syphilis is a notifiable disease, with over 130,000 cases in the United States reported to the CDC in 2020 (CDC, 2020) and over 6 million new cases reported worldwide (World Health Organization, 2018). Syphilis is caused by *Treponema pallidum* subspecies *pallidum*. The United States is currently experiencing a syphilis epidemic, with sustained increases in primary and secondary syphilis. In 2000, 5,979 cases were reported; in 2020 the figure rose to 133,945 cases, a 2,140% increase (CDC, 2001, 2020). The epidemic is characterized by health disparities, particularly among sexual and gender minority populations, intersections with the HIV and substance use epidemics, and increased morbidity and mortality attributable to congenital syphilis infections (CDC, 2020). Laboratories play a critical role in the public health response to the syphilis epidemic. The responsibility of the laboratory is to test specimens and report results in a timely manner, allowing clinicians to efficiently make diagnoses and institute patient management protocols. Public health reporting by laboratories also allows local health departments and

CDC to conduct surveillance and monitoring of disease trends. CDC used current evidence to draft the proposed Laboratory Recommendations for Syphilis Testing in the United States to improve laboratory testing for syphilis and aid laboratorians and clinicians in the diagnosis of the disease.

Dated: March 31, 2023.

Tiffany Brown,

Acting Executive Secretary, Centers for Disease Control and Prevention.

[FR Doc. 2023-07057 Filed 4-4-23; 8:45 am]

BILLING CODE 4163-18-P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Food and Drug Administration

[Docket No. FDA-2023-D-0592]

Human User Safety in New and Abbreviated New Animal Drug Applications; Draft Guidance for Industry; Availability

AGENCY: Food and Drug Administration, HHS.

ACTION: Notice of availability.

SUMMARY: The Food and Drug Administration (FDA or Agency) is announcing the availability of a draft guidance for industry #278 (GFI #278) entitled “Human User Safety in New and Abbreviated New Animal Drug Applications.” Human User Safety (HUS) is an integral component of the overall safety evaluation of proposed new animal drugs. FDA is issuing this guidance to clarify the current approaches and recommendations of FDA’s Center for Veterinary Medicine (CVM) for HUS assessment and submission of HUS information to support the overall safety of proposed new animal drugs prior to approval.

DATES: Submit either electronic or written comments on the draft guidance by June 5, 2023 to ensure that the Agency considers your comment on this draft guidance before it begins work on the final version of the guidance.

ADDRESSES: You may submit comments on any guidance at any time as follows:

Electronic Submissions

Submit electronic comments in the following way:

- *Federal eRulemaking Portal:* <https://www.regulations.gov>. Follow the instructions for submitting comments. Comments submitted electronically, including attachments, to <https://www.regulations.gov> will be posted to the docket unchanged. Because your comment will be made public, you are

solely responsible for ensuring that your comment does not include any confidential information that you or a third party may not wish to be posted, such as medical information, your or anyone else’s Social Security number, or confidential business information, such as a manufacturing process. Please note that if you include your name, contact information, or other information that identifies you in the body of your comments, that information will be posted on <https://www.regulations.gov>.

- If you want to submit a comment with confidential information that you do not wish to be made available to the public, submit the comment as a written/paper submission and in the manner detailed (see “Written/Paper Submissions” and “Instructions”).

Written/Paper Submissions

Submit written/paper submissions as follows:

- *Mail/Hand Delivery/Courier (for written/paper submissions):* Dockets Management Staff (HFA-305), Food and Drug Administration, 5630 Fishers Lane, Rm. 1061, Rockville, MD 20852.

- For written/paper comments submitted to the Dockets Management Staff, FDA will post your comment, as well as any attachments, except for information submitted, marked and identified, as confidential, if submitted as detailed in “Instructions.”

Instructions: All submissions received must include the Docket No. FDA-2023-D-0592 for “Human User Safety in New and Abbreviated New Animal Drug Applications.” Received comments will be placed in the docket and, except for those submitted as “Confidential Submissions,” publicly viewable at <https://www.regulations.gov> or at the Dockets Management Staff between 9 a.m. and 4 p.m., Monday through Friday, 240-402-7500.

- **Confidential Submissions**—To submit a comment with confidential information that you do not wish to be made publicly available, submit your comments only as a written/paper submission. You should submit two copies total. One copy will include the information you claim to be confidential with a heading or cover note that states “THIS DOCUMENT CONTAINS CONFIDENTIAL INFORMATION.” The Agency will review this copy, including the claimed confidential information, in its consideration of comments. The second copy, which will have the claimed confidential information redacted/blacked out, will be available for public viewing and posted on <https://www.regulations.gov>. Submit both copies to the Dockets Management Staff. If you do not wish your name and

contact information to be made publicly available, you can provide this information on the cover sheet and not in the body of your comments and you must identify this information as “confidential.” Any information marked as “confidential” will not be disclosed except in accordance with 21 CFR 10.20 and other applicable disclosure law. For more information about FDA’s posting of comments to public dockets, see 80 FR 56469, September 18, 2015, or access the information at: <https://www.govinfo.gov/content/pkg/FR-2015-09-18/pdf/2015-23389.pdf>.

Docket: For access to the docket to read background documents or the electronic and written/paper comments received, go to <https://www.regulations.gov> and insert the docket number, found in brackets in the heading of this document, into the “Search” box and follow the prompts and/or go to the Dockets Management Staff, 5630 Fishers Lane, Rm. 1061, Rockville, MD 20852, 240-402-7500.

You may submit comments on any guidance at any time (see 21 CFR 10.115(g)(5)).

Submit written requests for single copies of the guidance to the Policy and Regulations Staff (HFV-6), Center for Veterinary Medicine, Food and Drug Administration, 7500 Standish Pl., Rockville, MD 20855. Send one self-addressed adhesive label to assist that office in processing your requests. See the **SUPPLEMENTARY INFORMATION** section for electronic access to the draft guidance document.

FOR FURTHER INFORMATION CONTACT: Karen Sussman, Center for Veterinary Medicine (HFV-114), Food and Drug Administration, 7500 Standish Pl., Rockville, MD 20855, 240-402-0876, karen.sussman@fda.hhs.gov.

SUPPLEMENTARY INFORMATION:

I. Background

FDA is announcing the availability of draft GFI #278 entitled “Human User Safety in New and Abbreviated New Animal Drug Applications.” This draft guidance is intended for sponsors interested in pursuing the approval, or conditional approval, of new animal drugs (including new generic animal drugs). This guidance addresses general principles of HUS assessment for new animal drugs, sources of data, mitigation strategies for proposed new animal drugs, potential recommendations to address HUS concerns, and how HUS information should be submitted to CVM.

This level 1 draft guidance is being issued consistent with FDA’s good guidance practices regulation (21 CFR

10.115). The draft guidance, when finalized, will represent the current thinking of FDA on “Human User Safety in New and Abbreviated New Animal Drug Applications.” It does not establish any rights for any person and is not binding on FDA or the public. You can use an alternative approach if it satisfies the requirements of the applicable statutes and regulations.

II. Paperwork Reduction Act of 1995

While this guidance contains no collection of information, it does refer to previously approved FDA collections of information. Therefore, clearance by the Office of Management and Budget (OMB) under the Paperwork Reduction Act of 1995 (PRA) (44 U.S.C. 3501–3521) is not required for this guidance. The previously approved collections of information are subject to review by OMB under the PRA. The collections of information in 21 CFR part 511 have been approved under OMB control number 0910–0117; in 21 CFR part 514 have been approved under OMB control numbers 0910–0032 and 0910–0284; in 21 CFR part 516 have been approved under OMB control numbers 0910–0605 and 0910–0620; and in section 512(n)(1) of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 360b(n)(1)) have been approved under OMB control number 0910–0669.

III. Electronic Access

Persons with access to the internet may obtain the draft guidance at <https://www.fda.gov/animal-veterinary/guidance-regulations/guidance-industry>, <https://www.fda.gov/regulatory-information/search-fda-guidance-documents>, or <https://www.regulations.gov>.

Dated: March 27, 2023.

Lauren K. Roth,

Associate Commissioner for Policy.

[FR Doc. 2023–07064 Filed 4–4–23; 8:45 am]

BILLING CODE 4164–01–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Health Resources and Services Administration

Agency Information Collection Activities: Submission to OMB for Review and Approval; Public Comment Request; The National Health Service Corps and Nurse Corps Interest Capture Form—Revision

AGENCY: Health Resources and Services Administration (HRSA), Department of Health and Human Services.

ACTION: Notice.

SUMMARY: In compliance with the Paperwork Reduction Act of 1995, HRSA submitted an Information Collection Request (ICR) to the Office of Management and Budget (OMB) for review and approval. Comments submitted during the first public review of this ICR will be provided to OMB. OMB will accept further comments from the public during the review and approval period. OMB may act on HRSA’s ICR only after the 30-day comment period for this notice has closed.

DATES: Comments on this ICR should be received no later than May 5, 2023.

ADDRESSES: Written comments and recommendations for the proposed information collection should be sent within 30 days of publication of this notice to www.reginfo.gov/public/do/PRAMain. Find this particular information collection by selecting “Currently under Review—Open for Public Comments” or by using the search function.

FOR FURTHER INFORMATION CONTACT: To request a copy of the clearance requests submitted to OMB for review, email Samantha Miller, the HRSA Information Collection Clearance Officer, at paperwork@hrsa.gov or call 301–594–4394.

SUPPLEMENTARY INFORMATION:

Information Collection Request Title: The National Health Service Corps and Nurse Corps Interest Capture Form OMB No. 0915–0337—Revision.

Abstract: The National Health Service Corps (NHSC) and the Nurse Corps Scholarship and Loan Repayment Programs of HRSA are both committed to improving the health of the nation’s underserved by uniting communities in need with caring health professionals and by supporting communities’ efforts to build better systems of care. The NHSC and Nurse Corps Interest Capture Form, which can be accessed on the HRSA website at <https://bhwh.hrsa.gov/about-us/ask-question>, is an optional form that a health profession student, licensed clinician, faculty member, clinical site administrator, or other interested individual can complete and submit to HRSA online. The purpose of the form is to enable individuals and clinical sites to ask questions about the NHSC and/or Nurse Corps Scholarship and Loan Repayment Programs, and to provide their contact information so that HRSA may provide them with periodic program updates and other general information via email. Completed forms

will contain information such as the names and roles of the individual(s), their phone number(s) and email address(es), and the HRSA program(s) in which they are interested or about which they have questions.

The revisions in this ICR are as follows:

a. The discontinuation of the print version of the NHSC and Nurse Corps Interest Capture Form, previously used by HRSA staff for sharing HRSA program information with health profession students and providers at national and regional conferences and campus recruiting events.

b. The addition of an online version of the NHSC and Nurse Corps Interest Capture Form, located on the HRSA website at <https://bhwh.hrsa.gov/about-us/ask-question>.

A 60-day notice published in the **Federal Register** on January 11, 2023, vol. 88, No. 7; pp. 1600–01. There were no public comments.

Need and Proposed Use of the Information: The need and purpose of this information collection is to share resources and information regarding the NHSC and Nurse Corps Scholarship and Loan Repayment Programs with interested HRSA website (<https://www.hrsa.gov/>) visitors.

Likely Respondents: Individuals and potential service sites interested in the NHSC or Nurse Corps Scholarship and Loan Repayment Programs.

Burden Statement: Burden in this context means the time expended by persons to generate, maintain, retain, disclose, or provide the information requested. This includes the time needed to review instructions; to develop, acquire, install, and utilize technology and systems for the purpose of collecting, validating, and verifying information, processing and maintaining information, and disclosing and providing information; to train personnel and to be able to respond to a collection of information; to search data sources; to complete and review the collection of information; and to transmit or otherwise disclose the information. The total annual burden hours estimated for this ICR are summarized in the table below.

TOTAL ESTIMATED ANNUALIZED BURDEN HOURS

Form name	Number of respondents	Number of responses per respondent	Total responses	Average burden per response (in hours)	Total burden hours
NHSC and Nurse Corps Interest Capture Form	16,144	1	16,144	.025	404
Total	16,144	16,144	404

Maria G. Button,

Director, Executive Secretariat.

[FR Doc. 2023-07045 Filed 4-4-23; 8:45 am]

BILLING CODE 4165-15-P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

[OMHA-2301-N]

Medicare Program; Administrative Law Judge Hearing Program for Medicare Claim and Entitlement Appeals; Quarterly Listing of Program Issuances—October Through December 2022

AGENCY: Office of Medicare Hearings and Appeals (OMHA), HHS.

ACTION: Notice.

SUMMARY: This quarterly notice lists the OMHA Case Processing Manual (OCPM) instructions that were published from October through December 2022. This manual standardizes the day-to-day procedures for carrying out adjudicative functions, in accordance with applicable statutes, regulations, and OMHA directives, and gives OMHA staff direction for processing appeals at the OMHA level of adjudication.

FOR FURTHER INFORMATION CONTACT: Jon Dorman, by telephone at (571) 457-7220, or by email at jon.dorman@hhs.gov.

SUPPLEMENTARY INFORMATION:

I. Background

The Office of Medicare Hearings and Appeals (OMHA), a staff division within the Office of the Secretary within the U.S. Department of Health and Human Services (HHS), administers the nationwide Administrative Law Judge hearing program for Medicare claim; organization, coverage, and at-risk determination; and entitlement appeals under sections 1869, 1155, 1876(c)(5)(B), 1852(g)(5), and 1860D-4(h) of the Social Security Act (the Act). OMHA ensures that Medicare beneficiaries and the providers and suppliers that furnish items or services to Medicare beneficiaries, as well as Medicare Advantage organizations (MAOs), Medicaid State agencies, and

applicable plans, have a fair and impartial forum to address disagreements with Medicare coverage and payment determinations made by Medicare contractors, MAOs, or Part D plan sponsors (PDPSs), and determinations related to Medicare eligibility and entitlement, Part B late enrollment penalty, and income-related monthly adjustment amounts (IRMAA) made by the Social Security Administration (SSA).

The Medicare claim, organization determination, coverage determination, and at-risk determination appeals processes consist of four levels of administrative review, and a fifth level of review with the Federal district courts after administrative remedies under HHS regulations have been exhausted. The first two levels of review are administered by the Centers for Medicare & Medicaid Services (CMS) and conducted by Medicare contractors for claim appeals, by MAOs and an Independent Review Entity (IRE) for Part C organization determination appeals, or by PDPSs and an IRE for Part D coverage determination and at-risk determination appeals. The third level of review is administered by OMHA and conducted by Administrative Law Judges and attorney adjudicators. The fourth level of review is administered by the HHS Departmental Appeals Board (DAB) and conducted by the Medicare Appeals Council (Council). In addition, OMHA and the DAB administer the second and third levels of appeal, respectively, for Medicare eligibility, entitlement, Part B late enrollment penalty, and IRMAA reconsiderations made by SSA; a fourth level of review with the Federal district courts is available after administrative remedies within SSA and HHS have been exhausted.

Sections 1869, 1155, 1876(c)(5)(B), 1852(g)(5), and 1860D-4(h) of the Act are implemented through the regulations at 42 CFR part 405 subparts I and J; part 417, subpart Q; part 422, subpart M; part 423, subparts M and U; and part 478, subpart B. As noted above, OMHA administers the nationwide Administrative Law Judge hearing program in accordance with these

statutes and applicable regulations. To help ensure nationwide consistency in that effort, OMHA established a manual, the OCPM. Through the OCPM, the OMHA Chief Administrative Law Judge establishes the day-to-day procedures for carrying out adjudicative functions, in accordance with applicable statutes, regulations, and OMHA directives. The OCPM provides direction for processing appeals at the OMHA level of adjudication for Medicare Part A and B claims; Part C organization determinations; Part D coverage determinations and at-risk determinations; and SSA eligibility and entitlement, Part B late enrollment penalty, and IRMAA determinations.

Section 1871(c) of the Act requires that the Secretary publish a list of all Medicare manual instructions, interpretive rules, statements of policy, and guidelines of general applicability not issued as regulations at least every three months in the **Federal Register**.

II. Format for the Quarterly Issuance Notices

This quarterly notice provides the specific updates to the OCPM that have occurred in the three-month period of October through December 2022. A hyperlink to the available chapters on the OMHA website is provided below. The OMHA website contains the most current, up-to-date chapters and revisions to chapters, and will be available earlier than we publish our quarterly notice. We believe the OMHA website provides more timely access to the current OCPM chapters for those involved in the Medicare claim; organization, coverage, and at-risk determination; and entitlement appeals processes. We also believe the website offers the public a more convenient tool for real time access to current OCPM provisions. In addition, OMHA has a listserv to which the public can subscribe to receive notification of certain updates to the OMHA website, including when new or revised OCPM chapters are posted. If accessing the OMHA website proves to be difficult, the contact person listed above can provide the information.

III. How To Use the Notice

This notice lists the OCPM chapters and subjects published during the quarter covered by the notice so the reader may determine whether any are of particular interest. The OCPM can be accessed at <https://www.hhs.gov/about/agencies/omha/the-appeals-process/case-processing-manual/index.html>.

IV. OCPM Releases for October Through December 2022

The OCPM is used by OMHA adjudicators and staff to administer the OMHA program. It offers day-to-day operating instructions, policies, and procedures based on statutes and regulations, and OMHA directives.

The following is a list and description of new OCPM provisions and the subject matter. This information is available on our website at <https://www.hhs.gov/about/agencies/omha/the-appeals-process/case-processing-manual/index.html>.

OCPM Chapter 12: Administrative Record and Exhibiting

On October 28, 2022, OMHA issued OCPM Chapter 12, which provides guidance on processing and developing the administrative record for OMHA appeals. OMHA is responsible for creating and organizing a complete record of the evidence and administrative proceedings of the appealed matter. This chapter explains how OMHA obtains the case file from the prior adjudicating entity, as well as how OMHA organizes and exhibits records, creates an index of the administrative record, and processes new evidence. The chapter also details how to document electronic and oral communications, ensure the record is complete, and address other record-related issues that could arise during the appeal process.

Karen Ames,

Executive Director of Operations, Office of Medicare Hearings and Appeals.

[FR Doc. 2023-06995 Filed 4-4-23; 8:45 am]

BILLING CODE 4150-46-P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Request for Nominations to the Advisory Council on Alzheimer's Research, Care, and Services

AGENCY: Office of the Assistant Secretary for Planning and Evaluation, Department of Health and Human Services.

ACTION: Notice.

SUMMARY: The Secretary of HHS established the Advisory Council on Alzheimer's Research, Care, and Services to provide advice and consultation to the Secretary on how to prevent or reduce the burden of Alzheimer's disease and related dementias on people with the disease and their caregivers. The Secretary signed the charter establishing the Advisory Council on May 23, 2011. *HHS is soliciting nominations for six (6) new non-federal members of the Advisory Council to replace the six (6) members whose terms will end September 30, 2023.* Nominations should include, at a minimum, the nominee's contact information (current mailing address, email address, and telephone number) and current curriculum vitae or resume.

DATES: Submit nominations by email or USPS mail before COB on April 28, 2023.

ADDRESSES: Nominations should be sent by email to: Helen Lamont, Ph.D., HHS Office of the Assistant Secretary for Planning and Evaluation, Room 424E, Humphrey Building, 200 Independence Avenue SW, Washington, DC 20201, helen.lamont@hhs.gov and napa@hhs.gov.

FOR FURTHER INFORMATION CONTACT: Helen Lamont (202) 260-6075, helen.lamont@hhs.gov.

SUPPLEMENTARY INFORMATION: The Advisory Council on Alzheimer's Research, Care, and Services meets quarterly to discuss programs that impact people with Alzheimer's disease and related dementias and their caregivers. The Advisory Council makes recommendations to Congress and the Secretary of Health and Human Services about ways to reduce the financial impact of Alzheimer's disease and related dementias and to improve the health outcomes of people with these conditions. The Advisory Council also provides feedback on a National Plan to Address Alzheimer's disease. On an annual basis, the Advisory Council evaluates the implementation of the recommendations through an updated National Plan. The National Alzheimer's Project Act, Public Law 111-375 (42 U.S.C. 11225), requires that the Secretary of Health and Human Services (HHS) establish the Advisory Council on Alzheimer's Research, Care, and Services. The Advisory Council is governed by provisions of Public Law 92-463 (5 U.S.C. Appendix 2), which sets forth standards for the formation and use of advisory committees.

The Advisory Council consists of 22 members. Ten members are designees

from Federal agencies including the Centers for Disease Control and Prevention, Administration for Community Living, Centers for Medicare & Medicaid Services, Indian Health Service, National Institutes of Health, National Science Foundation, Food and Drug Administration, Agency for Healthcare Research and Quality, Health Resources and Services Administration, and Department of Veterans Affairs. The Advisory Council also consists of 12 non-federal members selected by the Secretary who represent 6 categories of people impacted by dementia: dementia caregivers (2), health care providers (2), representatives of State or local health departments (2), researchers with dementia-related expertise in basic, translational, clinical, or drug development science (2), voluntary health association representatives (2), and dementia patient advocates (2), including one advocate who is currently living with dementia.

At this time, the Secretary of HHS is seeking nominations for new members for each category (caregiver, health care provider, state representative, researcher, association representative, dementia patient advocate currently living with Alzheimer's disease or a related dementia), to replace the members whose terms will end on September 30, 2023, for a total of six (6) new members to the Advisory Council. After receiving nominations, the Secretary, with input from his staff, will make the final decision, and the new members will be announced soon after. Members shall be invited to serve until the Advisory Council sunsets on December 31, 2025 or a 4-year term if the National Alzheimer's Project Act is reauthorized. Members will serve as Special Government Employees.

Dated: March 20, 2023.

Miranda Lynch-Smith,

Senior Official Performing the Duties of the Assistant Secretary for Planning and Evaluation.

[FR Doc. 2023-07007 Filed 4-4-23; 8:45 am]

BILLING CODE 4150-05-P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Solicitation of Nominations for Appointment to the Advisory Committee on Blood and Tissue Safety and Availability (ACBTSA)

AGENCY: Office of the Assistant Secretary for Health, Office of the Secretary, U.S. Department of Health and Human Services.

ACTION: Notice.

SUMMARY: The Office of the Assistant Secretary for Health (OASH) is seeking nominations for membership on the Advisory Committee on Blood and Tissue Safety and Availability (referred to as ACBTSA and/or the Committee). This announcement is to solicit nominations of qualified candidates to five public member positions on the ACBTSA. The ACBTSA is a federal advisory committee within the U.S. Department of Health and Human Services (HHS). Qualified individuals will be nominated to the Secretary of Health and Human Services for consideration of appointment as members of the ACBTSA. Members are invited to serve on the Committee for up to four-year terms. The Committee was established to provide advice to the Secretary on a range of policy issues related to blood, blood products, and tissues. The functions of the Committee are solely advisory in nature.

DATES: Nominations for membership on the ACBTSA must be received no later than 5:00 p.m. (ET), May 5, 2023. Packages received after this time will not be considered for the current membership cycle.

ADDRESSES: All nominations should be electronically mailed in one email to ACBTSA@hhs.gov. Please include in the subject line of the email: ACBTSA Application.

FOR FURTHER INFORMATION CONTACT: James Berger, Designated Federal Officer for the ACBTSA; Office of Infectious Disease and HIV/AIDS Policy, Office of the Assistant Secretary for Health, Department of Health and Human Services, Tower Building, 1101 Wootton Parkway, Rockville, MD 20852. Email: ACBTSA@hhs.gov. Phone: 202-795-7608. Additional information about ACBTSA can be obtained by accessing the Committee's website at <https://www.hhs.gov/oidp/advisory-committee/blood-tissue-safety-availability/index.html>.

SUPPLEMENTARY INFORMATION: ACBTSA is authorized under 42 U.S.C. 217a, section 222 of the Public Health Service (PHS) Act, as amended. The Committee is governed by the provisions of the Federal Advisory Committee Act (FACA), Public Law 92-463, as amended, which sets forth standards for the formation and use of advisory committees. The ACBTSA advises, assists, consults with, and makes policy recommendations to the Secretary, through the Assistant Secretary for Health, regarding broad responsibilities related to the safety of blood, blood products, tissues, and organs. For solid

organs and blood stem cells, the Committee's work is limited to policy issues related to donor derived infectious disease complications of transplantation.

The Advisory Committee consists of up to 29 members, including the voting and non-voting members and the Chair and Vice Chair or Co-Chairs. The Committee consists of not more than 23 voting members; 14 public members, including the Chair, and nine (9) individuals designated to serve as official representative members. The public members are selected from state and local organizations, patient advocacy groups, provider organizations, academic researchers, ethicists, physicians, surgeons, scientists, risk communication experts, consumer advocates, and from among communities of persons who are frequent recipients of blood or blood products or who have received tissues or organs. The nine individuals who are appointed as official representatives are selected to serve the interests of the blood, blood products, tissue and organ professional organizations or business sectors. The representative members are selected from the following groups: The AABB (formerly the American Association of Blood Banks); American Association of Tissue Banks; Eye Bank Association of America; Association of Organ Procurement Organizations; and one of either the American Red Cross or America's Blood Centers. The Committee composition can include additional representation from either the plasma protein fraction community or a trade organization; a manufacturer of blood, plasma, or other tissue/organ test kits; a manufacturer of blood, plasma or other tissue/organ equipment; a major hospital organization; or a major hospital accreditation organization.

All voting members are appointed by the Secretary or designee. Public voting members are classified as special government employees (SGEs) and are subject to government ethics rules. Pursuant to an advance written agreement, SGE voting members shall receive no stipend from the federal government for the services they perform during their tenure on the Committee. However, the SGE voting members are entitled to receive per diem and reimbursement for travel expenses incurred for attending meetings of the Advisory Committee.

Nominations

Nominations are being sought for individuals who have expertise and qualifications necessary to contribute to the accomplishment of the ACBTSA's objectives. The U.S. Department of

Health and Human Services policy stipulates that committee membership be balanced in terms of points of view represented and the committee's function. Appointments shall be made without discrimination on the basis of age, race, ethnicity, sexual orientation, gender identity, disability, veteran status, and cultural or religious status. In order to help ensure diverse groups and points of view are represented on the committee, nominees may provide this information when applying. Nominees must be U.S. citizens and cannot be full-time employees of the U.S. Government. Public members of the Committee are Special Government Employees (SGEs), requiring the filing of financial disclosure reports at the beginning and annually during their terms. Individuals who are selected for appointment will be required to provide detailed information regarding their financial interests and must receive annual ethics training. Candidates should submit the following items to be considered of appointment:

- Current curriculum vitae or resume, including complete contact information (telephone numbers, mailing address, email address).
- A letter of interest or personal statement from the nominee stating how their expertise would inform the work of ACBTSA (300 words or fewer).
- Nominees are invited to identify any or some of the following: race, ethnicity, sexual orientation, gender identity, disability, veteran status and cultural or religious status. This is not mandatory for a complete application.

Individuals can nominate themselves for consideration of appointment to the Committee. All nominations must include the required information in one email sent to ACBTSA@hhs.gov with the subject line, "ACBTSA Application." Incomplete nomination applications will not be processed for consideration.

Dated: March 13, 2023.

James J. Berger,

Senior Advisor for Blood and Tissue Policy, Designated Federal Officer, Advisory Committee on Blood and Tissue Safety and Availability, Office of the Assistant Secretary for Health, Department of Health and Human Services.

[FR Doc. 2023-07038 Filed 4-4-23; 8:45 am]

BILLING CODE 4150-41-P

DEPARTMENT OF HEALTH AND HUMAN SERVICES**National Institutes of Health****National Institute of Environmental Health Sciences; Notice of Closed Meeting**

Pursuant to section 10(d) of the Federal Advisory Committee Act, as amended, notice is hereby given of the following meeting.

The meeting will be closed to the public in accordance with the provisions set forth in sections 552b(c)(4) and 552b(c)(6), title 5 U.S.C., as amended. The grant applications and the discussions could disclose confidential trade secrets or commercial property such as patentable material, and personal information concerning individuals associated with the grant applications, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.

Name of Committee: National Institute of Environmental Health Sciences Special Emphasis Panel: R21 Mechanism for Time-Sensitive Research Opportunities in Environmental Health Sciences.

Date: April 20, 2023.

Time: 1:00 p.m. to 2:30 p.m.

Agenda: To review and evaluate grant applications.

Place: National Institute of Environmental Health Sciences, Keystone Building, 530 Davis Drive, Research Triangle Park, NC 27713 (Virtual Meeting).

Contact Person: Leroy Worth, Ph.D., Scientific Review Officer, Scientific Review Branch, Division of Extramural Research and Training, Nat. Institute of Environmental Health Sciences, P.O. Box 12233, MD EC-30/Room 3171, Research Triangle Park, NC 27709, 984-287-3340, worth@niehs.nih.gov.

This notice is being published less than 15 days prior to the meeting due to the timing limitations imposed by the review and funding cycle.

(Catalogue of Federal Domestic Assistance Program Nos. 93.115, Biometry and Risk Estimation—Health Risks from Environmental Exposures; 93.142, NIEHS Hazardous Waste Worker Health and Safety Training; 93.143, NIEHS Superfund Hazardous Substances—Basic Research and Education; 93.894, Resources and Manpower Development in the Environmental Health Sciences; 93.113, Biological Response to Environmental Health Hazards; 93.114, Applied Toxicological Research and Testing, National Institutes of Health, HHS)

Dated: March 30, 2023.

David W. Freeman,

Program Analyst, Office of Federal Advisory Committee Policy.

[FR Doc. 2023-07048 Filed 4-4-23; 8:45 am]

BILLING CODE 4140-01-P

DEPARTMENT OF HEALTH AND HUMAN SERVICES**Substance Abuse and Mental Health Services Administration****Meeting of the Substance Abuse and Mental Health Services Administration, Center for Substance Abuse Prevention National Advisory Council**

AGENCY: Substance Abuse and Mental Health Services Administration, HHS.

ACTION: Notice.

SUMMARY: Notice is hereby given for the meeting on April 25, 2023, of the Center for Substance Abuse Prevention National Advisory Council (CSAP NAC). The meeting is open to the public and can also be accessed virtually. Agenda with call-in information will be posted on the SAMHSA website prior to the meeting at: <https://www.samhsa.gov/about-us/advisory-councils/meetings>. The meeting will include, but not be limited to, remarks from the Assistant Secretary for Mental Health and Substance Use; approval of the meeting minutes of August 8, 2022; presentations on substance use prevention priorities and CSAP program developments; Council discussion and public comments.

DATES: March 25, 2023, 9:00 a.m. to approximately 4:00 p.m. EDT, Open.

ADDRESSES: 5600 Fishers Lane, Rockville, Maryland 20857 (Room 5N76).

FOR FURTHER INFORMATION CONTACT:

Michelle McVay, Designated Federal Official; Substance Abuse and Mental Health Service Administration, CSAP National Advisory Council, 5600 Fishers Lane, Rockville, Maryland 20857 (mail); telephone: (240) 276-0446; email: michelle.mcvay@samhsa.hhs.gov.

SUPPLEMENTARY INFORMATION: The CSAP NAC was established to advise the Secretary, Department of Health and Human Services (HHS), and the Assistant Secretary for Mental Health and Substance Use, SAMHSA; and the Director, CSAP, concerning matters relating to the activities carried out by and through the Center and the policies respecting such activities.

Interested persons may present data, information, or views orally or in writing, on issues pending before the Council. Written submissions must be forwarded to the contact person no later than 7 days before the meeting. Oral presentations from the public will be scheduled for the public comment section at the end of the council discussion. Individuals interested in

making oral presentations must notify the contact person by 1:00 p.m. (EDT), April 17, 2023. Up to three minutes will be allotted for each presentation, and as time permits, as these are presented in the order received. Public comments received will become part of the meeting records.

To obtain the call-in number, access code, and/or web access link; submit written or brief oral comments; or request special accommodations for persons with disabilities, please register on-line at: <https://snacregister.samhsa.gov>, or communicate with the contact person. Meeting information and a roster of Council members may be obtained either by accessing the CSAP Council's website at <https://www.samhsa.gov/about-us/advisory-councils>, or by contacting Michelle McVay.

Dated: March 30, 2023.

Carlos Castillo,

Committee Management Officer.

[FR Doc. 2023-07033 Filed 4-4-23; 8:45 am]

BILLING CODE 4162-20-P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2022-0058]

Homeland Security Academic Partnership Council

AGENCY: The Department of Homeland Security (DHS), Office of Partnership and Engagement (OPE).

ACTION: Notice of Charter amendment with modifications to the Council Name, Charter Scope of Activities, and Membership Composition.

SUMMARY: The Secretary of Homeland Security (Secretary) approved the Homeland Security Academic Advisory Council (HSAAC) name change to Homeland Security Academic Partnership Council (HSAPC, hereinafter "Council") to avoid confusion with the name of the Homeland Security Advisory Council (HSAC). The primary purpose of the Council is to provide organizationally independent, strategic, timely, specific, and actionable recommendations to the Secretary on key issues across the homeland security enterprise as they relate to the intersection of education and academia and the DHS mission.

The Council will consist of up to 30 members who are appointed by and serve at the pleasure of the Secretary of Homeland Security. All members are appointed as Representative members. The Secretary approved modifications to the categories and removal of the

numerical limitations to the categories to allow for increased flexibility across the broad categories of membership. The Council Representative members, as well as being diverse and an inclusive membership will represent one or more of the categories below:

- (a) Academic associations;
- (b) School safety, campus safety, public safety, or emergency management associations;
- (c) State, local or tribal law enforcement or related association;
- (d) President or Chancellor of a public or private:
 - Four-year college or university;
 - Two-year community college; or
 - Minority Serving Institution (MSIs);
- (e) Superintendent or comparable of a K–12 public school system;
- (f) President or CEO of an Education Employee Association or Education Employee Labor Organization; and/or
- (g) President or CEO of a private sector company, non-governmental organization, or civil society.

Appointments are made without regard to political affiliation. In order for DHS to fully leverage broad-ranging experience and education, the HSAPC must be diverse with regard to professional and technical expertise. DHS is committed to pursuing opportunities, consistent with applicable law, to compose a committee that reflects the diversity of the nation's people.

The Council is the sole advisory committee within DHS providing advice and recommendations on matters relating to the intersection of education and academia and the DHS mission.

The Council will operate in an advisory capacity only. The Council is necessary and in the public interest. This notice is provided in accordance with the Federal Advisory Committee Act, as amended, 5 U.S.C. App. The Council will terminate two years from the date of its establishment, unless renewed by the Secretary.

Revisions were made to the committee's objectives and scope of activities to encompass broader topics to align with the challenges facing the education and academic sectors. These broader topics allow the Secretary to receive recommendations on more facets of issues pertaining to these sectors. The committee's revised objectives and scope of activities provide for the committee to make recommendations that may relate to, but are not limited to:

- (a) DHS-wide funding opportunities, such as grants, scholarships, programs, and hiring surges;
- (b) Safety and security, including prevention, response, mitigation,

recovery, and other emergency management and preparedness measures;

(c) Improving coordination and sharing of threat and security related information including threats of violence, and targeted violence and terrorism prevention;

(d) Methods to develop career opportunities to support a 21st century DHS workforce; and

(e) Enhancing and expanding research opportunities, such as the DHS Science and Technology Centers of Excellence and DHS/National Security Agency joint Centers of Academic Excellence.

Finally, to allow for more external (non-Federal) voices, the revised charter removes DHS and Interagency members, which included "up to one representative" from six DHS offices/components and four federal agencies who served as non-voting ex officio members. Under the revised charter, the Secretary may invite participation from other federal Departments and Interagency members as necessary.

FOR FURTHER INFORMATION CONTACT: Z. Traci Silas at 202–447–3497, DHSacademic@hq.dhs.gov.

Zarinah Traci Silas,
Executive Director and Designated Federal Officer.

[FR Doc. 2023–07058 Filed 4–4–23; 8:45 am]

BILLING CODE 9112–FN–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA–2023–0010]

Agency Information Collection Activities: Sector Outreach and Programs Online Meeting Registration Tool

AGENCY: Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS).

ACTION: 60-Day notice and request for comments; revision, 1670–0019.

SUMMARY: The Infrastructure Security Division (ISD) within the Cybersecurity and Infrastructure Security Agency (CISA) will submit the following Information Collection Request (ICR) to the Office of Management and Budget (OMB) for review and clearance. This notice solicits comments on the information collection during a 60-day public comment period prior to the submission of this ICR to OMB. The submission proposes to renew the information collection for an additional three years and update the burden estimates associated with collecting

information for the purposes of registration for meetings and events.

DATES: Comments are due by June 5, 2023.

ADDRESSES: You may send comments, identified by docket number through the Federal eRulemaking Portal: <http://www.regulations.gov>. Follow the instructions for sending comments.

Instructions: All submissions must include the agency name 'CISA' and docket number CISA–2023–0010. Comments received will be posted without alteration at <http://www.regulations.gov>, including any personal information provided.

Comments that include protected information such as trade secrets, confidential commercial or financial information, Chemical-terrorism Vulnerability Information (CVI),¹ Sensitive Security Information (SSI),² or Protected Critical Infrastructure Information (PCII)³ should not be submitted to the public docket. Comments containing protected information should be appropriately marked and packaged in accordance with all applicable requirements and submission must be coordinated with the point of contact for this notice provided in the **FOR FURTHER INFORMATION CONTACT** section.

Docket: For access to the docket to read background documents or comments received, go to <http://www.regulations.gov>.

FOR FURTHER INFORMATION CONTACT: Dr. Ryan Donaghy, 703–603–5000, CISARegulations@cisa.dhs.gov.

SUPPLEMENTARY INFORMATION: The Critical Infrastructure Protection Act of 2001, 42 U.S.C. 5195c, states that any physical or virtual disruption of the operation of the critical infrastructures of the United States be rare, brief, geographically limited in effect, manageable, and minimally detrimental to the economy, human and government services, and national security of the United States; and that actions necessary to achieve the policy stated be carried out in a public-private partnership involving corporate and non-governmental organizations. On behalf of the DHS, the Cybersecurity and Infrastructure Security Agency's Infrastructure Security Division (CISA ISD) manages the Department's program

¹ For more information about CVI see 6 CFR 27.400 and the CVI Procedural Manual at www.dhs.gov/publication/safeguarding-cvi-manual.

² For more information about SSI see 49 CFR part 1520 and the SSI Program web page at www.tsa.gov/for-industry/sensitive-security-information.

³ For more information about PCII see 6 CFR part 29 and the PCII Program web page at www.dhs.gov/pcii-program.

to protect the Nation's 16 critical infrastructure sectors by implementing the National Infrastructure Protection Plan (NIPP) 2013, Partnering for Critical Infrastructure Security and Resilience. Pursuant to Presidential Policy Directive 21 on Critical Infrastructure Security and Resilience (February 2013), each sector is assigned a Sector-Specific Agency (SSA) to oversee Federal interaction with the array of sector security partners, both public and private. An SSA is responsible for leading a unified public-private sector effort to develop, coordinate, and implement a comprehensive physical, human, and cyber security strategy for its assigned sector. There are six critical infrastructure sectors assigned to CISA ISD, including the Chemical sector. In addition to fulfilling the regulatory obligations set forth by Congress, the CISA Office of Chemical Security coordinates with and builds sustainable partnerships with its public and private sector stakeholders to enable more effective coordination, information sharing, and program development and implementation. These partnerships are sustained through the NIPP Sector Partnership Model.⁴

Information sharing is a key component of the NIPP Partnership Model, and DHS sponsored conferences are one mechanism for information sharing. To facilitate conference planning and organization. This voluntary information collection tool for online event registration is maintained and leveraged by the Office of Chemical Security within CISA ISD. The information collected with this tool is used to register public and private sector stakeholders for meetings hosted by the Office of Chemical Security, principally the annual Chemical Security Summit. This tool is also used for private sector stakeholders to register their interest in being contacted by chemical security personnel regarding services provided under the voluntary ChemLock security program. The Office of Chemical Security uses the information collected to ensure that sufficient space and resources are available at meetings; to follow up with registrants when required; to develop meeting materials for attendees; and efficiently generate attendee and speaker nametags. Additionally, it enables the Office of Chemical Security to gain a better understanding of the organizations participating in chemical security events, and subsequently also identify which segments of the sector are underrepresented. This then allows

for the Office to target these underrepresented sector elements through outreach and awareness initiatives.

The changes to the collection include: changes to the burden costs, annual government costs, and revised and added data fields. Historically retained fields that collect redundant or unnecessary information have been removed and existing fields have been updated for accuracy and ease of use. Also, the following two fields have been added:

- 'How did you hear of this event,' a field which was included in the original instrument for this collection, and removed in a previous revision, has now been re-added to the instrument
- A field for the registrant's company website has been added

The annual burden cost for the collection has increased by \$5,751, from \$1,802 to \$7,553, largely due to an increase in the number of respondents associated with the shift to a hybrid event and updated compensation rates. Additionally, the scope of the collection has increased twofold: (1) the annual Chemical Security Summit, the event with which the calculations for this collection have been historically based, has moved to a hybrid format that allows for a dramatic increase in estimated registration numbers (from 400 previously to 1400), and (2) the utilization of this collection for the voluntary ChemLock program which adds an estimated 200 users per year. The annual government cost for the collection has increased by \$53,757, from \$8,347 to \$62,104, due to the shift to a hybrid event format and the associated increase in the number of registrations, which increased from 1,000 to 7,106.

This is a revision and renewal of an information collection.

OMB is particularly interested in comments that:

1. Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;
2. Evaluate the accuracy of the agency's estimate of the burden of the proposed collection of information,
3. including the validity of the methodology and assumptions used;
4. Enhance the quality, utility, and clarity of the information to be collected; and
5. Minimize the burden of the collection of information on those who are to respond, including through the

use of appropriate automated, electronic, mechanical, or other technological collection techniques or

6. Other forms of information technology, e.g., permitting electronic submissions of responses.

Analysis

Agency: Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS).

Title of Collection: Sector Outreach and Programs Online Meeting Registration Tool.

OMB Control Number: 1670-0019.

Frequency: Annually.

Affected Public: State, local, Tribal, and Territorial governments and private sector individuals.

Number of Annualized Respondents: 1,600.

Estimated Time per Respondent: 0.05 hours.

Total Annualized Burden Hours: 80 hours.

Total Annualized Respondent

Opportunity Cost: \$7,553.33.

Total Annualized Respondent Out-of-Pocket Cost: \$0.

Total Annualized Government Cost: \$62,103.77.

Robert J. Costello,

Chief Information Officer, Department of Homeland Security, Cybersecurity and Infrastructure Security Agency.

[FR Doc. 2023-07099 Filed 4-4-23; 8:45 am]

BILLING CODE 4410-10-P

DEPARTMENT OF HOMELAND SECURITY

U.S. Citizenship and Immigration Services

[OMB Control Number 1615-0045]

Agency Information Collection Activities; Revision of a Currently Approved Collection: Petition by Investor To Remove Conditions on Permanent Resident Status

AGENCY: U.S. Citizenship and Immigration Services, Department of Homeland Security.

ACTION: 30-Day notice.

SUMMARY: The Department of Homeland Security (DHS), U.S. Citizenship and Immigration Services (USCIS) will be submitting the following information collection request to the Office of Management and Budget (OMB) for review and clearance in accordance with the Paperwork Reduction Act of 1995. The purpose of this notice is to allow an additional 30 days for public comments.

⁴ NIPP 2013 Partnering for Critical Infrastructure Security and Resilience, pp 10-12.

DATES: Comments are encouraged and will be accepted until May 5, 2023.

ADDRESSES: Written comments and/or suggestions regarding the item(s) contained in this notice, especially regarding the estimated public burden and associated response time, must be submitted via the Federal eRulemaking Portal website at <http://www.regulations.gov> under e-Docket ID number USCIS-2006-0009. All submissions received must include the OMB Control Number 1615-0045 in the body of the letter, the agency name and Docket ID USCIS-2006-0009.

FOR FURTHER INFORMATION CONTACT: USCIS, Office of Policy and Strategy, Regulatory Coordination Division, Jerry Rigdon, Deputy Chief, Telephone number (240) 721-3000 (This is not a toll-free number; comments are not accepted via telephone message.). Please note contact information provided here is solely for questions regarding this notice. It is not for individual case status inquiries. Applicants seeking information about the status of their individual cases can check Case Status Online, available at the USCIS website at <http://www.uscis.gov>, or call the USCIS Contact Center at 800-375-5283 (TTY 800-767-1833).

SUPPLEMENTARY INFORMATION:

Comments

The information collection notice was previously published in the **Federal Register** on December 27, 2022 at 87 FR 79345, allowing for a 60-day public comment period. USCIS received two comments in connection with the 60-day notice.

You may access the information collection instrument with instructions, or additional information by visiting the Federal eRulemaking Portal site at: <http://www.regulations.gov> and enter USCIS-2006-0009 in the search box. The comments submitted to USCIS via this method are visible to the Office of Management and Budget and comply with the requirements of 5 CFR 1320.12(c). All submissions will be posted, without change, to the Federal eRulemaking Portal at <http://www.regulations.gov>, and will include any personal information you provide. Therefore, submitting this information makes it public. You may wish to consider limiting the amount of personal information that you provide in any voluntary submission you make to DHS. DHS may withhold information provided in comments from public viewing that it determines may impact the privacy of an individual or is offensive. For additional information, please read the Privacy Act notice that

is available via the link in the footer of <http://www.regulations.gov>.

Written comments and suggestions from the public and affected agencies should address one or more of the following four points:

(1) Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;

(2) Evaluate the accuracy of the agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used;

(3) Enhance the quality, utility, and clarity of the information to be collected; and

(4) Minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submission of responses.

Overview of This Information Collection

(1) *Type of Information Collection Request:* Revision of a currently approved collection.

(2) *Title of the Form/Collection:* Petition by Investor to Remove Conditions on Permanent Resident Status.

(3) *Agency form number, if any, and the applicable component of the DHS sponsoring the collection:* I-829; USCIS.

(4) *Affected public who will be asked or required to respond, as well as a brief abstract:* *Primary:* Individuals or households; business or other for-profit. This form is used by a conditional permanent resident who obtained such status through a qualifying investment to apply to remove conditions on their conditional residence.

(5) *An estimate of the total number of respondents and the amount of time estimated for an average respondent to respond:* The estimated total number of respondents for the information collection I-829 is 1,010 and the estimated hour burden per response is 3 hours and 48 minutes. The estimated total number of respondents for the information collection of Biometrics is 1,010 and the estimated hour burden per response is 1 hour and 10 minutes.

(6) *An estimate of the total public burden (in hours) associated with the collection:* The total estimated annual hour burden associated with this collection is 5,020 hours.

(7) *An estimate of the total public burden (in cost) associated with the collection:* The estimated total annual cost burden associated with this collection of information is \$437,330.

Dated: March 30, 2023.

Jerry L. Rigdon,

Deputy Chief, Regulatory Coordination Division, Office of Policy and Strategy, U.S. Citizenship and Immigration Services, Department of Homeland Security.

[FR Doc. 2023-07013 Filed 4-4-23; 8:45 am]

BILLING CODE 9111-97-P

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

[Docket No. FR-7070-N-18; OMB Control No. 2506-0165]

30-Day Notice of Proposed Information Collection: Disaster Recovery Grant Reporting System

AGENCY: Office of Policy Development and Research, Chief Data Officer, HUD.

ACTION: Notice.

SUMMARY: HUD is seeking approval from the Office of Management and Budget (OMB) for the information collection described below. In accordance with the Paperwork Reduction Act, HUD is requesting comment from all interested parties on the proposed collection of information. The purpose of this notice is to allow for an additional 30 days of public comment.

DATES: *Comments Due Date:* May 5, 2023.

ADDRESSES: Interested persons are invited to submit comments regarding this proposal. Written comments and recommendations for the proposed information collection should be sent within 30 days of publication of this notice to www.reginfo.gov/public/do/PRAMain. Find this particular information collection by selecting "Currently under 30-day Review—Open for Public Comments" or by using the search function.

FOR FURTHER INFORMATION CONTACT: Colette Pollard, Reports Management Officer, REE, Department of Housing and Urban Development, 451 7th Street SW, Washington, DC 20410; email PaperworkReductionActOffice@hud.gov or telephone 202-402-3400. This is not a toll-free number, HUD welcomes and is prepared to receive calls from individuals who are deaf or hard of hearing, as well as individuals with speech or communication disabilities. To learn more about how to make an accessible telephone call, please visit: <https://www.fcc.gov/consumers/guides/>

telecommunications-relay-service-trs. Copies of available documents submitted to OMB may be obtained from Ms. Pollard.

SUPPLEMENTARY INFORMATION: This notice informs the public that HUD is seeking approval from OMB for the information collection described in Section A.

The **Federal Register** notice that solicited public comment on the information collection for a period of 60 days was published on November 22, 2022 at 87 FR 71351.

A. Overview of Information Collection

Title of Information Collection:

Disaster Recovery Grant Reporting System (DRGR).

OMB Approval Number: 2506–0165.

Type of Request: Revision.

Form Number: SF–424 Application for Federal Assistance.

Description of the need for the information and proposed use: The Disaster Recovery Grant Reporting (DRGR) System is a grants management system used by the Office of Community Planning and Development to monitor special appropriation grants under the Community Development Block Grant program. This collection pertains to Community Development Block Grant Disaster Recovery (CDBG–DR), Community Development Block Grant Mitigation (CDBG–MIT), Community Development Block Grant National Disaster Resilience Competition (CDBG–NDR), Neighborhood Stabilization Program (NSP), Rural Capacity Building (RCB), Section 4, and Recovery Housing Program (RHP) grant funds.

The CDBG program is authorized under Title I of the Housing and Community Development Act of 1974, as amended. Following major disasters, Congress appropriates supplemental CDBG funds for disaster recovery. According to Section 104(e)(1) of the Housing and Community Development Act of 1974, HUD is responsible for reviewing grantees' compliance with applicable requirements and their continuing capacity to carry out their programs. Grant funds are made available to states and units of general local government, Indian tribes, and insular areas, unless provided otherwise by supplemental appropriations statute, based on their unmet disaster recovery needs.

The Neighborhood Stabilization Program (NSP) was established for the purpose of stabilizing communities that have suffered from foreclosures and property abandonment. Authorized under Section 1497 of the Wall Street Reform and Consumer Protection Act of 2010 (Pub. L. 111–203, approved July

21, 2010) (“NSP3”), NSP3 Technical Assistance (TA) provides \$20 million to organizations that are experienced and successful in providing program, technical, planning, financial, and organizational capacity building assistance, or consulting in such areas as community development, affordable housing, organizational management, financing and underwriting, construction and rehabilitation management, land banking, project management and strategic planning.

Through the funding of national organizations with expertise in rural housing and community development, the Rural Capacity Building (RCB) and Section 4 programs enhance the capacity and ability of local governments, Indian tribes, housing development organizations, rural Community Development Corporations (CDCs), and rural Community Housing Development Organizations (CHDOs), to carry out community development and affordable housing activities that benefit low-and moderate-income families and persons in rural areas.

The Recovery Housing Program (RHP) was authorized under section 8071 of the Support for Patients and Communities (SUPPORT) Act. HUD published its formula in the **Federal Register** on April 17, 2019 (84 FR 16027), identifying the 35 eligible grantees and allocation percentages. Section 8071 of the SUPPORT Act (Section 8071) required funds appropriated or made available for the RHP be treated as CDBG funds under title I of the Housing and Community Act of 1974, unless otherwise provided in Section 8071 or modified by waivers and alternative requirements.

Estimated Number of Respondents: 2,378.

Estimated Number of Responses: 46,150.

Frequency of Response: Varies.

Average Hours per Response: Varies.

Total Estimated Burdens: 59,890.50 hours.

B. Solicitation of Public Comment

This notice is soliciting comments from members of the public and affected parties concerning the collection of information described in Section A on the following:

(1) Whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;

(2) The accuracy of the agency's estimate of the burden of the proposed collection of information;

(3) Ways to enhance the quality, utility, and clarity of the information to be collected; and

(4) Ways to minimize the burden of the collection of information on those who are to respond; including through the use of appropriate automated collection techniques or other forms of information technology, *e.g.*, permitting electronic submission of responses.

(5) Ways to minimize the burden of the collection of information on those who are to respond, including the use of automated collection techniques or other forms of information technology.

HUD encourages interested parties to submit comments in response to these questions.

C. Authority

Section 3507 of the Paperwork Reduction Act of 1995, 44 U.S.C. Chapter 35.

Colette Pollard,

*Department Reports Management Officer,
Office of Policy Development and Research,
Chief Data Officer.*

[FR Doc. 2023–07076 Filed 4–4–23; 8:45 am]

BILLING CODE 4210–67–P

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

[Docket No. FR–7070–N–17; OMB Control No. 2506–0183]

30-Day Notice of Proposed Information Collection: Notice of Proposed Information Collection: Continuum of Care Homeless Assistance—Technical Submission

AGENCY: Office of Policy Development and Research, Chief Data Officer, HUD.

ACTION: Notice.

SUMMARY: HUD is seeking approval from the Office of Management and Budget (OMB) for the information collection described below. In accordance with the Paperwork Reduction Act, HUD is requesting comment from all interested parties on the proposed collection of information. The purpose of this notice is to allow for an additional 30 days of public comment.

DATES: *Comments due date:* May 5, 2023.

ADDRESSES: Interested persons are invited to submit comments regarding this proposal. Written comments and recommendations for the proposed information collection should be sent within 30 days of publication of this notice to *OIRA_submission@omb.eop.gov* or *www.reginfo.gov/public/do/PRAMain*. Find this particular information collection by selecting

“Currently under 30-day Review—Open for Public Comments” or by using the search function.

FOR FURTHER INFORMATION CONTACT: Colette Pollard, Reports Management Officer, REE, Department of Housing and Urban Development, 7th Street SW, Room 8210, Washington, DC 20410; email PaperworkReductionActOffice@hud.gov or telephone 202-402-3400. This is not a toll-free number. HUD welcomes and is prepared to receive calls from individuals who are deaf or hard of hearing, as well as individuals with speech or communication disabilities. To learn more about how to make an accessible telephone call, please visit <https://www.fcc.gov/consumers/guides/telecommunications-relay-service-trs>. Copies of available documents submitted to OMB may be obtained from Ms. Pollard.

SUPPLEMENTARY INFORMATION: This notice informs the public that HUD is seeking approval from OMB for the information collection described in Section A.

The **Federal Register** notice that solicited public comment on the information collection for a period of 60 days was published on February 6, 2023 at 88 FR 7750.

This Notice also lists the following information:

Title of Information Collection

OMB Approval Number: 2506-0183.
Type of Request: Extension of currently approved collection.
Form Number: HUD-40090-3a.
Description of the need for the information and proposed use: This submission is to request an extension of a currently approved collection for reporting burden associated with the Technical Submission phase of the Continuum of Care (CoC) Program Application. This submission is limited to the Technical Submission process under the CoC Program interim rule, as authorized by the HEARTH Act. Applicants who are successful in the CoC Program Competition are required to submit more detailed technical information before grant agreement. The information to be collected will be used to ensure that technical requirements are met prior to the execution of a grant agreement. The technical requirements relate to a more extensive description of the budgets for administration costs, timelines for project implementation, match documentation and other project specific documentation, and information to support the resolution of grant conditions. HUD will use this detailed information to determine if a project is financially feasible and whether all proposed activities are

eligible. All information collected is used to carefully consider conditional applicants for funding. If HUD collects less information, or collected it less frequently, the Department could not make a final determination concerning the eligibility of applicants for grant funds and conditional applicants would not be eligible to sign grant agreements and receive funding. To see the regulations for the CoC Program and applicable supplementary documents, visit HUD’s Homeless Resource Exchange page at <http://https://www.hudexchange.info/programs/coc/>. The statutory provisions and the implementing interim rule (also found at 24 CFR part 587) that govern the program require the information provided by the Technical Submission.

Respondents: Applicants that are successful in the Continuum of Care Homeless Assistance Grant competition.

Estimated Number of Respondents: 750.

Estimated Number of Responses: 750.

Frequency of Response: 1 time annually.

Average Hours per Response: 8.

Total Estimated Burdens: The total number of hours needed for all reporting is 126,000 hours.

Information collection	Number of respondents	Frequency of response	Responses per annum	Burden hour per response	Annual burden hours	Hourly cost per response	Annual cost
Exhibit 3 CoC Technical Submissions <i>e-snaps</i> Forms, formerly HUD-40090-3(a-b)	750	1	750	8	6,000	53.67	322,020
Submission Subtotal	750	1	750	8	6,000	53.67	322,020
Total Grant Program Application Collection
Total	750	1	750	8	6,000	53.67	322,020

B. Solicitation of Public Comment

This notice is soliciting comments from members of the public and affected parties concerning the collection of information described in Section A on the following:

- (1) Whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;
- (2) The accuracy of the agency’s estimate of the burden of the proposed collection of information;
- (3) Ways to enhance the quality, utility, and clarity of the information to be collected; and
- (4) Ways to minimize the burden of the collection of information on those who are to respond; including through the use of appropriate automated collection techniques or other forms of information technology, *e.g.*, permitting electronic submission of responses.

(5) ways to minimize the burden of the collection of information on those who are to respond, including the use of automated collection techniques or other forms of information technology.

HUD encourages interested parties to submit comment in response to these questions.

C. Authority

Section 3507 of the Paperwork Reduction Act of 1995, 44 U.S.C. Chapter 35.

Colette Pollard,

Department Reports Management Officer, Office of Policy Development and Research, Chief Data Officer.

[FR Doc. 2023-07077 Filed 4-4-23; 8:45 am]

BILLING CODE 4210-67-P

DEPARTMENT OF THE INTERIOR

Bureau of Land Management

[L13100000.PP0000.LLHQ310000.234; OMB Control No. 1004-0209]

Agency Information Collection Activities; Submission to the Office of Management and Budget for Review and Approval; Measurement of Oil

AGENCY: Bureau of Land Management, Interior.

ACTION: Notice of information collection; request for comment.

SUMMARY: In accordance with the Paperwork Reduction Act of 1995 (PRA), the Bureau of Land Management (BLM) proposes to renew an information collection.

DATES: Interested persons are invited to submit comments on or before May 5, 2023.

ADDRESSES: Written comments and recommendations for this information collection request (ICR) should be sent within 30 days of publication of this notice to www.reginfo.gov/public/do/PRAMain. Find this particular information collection by selecting “Currently under 30-day Review—Open for Public Comments” or by using the search function.

FOR FURTHER INFORMATION CONTACT: To request additional information about this ICR, contact Jennifer Spencer by email at j35spenc@blm.gov, or by telephone at (307) 775-6261. Individuals in the United States who are deaf, deafblind, hard of hearing, or have a speech disability may dial 711 (TTY, TDD, or TeleBraille) to access telecommunications relay services. Individuals outside the United States should use the relay services offered within their country to make international calls to the point-of-contact in the United States. You may also view the ICR at <https://www.reginfo.gov/public/do/PRAMain>.

SUPPLEMENTARY INFORMATION: In accordance with the PRA (44 U.S.C. 3501 *et seq.*) and 5 CFR 1320.8(d)(1), we invite the public and other Federal agencies to comment on new, proposed, revised and continuing collections of information. This helps the BLM assess impacts of its information collection requirements and minimize the public’s reporting burden. It also helps the public understand BLM information collection requirements and ensure requested data are provided in the desired format.

A Federal Register notice with a 60-day public comment period soliciting comments on this collection of information was published on November 15, 2022 (87 FR 68516). No comments were received in response to that notice.

As part of our continuing effort to reduce paperwork and respondent burdens, we are again inviting the public and other Federal agencies to comment on the proposed ICR described below. The BLM is especially interested in public comment addressing the following:

(1) Whether the collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility.

(2) The accuracy of our estimate of the burden for this collection of information, including the validity of the methodology and assumptions used.

(3) Ways to enhance the quality, utility, and clarity of the information to be collected; and

(4) How might the agency minimize the burden of the collection of information on those who are to respond, including the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, *e.g.*, permitting electronic submission of response.

Comments submitted in response to this notice are a matter of public record. Before including your address, phone number, email address, or other personal identifying information in your comment, you should be aware that your entire comment—including your personal identifying information—may be made publicly available at any time. While you can ask us in your comment to withhold your personal identifying information from public review, we cannot guarantee that we will be able to do so.

Abstract: This collection of information enables the BLM to ensure compliance with standards for the measurement of oil produced from Federal and Indian (except Osage Tribe) leases and compliance with pertinent statutes. This OMB Control Number is currently scheduled to expire on April 30, 2023. The BLM request that OMB renew this OMB Control Number for an additional three years.

Title of Collection: Measurement of Oil (43 CFR Subpart 3174).

OMB Control Number: 1004-0209.

Form Numbers: None.

Type of Review: Extension of a currently approved collection.

Respondents/Affected Public:

Businesses that participate in the production of oil from Federal and Indian (except Osage Tribe) leases.

Total Estimated Number of Annual Respondents: 11,742.

Total Estimated Number of Annual Responses: 11,742.

Estimated Completion Time per

Response: Varies from 6 minutes to 80 hours, depending on activity.

Total Estimated Number of Annual Burden Hours: 5,884.

Respondent’s Obligation: Required to obtain or retain a benefit.

Frequency of Collection: On occasion for all except the following information collection one-time activities pertaining to measurement equipment in use for the measurement of Federal or Indian fluid minerals:

- Documentation of Testing for Approval of a Coriolis Meter;
- Request to Use Alternate Oil Measurement System; and
- Testing of Alternate Oil Measurement System.

Total Estimated Annual Nonhour Burden Cost: \$5,580,305.

An agency may not conduct or sponsor and, notwithstanding any other provision of law, a person is not required to respond to a collection of information unless it displays a currently valid OMB control number.

The authority for this action is the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*).

Darrin King,

Information Collection Clearance Officer.

[FR Doc. 2023-06999 Filed 4-4-23; 8:45 am]

BILLING CODE 4310-84-P

DEPARTMENT OF THE INTERIOR

Bureau of Land Management

[BLM_MT_FRN_MO#4500169625]

Notice of Western Montana Resource Advisory Council Meeting

AGENCY: Bureau of Land Management, Interior.

ACTION: Notice of public meeting.

SUMMARY: In accordance with the Federal Land Policy and Management Act of 1976 and the Federal Advisory Committee Act of 1972, the U.S. Department of the Interior, Bureau of Land Management (BLM) Western Montana Resource Advisory Council (Council) will meet as follows.

DATES: The Council will hold an in-person meeting on Wednesday, April 26, 2023, in Butte, Montana. The meeting will start at 9 a.m. and conclude at 4 p.m. A virtual participation option will also be available.

ADDRESSES: The meeting will be held at the BLM Western Montana District Office, 101 N Parkmont, Butte, MT 59701. The meeting link, participation instructions, and final agenda will be made available to the public on the Council’s web page at <https://www.blm.gov/get-involved/resource-advisory-council/near-you/montana-dakotas/western-montana-rac>, and through personal contact at least 2 weeks prior to the meeting.

Written comments for the Council may be sent electronically in advance of the scheduled meeting to Public Affairs Specialist David Abrams at dabrams@blm.gov, or in writing to the BLM Western Montana District Office, Attention Public Affairs.

FOR FURTHER INFORMATION CONTACT: David Abrams, BLM Western Montana District Office, telephone: (406) 437-2562, email: dabrams@blm.gov. Individuals in the United States who are deaf, deafblind, hard of hearing, or have a speech disability may dial 711 (TTY,

TDD, or TeleBraille) to access telecommunications relay services for contacting Mr. Abrams. Individuals outside the United States should use the relay services offered within their country to make international calls to the point-of-contact in the United States.

SUPPLEMENTARY INFORMATION: The Council provides recommendations to the Secretary of the Interior concerning the planning and management of the public land resources located within the BLM's Western Montana District and offers advice on the implementation of the comprehensive, long-range plan for management, use, development, and protection of the public lands within the District. Agenda topics for the upcoming meetings include a discussion of RAC objectives and responsibilities; reports from the managers of the Butte, Dillon, and Missoula BLM Field Offices about activities in their areas; and other resource management issues the Council may raise.

All Council meetings are open to the public and a public comment period will be offered at 3:30 p.m. While the meeting is scheduled from 9 a.m. to 4 p.m., it may end earlier or later depending on the needs of group members. Therefore, members of the public interested in a specific agenda item or discussion should schedule their arrival accordingly. The BLM will provide a virtual participation option via Zoom. A link to the Zoom meeting will be posted on the RAC's web page 2 weeks in advance of the meeting. Individuals who want to participate virtually must register at least 1 week in advance of the meeting to allow the BLM to make appropriate accommodations.

Before including your address, phone number, email address, or other personal identifying information in your comment, you should be aware that your entire comment—including your personal identifying information—may be made publicly available at any time. While you can ask us in your comment to withhold your personal identifying information from public review, we cannot guarantee that we will be able to do so.

Meeting Accessibility/Special Accommodations: Please make requests in advance for sign language interpreter services, assistive listening devices, or other reasonable accommodations. We ask that you contact the person listed in the **FOR FURTHER INFORMATION CONTACT** section of this notice at least 7 business days prior to the meeting to give the Department of the Interior sufficient time to process your request. All

reasonable accommodation requests are managed on a case-by-case basis.

(Authority: 43 CFR 1784.4-2.)

Kathryn A. Stevens,

BLM Western Montana District Manager.

[FR Doc. 2023-07051 Filed 4-4-23; 8:45 am]

BILLING CODE 4331-20-P

DEPARTMENT OF THE INTERIOR

National Indian Gaming Commission

Renewals of Information Collections Under the Paperwork Reduction Act

AGENCY: National Indian Gaming Commission, Interior.

ACTION: Notice of request for comments.

SUMMARY: In compliance with the Paperwork Reduction Act of 1995, the National Indian Gaming Commission (NIGC or Commission) is seeking comments on the renewal of information collections. See **SUPPLEMENTARY INFORMATION** for the list of activities. These information collections expire on June 30, 2023 except for OMB Control Number 3141-0003, which expires on May 31, 2023.

DATES: Submit comments on or before June 5, 2023.

ADDRESSES: Comments can be mailed, faxed, or emailed to the attention of: Tim Osumi, National Indian Gaming Commission, 1849 C Street NW, MS 1621, Washington, DC 20240. Comments may be faxed to (202) 632-7066, and may be sent electronically to info@nigc.gov, subject: PRA renewals.

FOR FURTHER INFORMATION CONTACT: Tim Osumi at (202) 264-0676; fax (202) 632-7066 (not toll-free numbers).

SUPPLEMENTARY INFORMATION: We are seeking comments on the renewal of information collections for the following activities: (i) compliance and enforcement actions under the Indian Gaming Regulatory Act, as authorized by Office of Management and Budget (OMB) Control Number 3141-0001; (ii) approval of tribal ordinances, and background investigation and issuance of licenses, as authorized by OMB Control Number 3141-0003; (iii) National Environmental Policy Act submissions, as authorized by OMB Control Number 3141-0006; and (iv) issuance to tribes of certificates of self-regulation for Class II gaming, as authorized by OMB Control Number 3141-0008.

I. Request for Comments

You are invited to comment on these collections concerning: (i) whether the collections of information are necessary

for the proper performance of the functions of the agency, including whether the information will have practical utility; (ii) the accuracy of the agency's estimates of the burdens (including the hours and dollar costs) of the proposed collections of information, including the validity of the methodologies and assumptions used; (iii) ways to enhance the quality, utility, and clarity of the information to be collected; (iv) ways to minimize the burdens of the information collections on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other collection techniques or forms of information technology. Please note that an agency may not conduct or sponsor, and an individual need not respond to, a collection of information unless it has a valid OMB Control Number.

It is the Commission's policy to make all comments available to the public for review at the location listed in the **ADDRESSES** section. Before including your address, phone number, email address, or other personally identifiable information (PII) in your comment, you should be aware that your entire comment—including your PII—may be made publicly available at any time. While you may ask in your comment that the Commission withhold your PII from public review, the Commission cannot guarantee that it will be able to do so.

II. Data

Title: Indian Gaming Compliance and Enforcement.

OMB Control Number: 3141-0001.

Brief Description of Collection:

Although IGRA places primary responsibility with the tribes for regulating their gaming activities, 25 U.S.C. 2706(b) directs the Commission to monitor gaming conducted on Indian lands on a continuing basis. Amongst other actions necessary to carry out the Commission's statutory duties, the Act authorizes the Commission to access and inspect all papers, books, and records relating to gross revenues of a gaming operation. The Act also requires tribes to provide the Commission with annual independent audits of their gaming operations, including audits of all contracts in excess of \$25,000. 25 U.S.C. 2710(b)(2)(C), (D); 2710(d)(1)(A)(ii). The Act also authorizes the Commission to "promulgate such regulations and guidelines as it deems appropriate to implement" IGRA. 25 U.S.C. 2706(b)(10). Part 571 of title 25, Code of Federal Regulations, implements these statutory requirements.

Section 571.7(a) requires Indian gaming operations to keep/maintain permanent books of account and records sufficient to establish the amount of gross and net income, deductions and expenses, receipts and disbursements, and other relevant financial information. Section 571.7(c) requires that these records be kept for at least five years. Under § 571.7(b), the Commission may require a gaming operation to submit statements, reports, accountings, and specific records that will enable the NIGC to determine whether or not such operation is liable for fees payable to the Commission (and in what amount). Section 571.7(d) requires a gaming operation to keep copies of all enforcement actions that a tribe or a state has taken against the operation.

Section 571.12 requires tribes to prepare comparative financial statements covering all financial activities of each class II and class III gaming operation on the tribe's Indian lands, and to engage an independent certified public accountant to provide an annual audit of the financial statements of each gaming operation. Section 571.13 requires tribes to prepare and submit to the Commission two paper copies or one electronic copy of the financial statements and audits, together with management letter(s) and other documented auditor communications and/or reports as a result of the audit, setting forth the results of each fiscal year. The submission must be sent to the Commission within 120 days after the end of the fiscal year of each gaming operation, including when a gaming operation changes its fiscal year or when gaming ceases to operate. Section 571.14 requires tribes to reconcile quarterly fee reports with audited financial statements and to keep/maintain this information to be available to the NIGC upon request in order to facilitate the performance of compliance audits.

This information collection is mandatory and allows the Commission to fulfill its statutory responsibilities under IGRA to regulate gaming on Indian lands.

Respondents: Indian tribal gaming operations.

Estimated Number of Respondents: 720.

Estimated Annual Responses: 1,440.

Estimated Time per Response: Depending on the type of information collection, the range of time can vary from 4 burden hours to 476 burden hours for one item.

Frequency of Responses: Depending on the type of information collection, it can be quarterly or annually.

Estimated Total Annual Burden Hours on Respondents: 126,720.

Estimated Total Non-hour Cost Burden: \$38,376,960.

Title: Approval of Class II and Class III Ordinances, Background Investigations, and Gaming Licenses.

OMB Control Number: 3141-0003.

Brief Description of Collection: The Act sets standards for the regulation of gaming on Indian lands, including requirements for the approval or disapproval of tribal gaming ordinances. Specifically, § 2705(a)(3) requires the NIGC Chair to review all class II and class III tribal gaming ordinances. Section 2710 sets forth the specific requirements for the tribal gaming ordinances, including the requirement that there be adequate systems in place: to cause background investigations to be conducted on individuals in key employee and primary management official (PMO) positions (§ 2710(b)(2)(F)(i)); and to provide two prompt notifications to the Commission, including one containing the results of the background investigations before the issuance of any gaming licenses, and the other one of the issuance of such gaming licenses to key employees and PMOs (§ 2710(b)(2)(F)(ii)). In addition, § 2710(d)(2)(D)(ii) requires tribes who have, in their sole discretion, revoked any prior class III ordinance or resolution to submit a notice of such revocation to the NIGC Chair. The Act also authorizes the Commission to “promulgate such regulations and guidelines as it deems appropriate to implement” IGRA. 25 U.S.C.

2706(b)(10). Parts 519, 522, 556, and 558 of title 25, Code of Federal Regulations, implement these statutory requirements. Sections 519.1, 522.2(f) and 519.2 require a tribe, management contractor, and a tribal operator to designate an agent for service of process. Section 522.2(a) requires a tribe to submit a copy of an ordinance or resolution certified as authentic, and that meets the approval requirements in 25 CFR 522.5(b) or 522.7. Sections 522.11 and 522.12 require tribes to submit, respectively, an ordinance for the licensing of individually owned gaming operations other than those operating on September 1, 1986, and for the licensing of individually owned gaming operations operating on September 1, 1986. Section 522.3(a) requires a tribe to submit an amendment to an ordinance or resolution within 15 days after adoption of such amendment.

Section 522.2(b)–(h) requires tribes to submit to the Commission: (i) A copy of

the procedures to conduct or cause to be conducted background investigations on key employees and primary management officials and to ensure that key employees and primary management officials are notified of their rights under the Privacy Act; (ii) a copy of the procedures to issue tribal licenses to primary management officials and key employees; (iii) When an ordinance or resolution concerns class III gaming, a copy of any approved tribal-state compact or class III procedures as prescribed by the Secretary that are in effect at the time the ordinance or amendment is passed; (iv) A copy of the procedures for resolving disputes between the gaming public and the tribe or the management contractor; (v) Identification of the entity that will take fingerprints and a copy of the procedures for conducting a criminal history check. Such a criminal history check shall include a check of criminal history records information maintained by the Federal Bureau of Investigation; and (vi) Indian lands or tribal gaming regulations or environmental and public health and safety documentation that the Chair may request in the Chair's discretion. Section 522.3(a) requires a tribe to submit any amendment to these submissions within 15 days after adoption of such amendment. Section 522.13(a) requires a tribe to submit to the Commission a copy of an authentic ordinance revocation or resolution.

Section 556.4 requires tribes to mandate the submission of the following information from applicants for key employee and PMO positions: (i) full name, other names used (oral or written), social security number(s), birth date, place of birth, citizenship, gender, all languages (spoken or written); (ii) currently and for the previous five years: Business and employment positions held, ownership interests in those businesses, business and residence addresses, and driver's license numbers; (iii) the names and current addresses of at least three personal references; (iv) current business and personal telephone numbers; (v) a description of any existing and previous business relationships with Indian tribes, including ownership interests in those businesses; (vi) a description of any existing and previous business relationships with the gaming industry generally, including ownership interests in those businesses; (vii) the name and address of any licensing or regulatory agency with which the person has filed an application for a license or permit related to gaming, whether or not such license or permit was granted; (viii) for

each felony for which there is an ongoing prosecution or a conviction, the charge, the name and address of the court involved, and the date and disposition if any; (ix) for each misdemeanor conviction or ongoing misdemeanor prosecution (excluding minor traffic violations) within 10 years of the date of the application, the name and address of the court involved and the date and disposition; (x) for each criminal charge in the past 10 years that is not otherwise listed, the criminal charge, the name and address of the court, and the date and disposition; (xi) the name and address of any licensing or regulatory agency with which the person has filed an application for an occupational license or permit, whether or not such license or permit was granted; (xii) a photograph; and (xiii) fingerprints. Sections 556.2 and 556.3, respectively, require tribes to place a specific Privacy Act notice on their key employee and PMO applications, and to warn applicants regarding the penalty for false statements by also placing a specific false statement notice on their applications.

Sections 556.6(a) and 558.3(e) require tribes to keep/maintain the individuals' complete application files, investigative reports, and eligibility determinations during their employment and for at least three years after termination of their employment. Section 556.6(b)(1) requires tribes to create and maintain an investigative report on each background investigation that includes: (i) the steps taken in conducting a background investigation; (ii) the results obtained; (iii) the conclusions reached; and (iv) the basis for those conclusions. Section 556.6(b)(2) requires tribes to submit, no later than 60 days after an applicant begins work, a notice of results of the applicant's background investigation that includes: (i) the applicant's name, date of birth, and Social Security number; (ii) the date on which the applicant began or will begin work as a key employee or PMO; (iii) a summary of the information presented in the investigative report; and (iv) a copy of the eligibility determination.

Section 558.3(b) requires a tribe to notify the Commission of the issuance of PMO and key employee licenses within 30 days after such issuance. Section 558.3(d) requires a tribe to notify the Commission if the tribe does not issue a license to an applicant, and requires it to forward copies of its eligibility determination and notice of results to the Commission for inclusion in the Indian Gaming Individuals Record System. Section 558.4(e) requires a tribe, after a gaming license revocation hearing, to notify the

Commission of its decision to revoke or reinstate a gaming license within 45 days of receiving notification from the Commission that a specific individual in a PMO or key employee position is not eligible for continued employment.

These information collections are mandatory and allow the Commission to carry out its statutory duties.

Respondents: Indian tribal gaming operations.

Estimated Number of Respondents: 1,524.

Estimated Annual Responses: 225,484.

Estimated Time per Response: Depending on the type of information collection, the range of time can vary from 0.7 burden hour to 23 burden hours for one item.

Frequency of Response: Varies.

Estimated Total Annual Burden Hours on Respondents: 489,089.

Estimated Total Non-hour Cost Burden: \$3,264,177.

Title: NEPA Compliance.

OMB Control Number: 3141-0006.

Brief Description of Collection: The National Environmental Policy Act (NEPA), 42 U.S.C. 4321, *et seq.*, and the Council on Environmental Quality's (CEQ) implementing regulations, require federal agencies to prepare (or cause to be prepared) environmental documents for agency actions that may have a significant impact on the environment. Under NEPA, an Environmental Assessment (EA) must be prepared when the agency action cannot be categorically excluded, or the environmental consequences of the agency action will not result in a significant impact or the environmental impacts are unclear and need to be further defined. An Environmental Impact Statement (EIS) must be prepared when the agency action will likely result in significant impacts to the environment.

Amongst other actions necessary to carry out the Commission's statutory duties, the Act requires the NIGC Chair to review and approve third-party management contracts that involve the operation of tribal gaming facilities. 25 U.S.C. 2711. The Commission has taken the position that the NEPA process is triggered when a tribe and a potential contractor seek approval of a management contract. Normally, an EA or EIS and its supporting documents are prepared by an environmental consulting firm and submitted to the Commission by the tribe. In the case of an EA, the Commission independently evaluates the NEPA document, verifies its content, and assumes responsibility for the accuracy of the information contained therein. In the case of an EIS,

the Commission directs and is responsible for the preparation of the NEPA document, but the tribe or potential contractor is responsible for paying for the preparation of the document. The information collected includes, but is not limited to, maps, charts, technical studies, correspondence from other agencies (federal, tribal, state, and local), and comments from the public. These information collections are mandatory and allow the Commission to carry out its statutory duties.

Respondents: Tribal governing bodies, management companies.

Estimated Number of Respondents: 3.

Estimated Annual Responses: 3.

Estimated Time per Response:

Depending on whether the response is an EA or an EIS, the range of time can vary from 2 burden hours to 16.0 burden hours for one item.

Frequency of Response: Varies.

Estimated Total Annual Burden

Hours on Respondents: 20.5.

Estimated Total Non-hour Cost Burden: \$494,132.

Title: Issuance of Certificates of Self-Regulation to Tribes for Class II Gaming.

OMB Control Number: 3141-0008.

Brief Description of Collection: The Act sets the standards for the regulation of Indian gaming, including a framework for the issuance of certificates of self-regulation for class II gaming operations to tribes that meet certain qualifications. Specifically, 25 U.S.C. 2710(c) authorizes the Commission to issue a certificate of self-regulation if it determines that a tribe has: (i) conducted its gaming activity in a manner that has resulted in an effective and honest accounting of all revenues and a reputation for safe, fair, and honest operation of the activity, and has been generally free of evidence of criminal or dishonest activity; (ii) conducted its gaming operation on a fiscally and economically sound basis; (iii) conducted its gaming activity in compliance with the IGRA, NIGC regulations and the tribe's gaming ordinance and gaming regulations; (iv) adopted and is implementing adequate systems for the accounting of all revenues from the gaming activity, for the investigation, licensing, and monitoring of all employees of the gaming activity, for the investigation, enforcement, and prosecution of violations of its gaming ordinance and regulations, and for the prosecution of criminal or dishonest activity or referring of such activity for prosecution. The Act also authorizes the Commission to "promulgate such regulations and guidelines as it deems appropriate to implement" IGRA. 25

U.S.C. 2706(b)(10). Part 518 of title 25, Code of Federal Regulations, implements these statutory requirements.

Section 518.3(e) requires a tribe's gaming operation(s) and the tribal regulatory body (TRB) to have kept all records needed to support the petition for self-regulation for the three years immediately preceding the date of the petition submission. Section 518.4 requires a tribe petitioning for a certificate of self-regulation to submit the following to the Commission, accompanied by supporting documentation: (i) two copies of a petition for self-regulation approved by the tribal governing body and certified as authentic; (ii) a description of how the tribe meets the eligibility criteria in § 518.3; (iii) a brief history of each gaming operation, including the opening dates and periods of voluntary or involuntary closure(s); (iv) a TRB organizational chart; (v) a brief description of the criteria that individuals must meet before being eligible for employment as a tribal regulator; (vi) a brief description of the process by which the TRB is funded, and the funding level for the three years immediately preceding the date of the petition; (vii) a list of the current regulators and TRB employees, their complete resumes, their titles, the dates that they began employment, and if serving limited terms, the expiration date of such terms; (viii) a brief description of the accounting system(s) at the gaming operation that tracks the flow of the gaming revenues; (ix) a list of the gaming activity internal controls at the gaming operation(s); (x) a description of the recordkeeping system(s) for all investigations, enforcement actions, and prosecutions of violations of the tribal gaming ordinance or regulations, for the three-year period immediately preceding the date of the petition; and (xi) the tribe's current set of gaming regulations, if not included in the approved tribal gaming ordinance. Section 518.10 requires each Indian gaming tribe that has been issued a certificate of self-regulation to submit to the Commission the following information by April 15th of each year following the first year of self-regulation, or within 120 days after the end of each gaming operation's fiscal year: (i) an annual independent audit; and (ii) a complete resume for all TRB employees hired and licensed by the tribe subsequent to its receipt of a certificate of self-regulation.

Submission of the petition and supporting documentation is voluntary. Once a certificate of self-regulation has

been issued, the submission of certain other information is mandatory.

Respondents: Tribal governments.

Estimated Number of Respondents: 11.

Estimated Annual Responses: 11.

Estimated Time per Response:

Depending on the information collection, the range of time can vary from 1 burden hour to 202 burden hours for one item.

Frequency of Responses: Annually.

Estimated Total Annual Burden

Hours on Respondents: 257.

Estimated Total Non-hour Cost Burden: \$203,825.

Dated: March 22, 2023.

Christinia Thomas,

Deputy Chief of Staff.

[FR Doc. 2023-06288 Filed 4-4-23; 8:45 am]

BILLING CODE 7565-01-P

DEPARTMENT OF THE INTERIOR

National Park Service

**[NPS-WASO-NRNL-DTS#-35601;
PPWOCRADIO, PCU00RP14.R50000]**

National Register of Historic Places; Notification of Pending Nominations and Related Actions

AGENCY: National Park Service, Interior.

ACTION: Notice.

SUMMARY: The National Park Service is soliciting electronic comments on the significance of properties nominated before March 25, 2023, for listing or related actions in the National Register of Historic Places.

DATES: Comments should be submitted electronically by April 20, 2023.

ADDRESSES: Comments are encouraged to be submitted electronically to *National Register Submissions@nps.gov* with the subject line "Public Comment on <property or proposed district name, (County) State>." If you have no access to email, you may send them via U.S. Postal Service and all other carriers to the National Register of Historic Places, National Park Service, 1849 C Street NW, MS 7228, Washington, DC 20240.

FOR FURTHER INFORMATION CONTACT: Sherry A. Frear, Chief, National Register of Historic Places/National Historic Landmarks Program, 1849 C Street NW, MS 7228, Washington, DC 20240, *sherry_frear@nps.gov*, 202-913-3763.

SUPPLEMENTARY INFORMATION: The properties listed in this notice are being considered for listing or related actions in the National Register of Historic Places. Nominations for their consideration were received by the

National Park Service before March 25, 2023. Pursuant to Section 60.13 of 36 CFR part 60, comments are being accepted concerning the significance of the nominated properties under the National Register criteria for evaluation.

Before including your address, phone number, email address, or other personal identifying information in your comment, you should be aware that your entire comment—including your personal identifying information—may be made publicly available at any time. While you can ask us in your comment to withhold your personal identifying information from public review, we cannot guarantee that we will be able to do so.

Nominations submitted by State or Tribal Historic Preservation Officers

Key: State, County, Property Name, Multiple Name (if applicable), Address/Boundary, City, Vicinity, Reference Number.

ARIZONA

Maricopa County

Connor-Harold House, 5729 North Palo Cristi Rd., Paradise Valley, SG100008908
Ainsworth, Eliza and Charles, House, 9 East Country Club Dr., Phoenix, SG100008909

CALIFORNIA

Orange County

ELECTRA (motor yacht), 16591 Ensign Ct., Huntington Beach, SG100008894

COLORADO

Denver County

655 Broadway Building, Address Restricted, Denver vicinity, SG100008903

MINNESOTA

Hennepin County

Hiawatha Golf Course, 4553 Longfellow Ave., Minneapolis, SG100008905

NEW YORK

Dutchess County

Tioronda Estate-Craig House Historic District, 7 Craig House Ln., 21 Grandview Ave., 636 and 644 Wolcott Ave., Beacon vicinity, SG100008896

Monroe County

Todd Union, 415 Alumni Rd., Rochester, SG100008906

Tompkins County

Stewart Park, 1 James L. Gibbs Dr., Ithaca, SG100008895

Westchester County

Westminster Presbyterian Church, 76 Warburton Ave., Yonkers, SG100008899

OHIO

Franklin County

Ohio Historical Center and Ohio Village, 800 East 17th Ave., Columbus, SG100008897

PENNSYLVANIA**Northampton County**

Walnut Street Bridge, 200 ft. west of the intersection of Walnut St. and the Saucon Valley Rail Tr., Hellertown, SG100008901

VIRGINIA**Charlotte County**

Keysville Historic District, King and Church Sts., Railroad Ave., and others, Keysville, SG100008902

WISCONSIN**Milwaukee County**

North Milwaukee High School, 5372 North 37th St., Milwaukee, SG100008907

Additional documentation has been received for the following resources:

ARIZONA**Maricopa County**

Portland Street Historic District (Additional Documentation) (Roosevelt Neighborhood MRA), Portland St. between 3rd and 7th Aves., Phoenix, AD83003491

Pima County

Blenman-Elm Historic District (Additional Documentation), 2350 East Elm St., Tucson, AD03000318

VIRGINIA**Hanover County**

Little River UDC Jefferson Davis Highway Marker (Additional Documentation) (UDC Commemorative Highway Markers along the Jefferson Davis Highway in Virginia MPS), 15400 Washington Hwy., Doswell vicinity, AD100002355

Authority: Section 60.13 of 36 CFR part 60.

Dated: March 29, 2023.

Lisa P. Davidson,

Program Manager, National Historic Landmarks.

[FR Doc. 2023-07111 Filed 4-4-23; 8:45 am]

BILLING CODE 4312-52-P

INTERNATIONAL TRADE COMMISSION

[Investigation No. 731-TA-683 (Fifth Review)]

Fresh Garlic From China; Scheduling of an Expedited Five-Year Review

AGENCY: United States International Trade Commission.

ACTION: Notice.

SUMMARY: The Commission hereby gives notice of the scheduling of an expedited review pursuant to the Tariff Act of 1930 (“the Act”) to determine whether revocation of the antidumping duty order on fresh garlic from China would be likely to lead to continuation or

recurrence of material injury within a reasonably foreseeable time.

DATES: January 6, 2023.

FOR FURTHER INFORMATION CONTACT: Charles Cummings (202-708-1666), Office of Investigations, U.S. International Trade Commission, 500 E Street SW, Washington, DC 20436. Hearing-impaired persons can obtain information on this matter by contacting the Commission’s TDD terminal on 202-205-1810. Persons with mobility impairments who will need special assistance in gaining access to the Commission should contact the Office of the Secretary at 202-205-2000. General information concerning the Commission may also be obtained by accessing its internet server (<https://www.usitc.gov>). The public record for this proceeding may be viewed on the Commission’s electronic docket (EDIS) at <https://edis.usitc.gov>.

SUPPLEMENTARY INFORMATION:

Background.—On January 6, 2023, the Commission determined that the domestic interested party group response to its notice of institution (87 FR 59824, October 3, 2022) of the subject five-year review was adequate and that the respondent interested party group response was inadequate. The Commission did not find any other circumstances that would warrant conducting a full review.¹ Accordingly, the Commission determined that it would conduct an expedited review pursuant to section 751(c)(3) of the Tariff Act of 1930 (19 U.S.C. 1675(c)(3)).²

For further information concerning the conduct of this review and rules of general application, consult the Commission’s Rules of Practice and Procedure, part 201, subparts A and B (19 CFR part 201), and part 207, subparts A, D, E, and F (19 CFR part 207).

Staff report.—A staff report containing information concerning the subject matter of the review has been placed in the nonpublic record, and will be made available to persons on the Administrative Protective Order service list for this review on April 12, 2023. A public version will be issued thereafter, pursuant to § 207.62(d)(4) of the Commission’s rules.

Written submissions.—As provided in § 207.62(d) of the Commission’s rules,

interested parties that are parties to the review and that have provided individually adequate responses to the notice of institution,³ and any party other than an interested party to the review may file written comments with the Secretary on what determination the Commission should reach in the review. Comments are due on or before April 20, 2023, and may not contain new factual information. Any person that is neither a party to the five-year review nor an interested party may submit a brief written statement (which shall not contain any new factual information) pertinent to the review by April 20, 2023. However, should the Department of Commerce (“Commerce”) extend the time limit for its completion of the final results of its review, the deadline for comments (which may not contain new factual information) on Commerce’s final results is three business days after the issuance of Commerce’s results. If comments contain business proprietary information (BPI), they must conform with the requirements of §§ 201.6, 207.3, and 207.7 of the Commission’s rules. The Commission’s *Handbook on Filing Procedures*, available on the Commission’s website at https://www.usitc.gov/documents/handbook_on_filing_procedures.pdf, elaborates upon the Commission’s procedures with respect to filings.

In accordance with §§ 201.16(c) and 207.3 of the rules, each document filed by a party to the review must be served on all other parties to the review (as identified by either the public or BPI service list), and a certificate of service must be timely filed. The Secretary will not accept a document for filing without a certificate of service.

Determination.—The Commission has determined this review is extraordinarily complicated and therefore has determined to exercise its authority to extend the review period by up to 90 days pursuant to 19 U.S.C. 1675(c)(5)(B).

Authority: This review is being conducted under authority of title VII of the Tariff Act of 1930; this notice is published pursuant to § 207.62 of the Commission’s rules.

By the order of the Commission.

¹ A record of the Commissioners’ votes, the Commission’s statement on adequacy, and any individual Commissioner’s statements will be available from the Office of the Secretary and at the Commission’s website.

² Chairman David S. Johanson determined that, in light of the time that has transpired since the Commission last conducted a full review of this order, conducting a full review was warranted.

³ The Commission has found the responses submitted on behalf of the Fresh Garlic Producers Association (“FGPA”) and its individual members Christopher Ranch L.L.C., The Garlic Company, and Valley Garlic, Inc., to be individually adequate. Comments from other interested parties will not be accepted (*see* 19 CFR 207.62(d)(2)).

Issued: March 30, 2023.

Lisa Barton,

Secretary to the Commission.

[FR Doc. 2023-07023 Filed 4-4-23; 8:45 am]

BILLING CODE 7020-02-P

INTERNATIONAL TRADE COMMISSION

[Investigation Nos. 731-TA-1588-1590 (Final)]

Certain Preserved Mushrooms From the Netherlands, Poland, and Spain; Supplemental Schedule for the Final Phase of Anti-Dumping Duty Investigations

AGENCY: United States International Trade Commission.

ACTION: Notice.

DATES: March 27, 2023.

FOR FURTHER INFORMATION CONTACT:

Kristina Lara ((202) 205-3386), Office of Investigations, U.S. International Trade Commission, 500 E Street SW, Washington, DC 20436. Hearing-impaired persons can obtain information on this matter by contacting the Commission's TDD terminal on 202-205-1810. Persons with mobility impairments who will need special assistance in gaining access to the Commission should contact the Office of the Secretary at 202-205-2000. General information concerning the Commission may also be obtained by accessing its internet server (<https://www.usitc.gov>). The public record for these investigations may be viewed on the Commission's electronic docket (EDIS) at <https://edis.usitc.gov>.

SUPPLEMENTARY INFORMATION: Effective September 15, 2022, the Commission established a general schedule for the conduct of the final phase of its antidumping duty investigations on certain preserved mushrooms from France, the Netherlands, Poland, and Spain (87 FR 57717, September 21, 2022), following a preliminary determination by the U.S. Department of Commerce ("Commerce") that imports of certain preserved mushrooms from France were being sold at less than fair value ("LTFV") (87 FR 55997, September 13, 2022). Notice of the scheduling of the final phase of the Commission's investigations and of a public hearing held in connection therewith was given by posting copies of the notice in the Office of the Secretary, U.S. International Trade Commission, Washington, DC, and by publishing the notice in the **Federal Register** on September 21, 2022 (87 FR 57717). The Commission conducted its

hearing on November 17, 2022. All persons who requested the opportunity were permitted to participate.

Commerce issued a final affirmative antidumping duty determination with respect to certain preserved mushrooms from France (87 FR 72963, November 28, 2022). The Commission subsequently issued its final determination that an industry in the United States was materially injured by reason of imports of certain preserved mushrooms from France provided for in subheading 2003.10.01 of the Harmonized Tariff Schedule of the United States ("HTSUS") (88 FR 2971, January 18, 2023).

Commerce issued final affirmative antidumping duty determinations with respect to imports of certain preserved mushrooms from the Netherlands, Poland, and Spain (88 FR 18115, 88 FR 18118, and 88 FR 18120, March 27, 2023). Accordingly, the Commission currently is issuing a supplemental schedule for its antidumping duty investigations on imports of certain preserved mushrooms from the Netherlands, Poland, and Spain.

This supplemental schedule is as follows: the deadline for filing supplemental party comments on Commerce's final antidumping duty determinations is April 7, 2023. Supplemental party comments may address only Commerce's final antidumping duty determinations regarding imports of certain preserved mushrooms from the Netherlands, Poland, and Spain. These supplemental final comments may not contain new factual information and may not exceed five (5) pages in length. The supplemental staff report in the final phase of the current investigations will be placed in the nonpublic record on April 20, and a public version will be issued thereafter.

For further information concerning this proceeding see the Commission's notices cited above and the Commission's Rules of Practice and Procedure, part 201, subparts A and B (19 CFR part 201), and part 207, subparts A and C (19 CFR part 207).

Additional written submissions to the Commission, including requests pursuant to section 201.12 of the Commission's rules, shall not be accepted unless good cause is shown for accepting such submissions, or unless the submission is pursuant to a specific request by a Commissioner or Commission staff.

In accordance with sections 201.16(c) and 207.3 of the Commission's rules, each document filed by a party to the investigations must be served on all other parties to the investigations (as

identified by either the public or BPI service list), and a certificate of service must be timely filed. The Secretary will not accept a document for filing without a certificate of service.

Please note the Secretary's Office will accept only electronic filings during this time. Filings must be made through the Commission's Electronic Document Information System (EDIS, <https://edis.usitc.gov>.) No in-person paper-based filings or paper copies of any electronic filings will be accepted until further notice.

Authority: This proceeding is being conducted under authority of title VII of the Tariff Act of 1930; this notice is published pursuant to section 207.21 of the Commission's rules.

By order of the Commission.

Issued: March 30, 2023.

Lisa Barton,

Secretary to the Commission.

[FR Doc. 2023-07022 Filed 4-4-23; 8:45 am]

BILLING CODE 7020-02-P

DEPARTMENT OF JUSTICE

Federal Bureau of Investigation

[OMB Number 1110-0052]

Agency Information Collection Activities; Proposed eCollection eComments Requested; Revision of a Currently Approved Collection; Identity History Summary Request Form (1-783)

AGENCY: Criminal Justice Information Services Division, Federal Bureau of Investigation, Department of Justice.

ACTION: 60-Day notice.

SUMMARY: Department of Justice (DOJ), Federal Bureau of Investigation (FBI), Criminal Justice Information Services (CJIS) Division will be submitting the following information collection request to the Office of Management and Budget (OMB) for review and approval in accordance with the Paperwork Reduction Act of 1995.

DATES: The DOJ encourages public comment and will accept input until June 5, 2023.

FOR FURTHER INFORMATION CONTACT: If you have additional comments especially on the estimated public burden or associated response time, suggestions, or need a copy of the proposed information collection instrument with instructions or additional information, please contact Larry E. Cotton-Zinn, Management and Program Analyst, FBI, CJIS, Criminal History Information and Policy Unit, BTC-3, 1000 Custer Hollow Road;

Clarksburg, WV 26306; phone: 304–625–5590 or email fbi-iii@fbi.gov.

SUPPLEMENTARY INFORMATION: Written comments and suggestions from the public and affected agencies concerning the proposed collection of information are encouraged. Your comments should address one or more of the following four points:

- > Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the DOJ FBI CJIS Division, including whether the information will have practical utility;
- > Evaluate the accuracy of the agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used;
- > Evaluate whether and if so how the quality, utility, and clarity of the information to be collected can be enhanced; and
- > Minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submission of responses.

Overview of This Information Collection

1. *Type of Information Collection:* Revision of a currently approved collection.

2. *Title of the Form/Collection:* Identity History Summary Request Form.

3. *Agency form number, if any, and the applicable component of the Department sponsoring the collection:* 1110–0052, Form 1–783 Identity History Summary Request Form; CJIS Division, FBI, DOJ.

4. *Affected public who will be asked or required to respond, as well as a brief abstract:* Primary: Individuals interested in obtaining a copy of their identification record contained in the FBI's Next Generation Identification System. The U.S. Department of Justice Order 556–773 directs the FBI to publish rules for the dissemination of arrest and conviction records to the subjects of such records upon request. This order resulted in a determination that 28 United States Code 534 does not prohibit the subjects of arrest and convictions records from having access to those records.

5. *An estimate of the total number of respondents and the amount of time estimated for an average respondent to respond:* It is estimated the time it takes to process the 1–783 is five minutes.

The BSS estimates 86,707 respondents yearly.

6. *An estimate of the total public burden (in hours) associated with the collection:* With 86,707 applicants responding, the formula for applicant burden hours would be as follows: (86,707 respondents divided by 12 per hour) = 7,226 hours.

If additional information is required contact: John R. Carlson, Assistant Director, United States Department of Justice, Justice Management Division, Policy and Planning Staff, Two Constitution Square, 145 N Street NE, Suite 3E.405B, Washington, DC 20530.

Dated: 31 March 2023.

John R. Carlson,

Department Clearance Officer for PRA, U.S. Department of Justice.

[FR Doc. 2023–07108 Filed 4–4–23; 8:45 am]

BILLING CODE 4410–AT–P

DEPARTMENT OF JUSTICE

Federal Bureau of Investigation

[OMB Number 1110–0070]

Agency Information Collection Activities; Proposed eCollection eComments Requested; Revision of a Currently Approved Collection; Credit Card Payment Form (1–786)

AGENCY: Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division.

ACTION: 60-Day notice.

SUMMARY: Department of Justice (DOJ), Federal Bureau of Investigation (FBI), Criminal Justice Information Services (CJIS) Division will be submitting the following information collection request to the Office of Management and Budget (OMB) for review and approval in accordance with the Paperwork Reduction Act of 1995.

DATES: The DOJ encourages public comment and will accept input until June 5, 2023.

FOR FURTHER INFORMATION CONTACT: If you have additional comments especially on the estimated public burden or associated response time, suggestions, or need a copy of the proposed information collection instrument with instructions or additional information, please contact Larry E. Cotton-Zinn, Management and Program Analyst, FBI, CJIS, Criminal History Information and Policy Unit, BTC–3, 1000 Custer Hollow Road; Clarksburg, WV 26306; phone: 304–625–5590 or email fbi-iii@fbi.gov.

SUPPLEMENTARY INFORMATION: Written comments and suggestions from the

public and affected agencies concerning the proposed collection of information are encouraged. Your comments should address one or more of the following four points:

- > Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the DOJ FBI CJIS Division, including whether the information will have practical utility;
- > Evaluate the accuracy of the agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used;
- > Evaluate whether and if so how the quality, utility, and clarity of the information to be collected can be enhanced; and
- > Minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submission of responses.

Overview of This Information Collection

1. *Type of Information Collection:* Revision of a currently approved collection.

2. *Title of the Form/Collection:* Credit Card Payment Form.

3. *Agency form number, if any, and the applicable component of the Department sponsoring the collection:* 1110–0070, Form 1–786 Credit Card Payment Form; CJIS Division, FBI, DOJ.

4. *Affected public who will be asked or required to respond, as well as a brief abstract:* Primary: Individuals interested in obtaining a copy of their identification record contained in the FBI's Next Generation Identification System. The U.S. Department of Justice Order 556–773 directs the FBI to publish rules for the dissemination of arrest and conviction records to the subjects of such records upon request. This order resulted in a determination that 28 United States Code 534 does not prohibit the subjects of arrest and convictions records from having access to those records.

5. *An estimate of the total number of respondents and the amount of time estimated for an average respondent to respond:* It is estimated the time it takes to process the 1–786 is two minutes. The BSS estimates 28,039 respondents yearly.

6. *An estimate of the total public burden (in hours) associated with the collection:* With 28,039 applicants responding, the formula for applicant

burden hours would be as follows: (28,039 respondents divided by 30 per hour) = 934.6 hours.

If additional information is required contact: John R. Carlson, Assistant Director, United States Department of Justice, Justice Management Division, Policy and Planning Staff, Two Constitution Square, 145 N Street NE, Suite 3E.405B, Washington, DC 20530.

Dated: March 31, 2023.

John R. Carlson,

Department Clearance Officer for PRA, U.S. Department of Justice.

[FR Doc. 2023-07110 Filed 4-4-23; 8:45 am]

BILLING CODE 4410-AT-P

DEPARTMENT OF JUSTICE

[OMB Number 1121-0355]

Agency Information Collection Activities; Proposed eCollection eComments Requested; Reinstatement, With Change, of a Previously Approved Collection for Which Approval Has Expired: 2023 National Census of Victim Service Providers

AGENCY: Bureau of Justice Statistics, Department of Justice.

ACTION: 60-Day notice.

SUMMARY: The Department of Justice (DOJ), Office of Justice Programs, Bureau of Justice Statistics, will be submitting the following information collection request to the Office of Management and Budget (OMB) for review and approval in accordance with the Paperwork Reduction Act of 1995.

DATES: Comments are encouraged and will be accepted for 60 days until June 5, 2023.

FOR FURTHER INFORMATION CONTACT: If you have comments especially on the estimated public burden or associated response time, suggestions, or need a copy of the proposed information collection instrument with instructions or additional information, please contact Rachel Morgan, Bureau of Justice Statistics, 810 Seventh Street NW, Washington, DC 20531 (email: Rachel.Morgan@usdoj.gov; telephone: 202-598-9237).

SUPPLEMENTARY INFORMATION: Written comments and suggestions from the public and affected agencies concerning the proposed collection of information are encouraged. Your comments should address one or more of the following four points:

—Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the Bureau of Justice

Statistics, including whether the information will have practical utility; —Evaluate the accuracy of the agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used; —Evaluate whether and if so, how the quality, utility, and clarity of the information to be collected can be enhanced; and —Minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, *e.g.*, permitting electronic submission of responses.

Overview of This Information Collection

1. *Type of Information Collection:* Reinstatement, with change, of a previously approved collection for which approval has expired.

2. *Title of the Form/Collection:* 2023 National Census of Victim Service Providers (NCVSP).

3. *Agency form number, if any, and the applicable component of the Department of Justice sponsoring the collection:* There is no form number for the questionnaire. The applicable component within the Department of Justice is the Bureau of Justice Statistics (BJS), in the Office of Justice Programs. BJS requests clearance for the 2023 NCVSP under OMB Control No. 1121-0355. The NCVSP was last approved under OMB Control No. 1121-0355 (exp. date 05/31/2019).

4. *Affected public who will be asked or required to respond, as well as a brief abstract:* Programs and organizations that have been identified as providing services to victims of crime or abuse will be asked to respond.

The 2023 NCVSP will be the second administration of this data collection. The NCVSP provides national data on all programs and organizations that served victims of crime or abuse within the year prior to the survey. The NCVSP identifies the size and scope of the victim service provider (VSP) field, including the number of VSPs, where they are located, the number of victims they serve, and information about funding and staffing. Information from the NCVSP provides a sampling frame for follow-up surveys on victim service providers, including BJS's National Survey of Victim Service Providers.

5. *An estimate of the total number of respondents and the amount of time estimated for an average respondent to respond:* Similar to the 2017 NCVSP,

the first administration of the NCVSP, about 15% of the 20,000 VSPs on the current roster will no longer be in operation, will have stopped providing services to crime victims, or will be allied organizations that do not themselves directly assist victims. For those 3,000 out-of-scope organizations, the burden will be less than 5 minutes. For the remaining 17,000 active victim service providers, it will take the average interviewed respondent an estimated 30 minutes to respond. There are an estimated 8,750 total burden hours associated with this information collection. These estimates are based on previous estimates of item burden and input received from participants in the 2023 NCVSP cognitive testing procedures (generic OMB clearance, Control No. 1121-0339).

If additional information is required, contact: John R. Carlson, Department Clearance Officer, United States Department of Justice, Justice Management Division, Policy and Planning Staff, Two Constitution Square, 145 N Street NE, 4W-218, Washington, DC 20530.

Dated: March 30, 2023.

John R. Carlson,

Department Clearance Officer for PRA, Policy and Planning Staff, U.S. Department of Justice.

[FR Doc. 2023-07020 Filed 4-4-23; 8:45 am]

BILLING CODE 4410-18-P

DEPARTMENT OF LABOR

Employment and Training Administration

Workforce Innovation and Opportunity Act; Native American Employment and Training Council

AGENCY: Employment and Training Administration, U.S. Department of Labor.

ACTION: Notice of meeting.

SUMMARY: Pursuant to the Federal Advisory Committee Act (FACA), as amended, and the Workforce Innovation and Opportunity Act (WIOA), notice is hereby given of the next meeting of the Native American Employment and Training Council (Council), as constituted under WIOA.

DATES: The meeting will begin at 10 a.m. (Eastern Daylight Time) on Wednesday, May 3, 2023 and continue until 4:30 p.m. The meeting will reconvene at 1 p.m. on Thursday, May 4, 2023 and adjourn at 4:30 p.m. The period from 3 p.m., to 4 p.m. on May 4, 2023 is reserved for participation and comment by members of the public.

ADDRESSES: The meeting will be held in person at the Foxwoods Hotel, 240 Fox Tower Drive, Mashantucket, CT 06339, located in the Fox Tower, Celebrity Ballrooms A, B and C. The meeting will also be accessible virtually on the *Zoom.gov* platform. To join the meeting use the following URL: <https://www.zoomgov.com/j/1603344439?pwd=M1liREg0Z1kxdmdWWIA2TXB4LytIUT09>, Meeting ID: 1603344439, Passcode: 648175.

SUPPLEMENTARY INFORMATION: Council members and members of the public are encouraged to logon to *Zoom.gov* early to allow for connection issues and troubleshooting.

The meeting will be open to the public. Members of the public not present may submit a written statement by Friday, April 28, 2023, to be included in the record of the meeting. Statements are to be submitted to Nathaniel Coley, Designated Federal Officer (DFO), U.S. Department of Labor at coley.nathaniel.d@dol.gov. Persons who need special accommodations should contact Phillip Roulain at 703-209-5889 or proulain@tribaltechllc.com two business days before the meeting. The formal agenda will focus on the following topics: (1) Updates from the Employment and Training Administration, including implementation of Workforce Innovation and Opportunity Act programs, and status of previous NAETC recommendations; (2) Training and technical assistance updates and priorities; (3) NAETC workgroup updates; (4) updates on implementation of the 477 program; (5) Presentation on WIOA participants served and outcomes since the implementation of the Grantee Performance Management System (GPMS); (6) ETA/DINAP updates; and (7) public comment.

FOR FURTHER INFORMATION CONTACT: Nathaniel Coley, DFO, Division of Indian and Native American Programs, Employment and Training Administration, U.S. Department of Labor, Room C-4311, 200 Constitution Avenue NW, Washington, DC 20210. Telephone number (202) 693-4287 (VOICE) (this is not a toll-free number) or coley.nathaniel.d@dol.gov.

Brent Parton,

Acting Assistant Secretary for Employment and Training, Labor.

[FR Doc. 2023-07019 Filed 4-4-23; 8:45 am]

BILLING CODE 4510-FR-P

DEPARTMENT OF LABOR

Occupational Safety and Health Administration

[Docket No. OSHA-2012-0040]

The Standard on 4,4'—Methylenedianiline for General Industry of the Office of Management and Budget's (OMB) Approval of Information Collection (Paperwork) Requirements

AGENCY: Occupational Safety and Health Administration (OSHA), Labor.

ACTION: Request for public comments.

SUMMARY: OSHA solicits public comments concerning the proposal to extend the Office of Management and Budget's (OMB) approval of the information collection requirements specified in the Standard on 4,4'—Methylenedianiline for General Industry.

DATES: Comments must be submitted (postmarked, sent, or received) by June 5, 2023.

ADDRESSES:

Electronically: You may submit comments and attachments electronically at <http://www.regulations.gov>, which is the Federal eRulemaking Portal. Follow the instructions online for submitting comments.

Docket: To read or download comments or other material in the docket, go to <http://www.regulations.gov>. Documents in the docket are listed in the <http://www.regulations.gov> index; however, some information (e.g., copyrighted material) is not publicly available to read or download through the website. All submissions, including copyrighted material, are available for inspection through the OSHA Docket Office. Contact the OSHA Docket Office at (202) 693-2350 (TTY (877) 889-5627) for assistance in locating docket submissions.

Instructions: All submissions must include the agency name and OSHA docket number (OSHA-2012-0040) for the Information Collection Request (ICR). OSHA will place all comments, including any personal information, in the public docket, which may be made available online. Therefore, OSHA cautions interested parties about submitting personal information such as social security numbers and birthdates.

For further information on submitting comments, see the "Public Participation" heading in the section of this notice titled **SUPPLEMENTARY INFORMATION**.

FOR FURTHER INFORMATION CONTACT:

Seleda Perryman or Theda Kenney, Directorate of Standards and Guidance, OSHA, U.S. Department of Labor; telephone (202) 693-2222.

SUPPLEMENTARY INFORMATION:

I. Background

The Department of Labor, as part of the continuing effort to reduce paperwork and respondent (i.e., employer) burden, conducts a preclearance consultation program to provide the public with an opportunity to comment on proposed and continuing information collection requirements in accordance with the Paperwork Reduction Act of 1995 (PRA) (44 U.S.C. 3506(c)(2)(A)). This program ensures that information is in the desired format, reporting burden (time and costs) is minimal, the collection instruments are clearly understood, and OSHA's estimate of the information collection burden is accurate. The Occupational Safety and Health Act of 1970 (OSH Act) (29 U.S.C. 651 *et seq.*) authorizes information collection by employers as necessary or appropriate for enforcement of the OSH Act or for developing information regarding the causes and prevention of occupational injuries, illnesses, and accidents (29 U.S.C. 657). The OSH Act also requires that OSHA obtain such information with minimum burden upon employers, especially those operating small businesses, and to reduce to the maximum extent feasible unnecessary duplication of effort in obtaining information (29 U.S.C. 657).

The following sections describe who uses the information collected under each requirement, as well as how they use it. The purpose of these requirements specified in the 4,4'—Methylenedianiline Standard for General Industry (the "MDA Standard") (29 CFR 1910.1050) protect workers from the adverse health effects that may result from their exposure to MDA, including cancer, liver, and skin disease. The major paperwork requirements specify that employers must perform initial, periodic, and additional exposure monitoring; notify each worker in writing of their results as soon as possible but no longer than five (5) days after receiving exposure monitoring results; and routinely inspect the hands, face, and forearms of each worker potentially exposed to MDA for signs of dermal exposure to MDA. Employers must also establish a written compliance program; institute a respiratory protection program in accordance with OSHA's Respiratory Protection Standard (29 CFR 1910.134);

and to develop a written emergency plan for any construction operation that could have an MDA emergency (*i.e.*, an unexpected and potentially hazardous release of MDA).

Employers must label any material or products containing MDA, including containers used to store MDA-contaminated protective clothing and equipment. They also must inform personnel who launder MDA-contaminated clothing of the requirement to prevent release of MDA, while personnel who launder or clean MDA-contaminated protective clothing or equipment must receive information about the potentially harmful effects of MDA. In addition, employers are to post warning signs at entrances or access ways to regulated areas, as well as train workers exposed to MDA at the time of their initial assignment, and at least annually thereafter.

Other paperwork provisions of the MDA standard require employers to provide workers with medical examinations, including initial, periodic, emergency and follow-up examinations. As part of the medical surveillance program, employers must ensure that the examining physician receives specific written information, and that they obtain from the physician a written opinion regarding the worker's medical results and exposure limitations.

The MDA standard also specifies that employers are to establish and maintain exposure monitoring and medical surveillance records for each worker who is subject to these respective requirements, make any required record available to OSHA compliance officers and the National Institute for Occupational Safety and Health (NIOSH) for examination and copying, and provide exposure monitoring and medical surveillance records to workers and their designated representatives. Finally, employers who cease to do business within the period specified for retaining exposure monitoring and medical surveillance records, and who have no successor employer, must notify NIOSH at least 90 days before disposing of the records and transmit the records to NIOSH if so requested.

II. Special Issues for Comment

OSHA has a particular interest in comments on the following issues:

- Whether the proposed information collection requirements are necessary for the proper performance of the agency's functions to protect workers, including whether the information is useful;
- The accuracy of OSHA's estimate of the burden (time and costs) of the

information collection requirements, including the validity of the methodology and assumptions used;

- The quality, utility, and clarity of the information collected; and
- Ways to minimize the burden on employers who must comply; for example, by using automated or other technological information collection, and transmission techniques.

III. Proposed Actions

OSHA is requesting that OMB extend the approval of the information collection requirements contained in 4,4'-Methylenedianiline for General Industry. The agency is requesting to maintain previously approved burden hours calculations for this proposed ICR, which is 317 burden hours. The agency estimated an overall increase in the estimated number of covered establishments in specific industry sectors in the prior ICR and is not going to change the estimates for this request. OSHA is not requesting an adjustment for the Capital Costs, which is \$25,740, due to the increased cost of the samples and the CPI.

OSHA will summarize the comments submitted in response to this notice and will include this summary in the request to OMB to extend the approval of the information collection requirements.

Type of Review: Extension of a currently approved collection.

Title: 4,4'-Methylenedianiline Standard for General Industry (29 CFR 1910.1050).

OMB Control Number: 1218-0184.

Affected Public: Business or other for-profits; Not-for-profit organizations; Federal Government; State, Local, or Tribal government.

Number of Respondents: 10.

Number of Responses: 584.

Frequency of Responses: On occasion.

Average Time per Response: Varies.

Estimated Total Burden Hours: 317.

Estimated Cost (Operation and Maintenance): \$25,740.

IV. Public Participation—Submission of Comments on This Notice and Internet Access to Comments and Submissions

You may submit comments in response to this document as follows:

- (1) electronically at <http://www.regulations.gov>, which is the Federal eRulemaking Portal; (2) by facsimile (fax); if your comments, including attachments, are not longer than 10 pages you may fax them to the OSHA Docket Office at 202-693-1648; or (3) by hard copy. Please note: While OSHA's Docket Office is continuing to accept and process submissions by regular mail due to the COVID-19

pandemic, the Docket Office is closed to the public and not able to receive submissions to the docket by hand, express mail, messenger, and courier service. All comments, attachments, and other material must identify the agency name and the OSHA docket number for the ICR OSHA-2012-0040. You may supplement electronic submissions by uploading document files electronically. If you wish to mail additional materials in reference to an electronic or a facsimile submission, you must submit them to the OSHA Docket Office (see the section of this notice titled **ADDRESSES**). The additional materials must clearly identify your electronic comments by your name, date, and the docket number so that the agency can attach them to your comments.

Due to security procedures, the use of regular mail may cause a significant delay in the receipt of comments.

Comments and submissions are posted without change at <http://www.regulations.gov>. Therefore, OSHA cautions commenters about submitting personal information such as social security numbers and dates of birth. Although all submissions are listed in the <http://www.regulations.gov> index, some information (*e.g.*, copyrighted material) is not publicly available to read or download from this website. All submissions, including copyrighted material, are available for inspection and copying at the OSHA Docket Office. Information on using the <http://www.regulations.gov> website to submit comments and access the docket is available at the website's "User Tips" link. Contact the OSHA Docket Office at (202) 693-2350, (TTY) (877) 889-5627 for information about materials not available from the website, and for assistance in using the internet to locate docket submissions.

V. Authority and Signature

James S. Frederick, Deputy Assistant Secretary of Labor for Occupational Safety and Health, directed the preparation of this notice. The authority for this notice is the Paperwork Reduction Act of 1995 (44 U.S.C. 3506 *et seq.*) and Secretary of Labor's Order No. 8-2020 (85 FR 58393).

Signed at Washington, DC, on March 29, 2023.

James S. Frederick,

Deputy Assistant Secretary of Labor for Occupational Safety and Health.

[FR Doc. 2023-07047 Filed 4-4-23; 8:45 am]

BILLING CODE 4510-26-P

NATIONAL SCIENCE FOUNDATION**Notice of Intent To Seek Approval To Renew an Information Collection System; Grantee Reporting Requirements for the NSF Small Business Innovation Research and the Small Business Technology Transfer (SBIR/STTR) Programs****AGENCY:** National Science Foundation.**ACTION:** Notice and request for comments.

SUMMARY: Under the Paperwork Reduction Act of 1995, and as part of its continuing effort to reduce paperwork and respondent burden, the National Science Foundation (NSF) is inviting the general public or other Federal agencies to comment on this proposed continuing information collection.

DATES: Written comments on this notice must be received by June 5, 2023, to be assured consideration. Comments received after that date will be considered to the extent practicable. Send comments to address below.

FOR FURTHER INFORMATION CONTACT: Suzanne H. Plimpton, Reports Clearance Officer, National Science Foundation, 2415 Eisenhower Avenue, Suite E7400, Alexandria, Virginia 22314; telephone (703) 292-7556; or send email to splimpto@nsf.gov. Individuals who use a telecommunications device for the deaf (TDD) may call the Federal Information Relay Service (FIRS) at 1-800-877-8339, which is accessible 24 hours a day, 7 days a week, 365 days a year (including federal holidays).

Comments: Comments are invited on: (a) whether the proposed collection of information is necessary for the proper performance of the functions of the Foundation, including whether the information will have practical utility; (b) the accuracy of the Foundation's estimate of the burden of the proposed collection of information; (c) ways to enhance the quality, utility, and clarity of the information to be collected; and (d) ways to minimize the burden of the collection of information on those who are to respond, including through the use of automated collection techniques or other forms of information technology.

SUPPLEMENTARY INFORMATION:

Title of Collection: Grantee Reporting Requirements for the NSF Small Business Innovation Research and the Small Business Technology Transfer (SBIR/STTR) Programs.

OMB Number: 3145-0252.

Expiration Date of Approval: July 31, 2023.

Type of Request: Revision to and extension of approval of an information collection.

Abstract:

Proposed Project: This request is for renewal approval of interim reporting requirements for the NSF Small Business Innovation Research (SBIR)/Small Business Technology Transfer Research (STTR) programs.

The NSF SBIR/STTR programs focus on transforming scientific discovery into products and services with commercial potential and/or societal benefit. Unlike fundamental or basic research activities that focus on scientific and engineering discoveries, the NSF SBIR/STTR programs support the creation of opportunities to move fundamental science and engineering out of the lab and into the market at scale, through startups and small businesses representing deep technology ventures.

The NSF SBIR/STTR programs have two phases: Phase I and Phase II (with an optional Phase IIB as matching supplements). SBIR/STTR Phase I is a 6-12 month experimental or theoretical investigation that allows the awardees to determine the scientific and technical feasibility, as well as the commercial merit of the idea or concept. Phase II further develops the proposed concept, building on the feasibility project undertaken in Phase I, and accelerate the Phase I project to the commercialization stage and enhance the overall strength of the commercial potential. As such, Phase II SBIR/STTR awards have a longer expected period of performance of 24 months.

The NSF SBIR/STTR programs request approval from the Office of Management and Budget (OMB) on the renewal of the NSF SBIR/STTR Phase II interim/progress report data collection.

The interim/progress report will be required every six months for the life of the Phase II award. The report collects information on the technical progress of the funded NSF work, which allows managing Program Directors to monitor the project and ensure that the award is in good standing.

The report is divided into 6 sections: (1) Basic Reporting Data, (2) Level of Effort, (3) SBIR-wide Certifications, (4) Cooperative Agreement (NSF-specific Certifications), (5) Technical Narratives, and (6) Project Milestones.

The kinds of data collected from the report include name of the startup company, information on the principal investigator (PI) (name, email address, and phone number), the number of full-time equivalent (FTE) employees working at the startup, amount of funding received during the award period. In addition, information

pertaining to company officers and key personnel, their corresponding ownership status, and their levels of efforts provided to the startups are also requested. Collectively, these data will enable the managing Program Directors to (1) evaluate a given company's business structure, (2) ascertain the level of commitment of the PI(s), co-PI(s), and key personnel to the startup venture, and (3) identify conflicts of interests (if any), as part of the due diligence process that the programs undertake to verify that there are no fraudulent or inappropriate business practices.

The report also asks about: inputs (*i.e.*, project expenditures, efforts exerted by key personnel), outputs (*i.e.*, R&D activities, technical progresses), outcomes (*i.e.*, research milestones, fundraising activities), and impacts (*i.e.*, technical and/or commercial successes).

Finally, the report also requests: (1) a discussion of progresses highlighting key technical and commercial activity/results during the reporting period, (2) compliance requirements checklists from the Small Business Administration (SBA) and NSF, and (3) a Gantt chart describing the project status, as well as task assignments to key personnel in the project.

Use of the Information: The data collected will be used primarily for award monitoring. The data could also be used for congressional requests, inquiries from the NSF's Office of the Inspector General, supporting evidence of litigations, auditing, and other legal investigations, NSF internal reports, and program evaluations, if necessary.

Estimate of Burden: The estimated number of respondents is: 800. Average time to complete the interim report: 1.0 hour. The estimated total burden hours: 800 hours per year.

Respondents: The respondents are either PIs or Co-PIs listed on the NSF SBIR/STTR Proposals, Founders, and/or Co-founders of the startups funded by the NSF SBIR/STTR programs.

Dated: March 31, 2023.

Suzanne H. Plimpton,
Reports Clearance Officer, National Science Foundation.

[FR Doc. 2023-07070 Filed 4-4-23; 8:45 am]

BILLING CODE 7555-01-P

NUCLEAR REGULATORY COMMISSION

[Docket Nos. 50–387, 50–388, and 72–028; NRC–2022–0185]

In the Matter of Susquehanna Nuclear, LLC; Susquehanna Steam Electric Station, Units 1 and 2 and the Associated Independent Spent Fuel Storage Installation

AGENCY: Nuclear Regulatory Commission.

ACTION: Indirect transfer of licenses; order.

SUMMARY: The U.S. Nuclear Regulatory Commission (NRC) is issuing an order approving the application filed by Susquehanna Nuclear, LLC (Susquehanna Nuclear), on behalf of itself and the unsecured creditors of Talen Energy Supply, LLC, on September 29, 2022, as supplemented. Specifically, the order approves the indirect transfer of control of Susquehanna Nuclear's interests in the operating licenses for the Susquehanna Steam Electric Station (Susquehanna), Units 1 and 2 and the general license for the Susquehanna independent spent fuel storage installation, and conforming administrative amendments to the operating licenses.

DATES: The order was issued on March 30, 2023, and is effective for 1 year.

ADDRESSES: Please refer to Docket ID NRC–2022–0185 when contacting the NRC about the availability of information regarding this document. You may obtain publicly available information related to this document by using any of the following methods:

- *Federal Rulemaking Website:* Go to <https://www.regulations.gov> and search for Docket ID NRC–2022–0185. Address questions about Docket IDs in *Regulations.gov* to Stacy Schumann; telephone: 301–415–0624; email: Stacy.Schumann@nrc.gov. For technical questions, contact the individual listed in the **FOR FURTHER INFORMATION**

CONTACT section of this document.

- *NRC's Agencywide Documents Access and Management System (ADAMS):* You may obtain publicly available documents online in the ADAMS Public Documents collection at <https://www.nrc.gov/reading-rm/adams.html>. To begin the search, select "Begin Web-based ADAMS Search." For problems with ADAMS, please contact the NRC's Public Document Room (PDR) reference staff at 1–800–397–4209, 301–415–4737, or by email to PDR.Resource@nrc.gov. The order, the NRC staff safety evaluation supporting the order, and the draft conforming

amendments are available in ADAMS under Package Accession No. ML23073A126.

- *NRC's PDR:* You may examine and purchase copies of public documents, by appointment, at the NRC's PDR, Room P1 B35, One White Flint North, 11555 Rockville Pike, Rockville, Maryland 20852. To make an appointment to visit the PDR, please send an email to PDR.Resource@nrc.gov or call 1–800–397–4209 or 301–415–4737, between 8 a.m. and 4 p.m. eastern time, Monday through Friday, except Federal holidays.

FOR FURTHER INFORMATION CONTACT:

Audrey L. Klett, Office of Nuclear Reactor Regulation, U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001; telephone: 301–415–0489; email: Audrey.Klett@nrc.gov.

SUPPLEMENTARY INFORMATION: The text of the order is attached.

Dated: March 31, 2023.

For the Nuclear Regulatory Commission.

Audrey L. Klett,

Senior Project Manager, Plant Licensing Branch I, Division of Operator Reactor Licensing, Office of Nuclear Reactor Regulation.

Attachment—Order Approving Indirect Transfer of Licenses and Draft Conforming License Amendments

United States of America

Nuclear Regulatory Commission

In the Matter of Susquehanna Nuclear, LLC (Susquehanna Steam Electric Station,) 72–28 Units 1 and 2 and the associated independent spent fuel storage installation.

Docket Nos. 50–387, 50–388, and Renewed License Nos. NPF–14 and NPF–22

Order Approving Indirect Transfer of Licenses and Draft Conforming License Amendments

I.

Susquehanna Nuclear, LLC (Susquehanna Nuclear) and Allegheny Electric Cooperative, Inc. are the holders of Renewed Facility Operating License Nos. NPF–14 and NPF–22 and the general license for the independent spent fuel storage installation (ISFSI) (collectively, the licenses), which authorize the possession, use, and operation of the Susquehanna Steam Electric Station (Susquehanna), Units 1 and 2 and the Susquehanna ISFSI, respectively (the facilities). The facilities are located in Luzerne County, Pennsylvania.

II.

Pursuant to title 10 of the *Code of Federal Regulations* (10 CFR) section 50.80, "Transfer of licenses," and 10 CFR 72.50, "Transfer of license," and by letter PLA–8015 dated September 29, 2022, as supplemented by letters PLA–8032, PLA–8039, and PLA–8057 dated October 28, 2022, December 22, 2022, and March 15, 2023, respectively (the application), Susquehanna Nuclear, on behalf

of itself and the unsecured creditors (as described in the application) of Talen Energy Supply, LLC (Talen Energy Supply) (collectively, the applicants), requested that the U.S. Nuclear Regulatory Commission (NRC, the Commission) consent to the indirect transfer of control of Susquehanna Nuclear's interests in the licenses. The applicants requested that the NRC consent to this indirect license transfer to support a proposed transaction in which Susquehanna Nuclear would continue to be directly owned by Talen Energy Supply, but which, in turn, would be directly owned by an as-yet unnamed new parent company identified herein as Reorganized Talen Energy Corporation. Pursuant to 10 CFR 50.90, "Application for amendment of license, construction permit, or early site permit," the applicants also requested that the NRC approve conforming administrative amendments to the licenses to reflect a change in the entity (*i.e.*, from Talen Energy Corporation to Talen Energy Supply) responsible for providing a financial support agreement to Susquehanna Nuclear, as well as related editorial changes and changes regarding the investment of decommissioning trust funds, with such amendments to be effective at the consummation of the proposed transaction.

Susquehanna Nuclear is a direct, wholly-owned subsidiary of Talen Energy Supply. Talen Energy Supply is a direct, wholly-owned subsidiary of Talen Energy Corporation, the stock of which is held by affiliates of Riverstone Holdings, LLC. Commencing on May 9, 2022, Talen Energy Supply and certain of its subsidiaries (collectively, the debtors) each filed a voluntary case under chapter 11 of title 11 of the United States Code in the United States Bankruptcy Court for the Southern District of Texas. Also on May 9, 2022, the debtors executed a restructuring support agreement with certain holders of the debtors' unsecured notes. On September 9, 2022, the debtors, including Susquehanna Nuclear, filed a Joint Plan of Reorganization (the Plan) and related Disclosure Statement in the Bankruptcy Court. Under the terms of the Plan, along with certain supporting settlements and agreements, the debtors and Talen Energy Corporation intend to pursue a comprehensive restructuring pursuant to a debt-for-equity exchange in which the equity of the ultimate direct and indirect parent of Reorganized Talen Energy Corporation will be distributed to holders of unsecured notes claims and general unsecured claims (together, the unsecured creditors) and to eligible unsecured creditors that participate in a rights offering, through which such unsecured creditors can obtain additional shares of common equity in Reorganized Talen Energy Corporation (the Equitization Transaction), while allowing for an alternative transaction on certain terms, should one materialize. The Bankruptcy Court confirmed the Plan on December 15, 2022. The applicants also notified the NRC that the parent of Talen Energy Supply, Talen Energy Corporation, has itself filed a voluntary case under chapter 11 of title 11 of the United States Code, which is jointly administered with its subsidiary debtors' chapter 11 cases.

Pursuant to the restructuring support agreement, the debtors have agreed to move forward expeditiously with the confirmation and consummation of the Plan, and to be subject to certain milestones, including an effective date of the Plan by no later than May 9, 2023 (subject to a potential six-month extension). The applicants expect that at the conclusion of the proposed transaction, Susquehanna Nuclear will continue to be directly owned by Talen Energy Supply, which, in turn, will either be, or be directly owned by, Reorganized Talen Energy Corporation.

As a result of the Equitization Transaction set forth in the Plan, ownership, in the form of common equity shares in Reorganized Talen Energy Corporation will be spread among certain unsecured creditors, a class which involves numerous entities, only four of which are likely to exceed 5-percent ownership, and only three of which are likely to exceed 10-percent ownership. No single holder is expected to hold in excess of 25 percent of Reorganized Talen Energy Corporation, and no holders will have any special control rights over either Reorganized Talen Energy Corporation, Talen Energy Supply (to the extent another entity serves as Reorganized Talen Energy Corporation) or Susquehanna Nuclear.

On November 8, 2022, the NRC published a notice of consideration of approval of the application in the **Federal Register** (87 FR 67511). This notice provided an opportunity to comment, request a hearing, and petition for leave to intervene on the application. The NRC did not receive any written comments in response to the notice. On November 28, 2022, Eric J. Epstein submitted a petition for leave to intervene and hearing request; on March 17, 2023, the Commission denied this petition and hearing request and terminated the proceeding (Memorandum and Order CLI-23-01).

Pursuant to 10 CFR 50.80, no license for a utilization facility, or any right thereunder, shall be transferred, either voluntarily or involuntarily, directly or indirectly, through transfer of control of the license to any person, unless the Commission gives its consent in writing. Pursuant to 10 CFR 72.50, no license or any part included in a license issued under 10 CFR part 72 for an ISFSI shall be transferred, assigned, or in any manner disposed of, either voluntarily or involuntarily, directly or indirectly, through transfer of control of the license to any person, unless the Commission gives its consent in writing. Upon review of the information in the application, as supplemented, and other information before the Commission, and relying upon the representations contained in the application, the NRC staff has determined that Susquehanna Nuclear is qualified to hold the licenses, to the extent described in the application, and that the transfer of the licenses is otherwise consistent with applicable provisions of law, regulations, and orders issued by the Commission pursuant thereto, subject to the condition set forth below.

Upon review of the information in the application, as supplemented, for conforming license amendments to reflect the transfer,

the NRC staff has determined that: (1) there is reasonable assurance that the health and safety of the public will not be endangered by operation in the proposed manner, (2) there is reasonable assurance that such activities will be conducted in compliance with the Commission's regulations, and (3) the issuance of the amendments will not be inimical to the common defense and security or to the health and safety of the public.

The findings set forth above are supported by an NRC staff safety evaluation dated the same date as this order, which is available at Agencywide Documents Access and Management System (ADAMS) Accession No. ML23073A107 (non-proprietary).

III.

Accordingly, pursuant to Sections 161b, 161i, and 184 of the Atomic Energy Act of 1954, as amended, 42 U.S.C. 2201(b), 2201(i), and 2234; and 10 CFR 50.80, 10 CFR 72.50, and 10 CFR 50.90, *it is hereby ordered* that the application regarding the proposed indirect license transfer, as described herein, is approved, subject to the following condition:

At least 5 business days before the planned closing of the proposed transaction, the applicants shall submit, signed under oath or affirmation, the following information to the NRC in accordance with 10 CFR part 50: (1) the final legal entity name of Reorganized Talen Energy Corporation; (2) the state of incorporation and address for Reorganized Talen Energy Corporation; and (3) the names, addresses, and citizenship of the directors and principal officers of Reorganized Talen Energy Corporation.

It is further ordered that after receipt of all required regulatory approvals of the proposed transaction, the applicants shall inform the Director of the Office of Nuclear Reactor Regulation in writing of such receipt no later than 5 business days prior to the planned closing of the proposed transaction. Should the proposed transaction not be completed within 1 year of the date of this order, this order shall become null and void, provided, however, that upon written application to the Director of the Office of Nuclear Reactor Regulation and for good cause shown, such date may be extended by order. The condition of this order may be amended upon application by the applicants and approval by the NRC.

It is further ordered that consistent with 10 CFR 2.1315(b), the license amendments that make changes, as indicated in Enclosure 2 to the letter forwarding this order, to reflect the subject indirect transfer, are approved. The amendments shall be issued and made effective when the proposed indirect transfer actions are completed.

This order is effective upon issuance.

For further details with respect to this order, see the application dated September 29, 2022 (ML22272A603), as supplemented by letters dated October 28, 2022, December 22, 2022, and March 15, 2023 (ML22301A204, ML22356A306, and ML23074A336, respectively), and the associated NRC staff safety evaluation dated the same date as this order. Publicly available documents created or received at the NRC are accessible electronically through ADAMS in

the NRC Library at <https://www.nrc.gov/reading-rm/adams.html>. Persons who do not have access to ADAMS or who encounter problems in accessing the documents located in ADAMS, should contact the NRC Public Document Room reference staff by telephone at 1-800-397-4209, or 301-415-4737, or by email to pdr.resource@nrc.gov.

Dated: March 30, 2023.

For the Nuclear Regulatory Commission.

Jamie M. Heisserer,

Deputy Director, Division of Operating Reactor Licensing, Office of Nuclear Reactor Regulation.

[FR Doc. 2023-07073 Filed 4-4-23; 8:45 am]

BILLING CODE 7590-01-P

OFFICE OF SCIENCE AND TECHNOLOGY POLICY

Request for Information; National Nanotechnology Initiative Environmental, Health, and Safety Research Strategy

AGENCY: Office of Science and Technology Policy (OSTP).

ACTION: Notice of request for information.

SUMMARY: The National Nanotechnology Coordination Office (NNCO), on behalf of the Nanoscale Science, Engineering, and Technology (NSET) Subcommittee of the Committee on Technology, National Science and Technology Council (NSTC), seeks public input in updating the National Nanotechnology Initiative (NNI) Environmental, Health, and Safety (EHS) Research Strategy. The NNI's current strategy was prepared in 2011, with substantial public engagement. Federal agencies participating in NSET's Nanotechnology Environmental and Health Implications (NEHI) Working Group have begun to review the 2011 NNI EHS Research Strategy and request input to help inform a revised and updated EHS strategy.

DATES: Interested persons and organizations are invited to submit comments on or before 5 p.m. ET June 2, 2023.

ADDRESSES: Comments must be submitted via the Federal eRulemaking Portal at [regulations.gov](https://www.regulations.gov). However, if you require an accommodation or cannot otherwise submit your comments via [regulations.gov](https://www.regulations.gov), please contact the program contact person listed under **FOR FURTHER INFORMATION CONTACT**. OSTP will not accept comments by fax or by email, or comments submitted after the comment period closes. To ensure that OSTP does not receive duplicate copies, please submit your comments only once.

Additionally, please include the Docket ID at the top of your comments.

Federal eRulemaking Portal: Go to www.regulations.gov to submit your comments electronically. Information on how to use [Regulations.gov](http://www.regulations.gov), including instructions for accessing agency documents, submitting comments, and viewing the docket, is available on the site under “FAQ” (<https://www.regulations.gov/faq>).

Privacy Note: OSTP’s policy is to make all comments received from members of the public available for public viewing in their entirety on the Federal eRulemaking Portal at www.regulations.gov. Therefore, commenters should be careful to include in their comments only information that they wish to make publicly available. OSTP requests that no proprietary information, copyrighted information, or personally identifiable information be submitted in response to this RFI.

Instructions: Response to this RFI is voluntary. Respondents need not reply to all questions listed. For all submissions, clearly indicate which questions are being answered. Multiple submissions from an individual, group, or institution will be considered as supplements to the original response and not as new comments. Submissions should include the name(s) of the person(s) or organization(s) filing the comment.

Any information obtained from this RFI is intended to be used by the Government on a non-attribution basis for planning and strategy development. OSTP will not respond to individual submissions. A response to this RFI will not be viewed as a binding commitment to develop or pursue the project or ideas discussed. This RFI is not accepting applications for financial assistance or financial incentives. Please note that the United States Government will not pay for response preparation, or for the use of any information contained in a response.

FOR FURTHER INFORMATION CONTACT:

Rhema Bjorkland at info@nncn.gov or 202–517–1050. Individuals who use telecommunication devices for the deaf and hard of hearing (TDD) may call the Federal Relay Service (FRS) at 1–800–877–8339, 24 hours a day, every day of the year, including holidays.

SUPPLEMENTARY INFORMATION:

Background Information: NEHI, on behalf of the NNI, is engaging the community early in the process to allow the public and key stakeholders to inform revisions to the NNI EHS research strategy. In preparing comments, the public is invited to view

the core research areas and their associated needs as set out in the NNI 2011 Environmental, Health, and Safety (EHS) Research Strategy (<https://www.nano.gov/2011EHSStrategy>). The 2014 Progress Review on the Coordinated Implementation of the National Nanotechnology Initiative 2011 Environmental, Health, and Safety Research Strategy (<https://www.nano.gov/2014-EHS-Progress-Review>) and 2017 Highlights of Recent Research on the Environmental, Health, and Safety Implications of Engineered Nanomaterials (<https://www.nano.gov/Highlights-Federal-NanoEHS-Report>) provide additional information on the progress made in the core research areas.

Information Requested: Pursuant to 42 U.S.C. 6617, OSTP is soliciting public input through an RFI to obtain feedback from a wide variety of stakeholders, including individuals, industry, academia, research laboratories, nonprofits, and think tanks. OSTP is interested in public input to inform an updated nanotechnology EHS research strategy, specifically a strategy that focuses on the use of science-based risk analysis and risk management to protect public health and the environment while also fostering the technological advancements that benefit society. OSTP seeks responses to any or all of the following questions:

1. What are the research accomplishments in the following six core research areas identified in the 2011 NNI EHS Strategy? The six core research areas are (1) Nanomaterial Measurement Infrastructure, (2) Human Exposure Assessment, (3) Human Health, (4) Environment, (5) Risk Assessment and Risk Management Methods, and (6) Informatics and Modeling.

2. What research gaps remain in addressing the six NNI EHS core research areas listed in question 1?

3. The ethical, legal, and societal implications (ELSI) of nanotechnology are considered across the core research areas of the 2011 strategy. What additional ways could ELSI be more fully integrated throughout a refreshed NNI EHS research strategy?

4. What broad themes should the revised strategy adopt to integrate and connect the six research areas?

5. How should the updated NNI EHS research strategy reflect the evolution of nanotechnology beyond engineered nanomaterials to complex systems, structures, and devices?

6. The 2011 strategy focused on engineered nanomaterials and did not include incidental nanoscale materials

such as nanoplastics and certain nanoscale particulate emissions such as those from 3D printing. If the updated strategy is revised to include some non-engineered or incidental nanomaterials, describe how to scope the strategy in a way that complements rather than being redundant with existing health and environmental research (e.g., by excluding the large body of existing research on air pollution, which can include nanoscale particles).

Dated: March 31, 2023.

Stacy Murphy,

Deputy Chief Operations Officer/Security Officer.

[FR Doc. 2023–07074 Filed 4–4–23; 8:45 am]

BILLING CODE 3270–F1–P

SECURITIES AND EXCHANGE COMMISSION

[Release No. 34–97225; File No. SR–OCC–2023–003]

Self-Regulatory Organizations; The Options Clearing Corporation; Notice of Filing of Proposed Rule Change by The Options Clearing Corporation Concerning Clearing Member Cybersecurity Obligations

March 30, 2023.

Pursuant to Section 19(b)(1) of the Securities Exchange Act of 1934 (“Exchange Act” or “Act”),¹ and Rule 19b–4 thereunder,² notice is hereby given that on March 21, 2023, The Options Clearing Corporation (“OCC” or “Corporation”) filed with the Securities and Exchange Commission (“SEC” or “Commission”) the proposed rule change as described in Items I, II, and III below, which Items have been prepared primarily by OCC. The Commission is publishing this notice to solicit comments on the proposed rule change from interested persons.

I. Clearing Agency’s Statement of the Terms of Substance of the Proposed Rule Change

The proposed rule change would amend certain provisions in OCC’s Rules relating to Clearing Member cybersecurity obligations to address the occurrence of a cyber-related disruption or intrusion of a Clearing Member (“Security Incident”). The proposed changes would (i) require a Clearing Member to immediately notify OCC of a Security Incident; (ii) memorialize OCC’s ability to take actions reasonably necessary to mitigate any effects to its operations; and (iii) require such

¹ 15 U.S.C. 78s(b)(1).

² 17 CFR 240.19b–4.

Clearing Member to provide a form containing written representations addressing the incident and attesting to certain security requirements (“Reconnection Attestation”) and an associated checklist describing remediation efforts (“Reconnection Checklist” and together, “Reconnection Attestation and Checklist”).

The proposed changes to OCC’s Rules are included as Exhibit 5 to File No. SR–OCC–2023–003. Material proposed to be added to the Rules as currently in effect is underlined and material proposed to be deleted is marked in strikethrough text. All capitalized terms not defined herein have the same meaning as set forth in the OCC By-Laws and Rules.³

II. Clearing Agency’s Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change

In its filing with the Commission, OCC included statements concerning the purpose of and basis for the proposed rule change and discussed any comments it received on the proposed rule change. The text of these statements may be examined at the places specified in Item IV below. OCC has prepared summaries, set forth in sections (A), (B), and (C) below, of the most significant aspects of these statements.

(A) Clearing Agency’s Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change

(1) Purpose

Overview

The proposed rule change would amend certain provisions in the Rules relating to Clearing Member cybersecurity obligations to address the occurrence of a Security Incident. The proposed changes would (i) require a Clearing Member to immediately notify OCC of a Security Incident; (ii) memorialize OCC’s ability to take actions reasonably necessary to mitigate any effects to its operations; and (iii) require such Clearing Member to provide a Reconnection Attestation containing written representations addressing the incident and attesting to certain security requirements and an associated Reconnection Checklist describing remediation efforts. As described in more detail below, the proposed rule change is designed to help OCC assess and take appropriate action to manage the cybersecurity risks that may be introduced to OCC’s information and data systems due to a Security Incident.

³ OCC’s By-Laws and Rules can be found on OCC’s public website: <https://www.theocc.com/Company-Information/Documents-and-Archives/By-Laws-and-Rules>.

OCC believes it is prudent to implement a standardized approach to assess and manage the cybersecurity risks that OCC may face through its interconnections to Clearing Members. Cybersecurity incidents pose an ongoing risk to OCC, as well as market participants, as an attack on OCC can lead to the loss of data or system integrity, unauthorized disclosure of sensitive information, or an inability to conduct essential clearance and settlement functions. Moreover, as a designated systemically important financial market utility (“SIFMU”),⁴ a failure or disruption to OCC could increase the risk of significant liquidity problems spreading among financial institutions or markets and thereby threaten the stability of the financial system in the United States. Given its designation as a SIFMU, OCC believes it is prudent to enhance its management of Security Incidents so that OCC’s own information and data systems remain protected against cyberattacks.

The proposed rule change would amend certain provisions in the Rules relating to Clearing Member cybersecurity obligations to address the occurrence of a Security Incident. Clearing Member cybersecurity obligations are currently set out in Rule 219, which addresses requirements related to a firm’s cybersecurity program. The proposed rule change would expand the scope of this Rule to incorporate provisions that address the occurrence of a Security Incident, as further described below. The current Clearing Member cybersecurity obligations in this Rule would remain unchanged.

The proposed changes would clearly describe Clearing Member obligations and OCC rights with respect to a Security Incident. The proposal would require Clearing Members to immediately notify OCC of a Security Incident. OCC’s notification and reporting requirements for Clearing Members are currently set forth in various provisions of the By-Laws and the Rules and require, among other things, that Clearing Members provide OCC with such documents and information as OCC may require from time to time.⁵ These existing notification and reporting requirements do not directly address Security Incidents. The proposal would amend OCC’s notification and reporting

⁴ OCC was designated as a SIFMU under Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010. 12 U.S.C. 5465(e)(1).

⁵ See Article V, Section 1, Interpretation and Policy .07 of the By-Laws and Rules 201(b), 215, 216, 217(b), 303, 306, 308 and 310(a)–(c).

requirements to adopt a specific requirement in the Rules that Clearing Members immediately notify OCC of a Security Incident and promptly confirm such notice in writing.

The proposed changes would also memorialize in the Rules OCC’s ability to take actions reasonably necessary to mitigate any effects of a Security Incident to its operations. OCC’s existing right to disconnect access, or to modify the scope and specifications of access, of a Clearing Member to OCC information and data systems is based in the Agreement for OCC Services, which sets forth the terms of various services that OCC may provide to Clearing Members.⁶ OCC maintains various contracts and forms, including the Agreement for OCC Services, that in conjunction with OCC’s By-Laws and Rules, establish and govern the relationship between OCC and each Clearing Member.⁷ Pursuant to the Agreement for OCC Services, OCC may terminate electronic access to particular OCC information and data systems, or modify the scope and specifications of such access, from time to time. Codifying this ability of OCC to take actions reasonably necessary to mitigate any effects to its operations in the Rules would centralize relevant information pertaining to cybersecurity in the Rules.

The proposal would further implement a standardized approach to evaluate and manage the cybersecurity risks that OCC may face due to a Security Incident. The proposal would set out new procedures that would require a Clearing Member to submit, upon OCC’s request, the Reconnection Attestation and Checklist after reporting a Security Incident, both as provided by OCC from time to time. The Rule is designed to provide OCC with a degree of flexibility in requesting the Reconnection Attestation and Checklist to consider circumstances where there may be no risk or threat to OCC, such as when a Security Incident is contained to a part of a Clearing Member’s business with no relevance to OCC or its markets. The Reconnection Attestation and Checklist are designed to enable OCC to determine whether the risk or threat to OCC has been mitigated sufficiently, including whether to resume connectivity to a Clearing Member if connectivity was disconnected or modified. OCC would detail specific representations and information required of Clearing Members in the proposed Reconnection

⁶ See Exchange Act Release No. 34–73577 (Nov. 12, 2014), 79 FR 68733 (Nov. 18, 2014) (File No. SR–OCC–2014–20).

⁷ *Id.*

Attestation and Checklist, included in Exhibit 3 to File No. SR-OCC-2023-003. OCC believes an attestation-based format coupled with a checklist would be most effective in ascertaining a Clearing Member's response to a Security Incident, including whether the Clearing Member has appropriate security requirements and carried out suitable remediation measures, to determine any potential threats to OCC's information and data systems. The forms filter the requested information and representations into a standardized format, which would better enable OCC to review and identify areas of interest, concern, or heightened risk in respect of a Security Incident. Standardizing the form and contents of submissions would also improve efficiency for Clearing Members and OCC by reducing the potential uncertainty and time required to demonstrate an acceptable response to a Security Incident, which would facilitate OCC's ability to evaluate the potential risk or threat posed by the Security Incident and facilitate the resumption of Clearing Member connectivity.

Proposed Rule Changes

The proposed rule change would amend certain provisions in the Rules relating to Clearing Member cybersecurity obligations to address the occurrence of a Security Incident. In addition to expanding the scope of existing Rules, the proposed changes would (i) require a Clearing Member to immediately notify OCC of a Security Incident; (ii) memorialize OCC's ability to take actions reasonably necessary to mitigate any effects to its operations; and (iii) require such Clearing Member to provide a Reconnection Attestation and Checklist.

Amended Cybersecurity Obligations Provisions

The proposed changes would expand the scope of existing Rule 219 to address the occurrence of a Security Incident. Existing Rule 219, titled "Cybersecurity Confirmation," currently includes requirements related to a firm's cybersecurity program and requires Clearing Members and applicants for clearing membership to submit a form, referred to as the "Cybersecurity Confirmation," that confirms the existence of a cybersecurity program. To broaden the scope, OCC proposes to retitle this Rule from "Cybersecurity Confirmation" to "Cybersecurity Obligations" to address Security Incidents and centralize cybersecurity-related provisions in one section of the Rules. For clarity, OCC also proposes to add a heading to each paragraph in this

Rule to summarize its content. OCC proposes to add the following headings: "Cybersecurity Confirmation Submission" to paragraph (a), which relates to the submission of the Cybersecurity Confirmation; "Representations in the Cybersecurity Confirmation" to paragraph (b), which relates to the representations in the Cybersecurity Confirmation; and "Execution of the Cybersecurity Confirmation" to paragraph (c), which relates to the execution of the Cybersecurity Confirmation. OCC also proposes a minor edit to replace "OCC" with "the Corporation" in paragraphs (a) and (b) for consistency. Additionally, under the proposed rule change, existing Rule 219 would be renumbered as Rule 213.⁸

Occurrence of a Security Incident

The proposed changes would address the occurrence of a Security Incident in the Rules by: (i) requiring a Clearing Member to immediately notify OCC of a Security Incident; (ii) memorializing OCC's ability to take actions reasonably necessary to mitigate any effects to its operations; and (iii) requiring such Clearing Member to provide a Reconnection Attestation and Checklist. Each of these proposed changes is described in greater detail below.

(i) Notification of a Security Incident

The proposed rule change would adopt a new paragraph (d) to amended Rule 213, titled "Occurrence of a Security Incident," to address the occurrence of a Security Incident. Proposed Rule 213(d) would define Security Incident as a cyber-related disruption or intrusion of the Clearing Member, including, but not limited to, any disruption or degradation of the normal operation of the Clearing Member's systems or any unauthorized entry into the Clearing Member's systems. Proposed Rule 213(d) would require a Clearing Member to immediately notify OCC if there has been a Security Incident or if a Security Incident is occurring and to promptly confirm such notice in writing.

(ii) Memorialization of OCC's Ability To Take Action

Proposed paragraph (d) to amended Rule 213 would also memorialize OCC's ability to take actions reasonably necessary to mitigate any effects to its

operations in the case of a Security Incident. The proposed language specifies that upon notice from a Clearing Member of a Security Incident, or if OCC has a reasonable basis to believe that a Security Incident has occurred, or is occurring, OCC may take actions reasonably necessary to mitigate any effects to its operations. Such actions would include the right to disconnect access, or to modify the scope and specifications of access, of the Clearing Member to OCC's information and data systems, consistent with the Agreement for OCC Services.

(iii) Requirement To Provide Reconnection Attestation and Checklist

The proposed rule change would adopt new paragraph (e) to amended Rule 213, titled "Procedures for Connecting Following a Security Incident," to incorporate procedures for Clearing Members to follow in the case of a Security Incident, including in order to resume connectivity to OCC. Proposed Rule 213(e) would require a Clearing Member to complete and submit, upon OCC's request, the Reconnection Attestation and Checklist after reporting a Security Incident, both as provided by OCC from time to time. The Reconnection Attestation and Checklist would facilitate OCC's ability to determine whether the risk or threat to OCC has been mitigated sufficiently, including whether to resume connectivity to a Clearing Member if connectivity was disconnected or modified. The proposed Reconnection Attestation and Checklist are set out in more detail below.

Each Reconnection Attestation would be required to be in writing on a form provided by OCC and signed by a designated senior executive of the Clearing Member who is authorized to attest to these matters, as specified in proposed Rule 213(e)(1). Each Reconnection Attestation would contain representations addressing the incident and attesting to certain security requirements. In addition, Clearing Members would be required to describe the Security Incident. OCC is proposing to require that the following representations be included in the Reconnection Attestation in proposed Rule 213(e)(1)(A) through (E):

First, the Reconnection Attestation would include a representation that the Clearing Member has provided full, complete and accurate information in response to all requests made by OCC regarding the Security Incident, including all requests contained in the Reconnection Checklist, on a good faith, best efforts basis.

⁸ OCC proposes to renumber existing Rule 219 to Rule 213 following on proposed changes to OCC's clearing membership standards, which includes removal of current rules 213 through 218. See Exchange Act Release No. 34-97150 (Mar. 15, 2023), 88 FR 17046 (Mar. 21, 2023) (File No. SR-OCC-2023-002).

Second, the Reconnection Attestation would include a representation that the Clearing Member has provided full, complete and accurate information regarding any OCC data or systems that were potentially compromised during the Security Incident, including any potential exposure of credentials used to access OCC's systems, and will immediately notify OCC if it later becomes aware of a previously undetected or unreported compromise of OCC data or systems during the Security Incident.

Third, the Reconnection Attestation would include a representation that the Clearing Member has determined whether the Security Incident resulted, directly or indirectly, from any controls that failed or were circumvented by its employees, contractors or agents ("Failed Controls"). The proposed language would further specify that the Clearing Member has communicated Failed Controls to OCC and is remediating or has remediated all Failed Controls.

Fourth, the Reconnection Attestation would include a representation that the Clearing Member has implemented, or will implement promptly, technical and operational changes, both preventative and detective, with the intent to prevent a recurrence of the Security Incident and has provided written summaries of such changes to OCC.

Fifth, the Reconnection Attestation would include a representation that the Clearing Member has complied and will continue to comply with all applicable laws in connection with its response to the Security Incident, including any notifications required to be provided to government agencies, OCC, and third parties.

Furthermore, each Reconnection Checklist would be required to be in writing on a form provided by OCC. A Clearing Member would describe its remediation efforts as part of the Reconnection Checklist, including relevant information related to the Security Incident and the Clearing Member's response thereto. To account for the evolving nature of Security Incidents, OCC proposes flexibility regarding the information requirements under proposed Rule 213(e)(2). Namely, the Reconnection Checklist may require information including, but not limited to, the following under this Rule:

- whether the disconnection was the result of a cybersecurity-related incident;
- the nature of the incident;
- the steps taken to contain the incident;
- the OCC data, if any, that was compromised during the incident;

- the OCC systems, if any, that were impacted during the incident;
- whether there was any risk of exposure of credentials used to access OCC systems, and if so, whether the credentials were reissued;
- the controls that were circumvented or failed that led to the incident occurring;
- the changes, preventative and detective, that were implemented to prevent a reoccurrence;
- details on how data integrity has been preserved and what data checks have been performed;⁹
- whether third-parties, including government agencies, have been notified; and
- any additional details relevant to reconnection.

Together, the required representations and information in the Reconnection Attestation and Checklist are designed to provide OCC with evidence related to a Clearing Member's response to a Security Incident, including whether the Clearing Member has appropriate security requirements and carried out suitable remediation measures, to enable OCC to better understand and manage Security Incidents. By requiring such representations and information from a Clearing Member, the Reconnection Attestation and Checklist would provide OCC with key information to make decisions about risks and threats, perform additional monitoring, and determine whether to resume connectivity to a Clearing Member, as applicable, in order to protect OCC's information and data systems.

(2) Statutory Basis

OCC believes the proposed rule changes are consistent with the requirements of the Act and the rules and regulations thereunder applicable to a registered clearing agency. In particular, OCC believes that the proposed rule changes are consistent with Section 17A(b)(3)(F) of the Act,¹⁰ and Rules 17Ad-22(e)(17)(i) and (e)(17)(ii), each promulgated under the Act,¹¹ for the reasons described below.

Section 17A(b)(3)(F) of the Act requires that the rules of OCC be designed to, among other things, promote the prompt and accurate clearance and settlement of securities transactions and assure the safeguarding

of securities and funds which are in the custody or control of the clearing agency or for which it is responsible.¹² As described above, the proposed amendments are designed to help OCC assess and take appropriate action to manage the cybersecurity risks that may be introduced to OCC's information and data systems due to a Security Incident. OCC proposes edits to existing Rule 219, including to titles and headings, to expand the scope to address the occurrence of a Security Incident. Existing Rule 219 would be renumbered as Rule 213 and would clearly set out the obligation of Clearing Members to notify OCC of a Security Incident and the right of OCC to take actions reasonably necessary to mitigate any effects to its operations, thereby centralizing relevant information pertaining to cybersecurity in the Rules and promoting transparency. Moreover, the proposal would implement a standardized approach to assess and manage the cybersecurity risks that OCC may face through its interconnections to Clearing Members. The proposal would include procedures for Clearing Members to follow in the case of a Security Incident, including in order to resume connectivity to OCC. The proposed changes would require a Clearing Member to submit, upon OCC's request, the Reconnection Attestation and Checklist after reporting a Security Incident, both as provided by OCC from time to time. OCC proposes to set forth specific representations and information required of Clearing Members in the Reconnection Attestation and Checklist, which are designed to provide OCC with evidence related to a Clearing Member's response to a Security Incident, including whether the Clearing Member has appropriate security requirements and carried out suitable remediation measures, to enable OCC to better understand and manage Security Incidents. The Reconnection Attestation and Checklist would provide OCC with key information to make decisions about risks and threats, perform additional monitoring, and determine whether to resume connectivity to a Clearing Member, as applicable, to protect OCC's information and data systems. Risks, threats, and potential vulnerabilities could impact OCC's ability to clear and settle securities transactions, or to safeguard the securities and funds which are in its custody or control, or for which it is responsible. Therefore, by enhancing its processes to mitigate these risks, OCC believes the proposal would promote the prompt and accurate

⁹ OCC notes that the Reconnection Checklist would specifically request details on how data integrity has been preserved and what data checks have been performed "prior to reconnecting to and sending/receiving data to/from OCC." See Exhibit 3 to File No. SR-OCC-2023-003.

¹⁰ 15 U.S.C. 78q-1(b)(3)(F).

¹¹ 17 CFR 240.17Ad-22(e)(17)(i) and (e)(17)(ii).

¹² 15 U.S.C. 78q-1(b)(3)(F).

clearance and settlement of securities transactions and assure the safeguarding of securities and funds which are in the custody or control of the clearing agency or for which it is responsible, consistent with the requirements of Section 17A(b)(3)(F) of the Act.¹³

Rule 17Ad-22(e)(17)(i) under the Act requires that each covered clearing agency establish, implement, maintain and enforce written policies and procedures reasonably designed to manage the covered clearing agency's operational risks by identifying the plausible sources of operational risk, both internal and external, and mitigating their impact through the use of appropriate systems, policies, procedures, and controls.¹⁴ The proposed Reconnection Attestation and Checklist would reduce the cybersecurity risks to OCC by requiring a Clearing Member to provide written representations addressing the incident and attesting to certain security requirements and an associated checklist describing remediation efforts. The proposed Reconnection Attestation and Checklist would filter the requested information and representations into a standardized format, which would better enable OCC to review and identify areas of interest, concern, or heightened risk in respect of a Security Incident. The representations and information in these forms would help OCC mitigate its exposure to cybersecurity risk and, thereby, decrease the operational risks to OCC. The proposed Reconnection Attestation and Checklist would identify to OCC potential sources of external operational risks that may be introduced through its interconnections to Clearing Members and enable OCC to mitigate these risks and possible impacts to OCC's operations. Based on this information, OCC would make a determination regarding the resumption of connectivity to a Clearing Member if connectivity was disconnected or modified. As a result, OCC believes the proposal is consistent with the requirements of Rule 17Ad-22(e)(17)(i) under the Act.¹⁵

Rule 17Ad-22(e)(17)(ii) under the Act requires that each covered clearing agency establish, implement, maintain and enforce written policies and procedures reasonably designed to manage the covered clearing agency's operational risks by ensuring, in part, that systems have a high degree of security, resiliency, and operational

reliability.¹⁶ The proposed Reconnection Attestation and Checklist would help enhance the security, resiliency, and operational reliability of OCC's information and data systems. Namely, these forms would help OCC determine whether to take action against a Clearing Member, including preventing the reconnection of a Clearing Member, that may pose an increased cyber risk to OCC by not having appropriate security requirements or taking suitable remediation measures. Clearing Members that have not adequately addressed Security Incidents may present increased risk to OCC. For example, weaknesses within a Clearing Member's environment could allow for exploitation by a malicious actor of the link between a Clearing Member and OCC. By better enabling OCC to identify these risks, the proposed rule change would allow OCC to more effectively secure its environment against potential vulnerabilities. The required representations and information in the Reconnection Attestation and Checklist would provide OCC with key information to make decisions about risks and threats, perform additional monitoring, and determine whether to resume connectivity to a Clearing Member, as applicable, to protect OCC's information and data systems. As a result, OCC believes the proposal would improve OCC's ability to ensure that its systems have a high degree of security, resiliency, and operational reliability, and, as such, is consistent with the requirements of Rule 17Ad-22(e)(17)(ii) under the Act.¹⁷

(B) Clearing Agency's Statement on Burden on Competition

Section 17A(b)(3)(I) of the Act¹⁸ requires that the rules of a clearing agency not impose any burden on competition not necessary or appropriate in furtherance of the purposes of the Act. OCC does not believe that the proposed rule changes would impose any burden on competition not necessary or appropriate in furtherance of the purposes of the Act. As discussed above, OCC proposes to amend certain provisions in the Rules relating to Clearing Member cybersecurity obligations to address the occurrence of a Security Incident. The proposed changes would (i) require a Clearing Member to immediately notify OCC of a Security Incident; (ii) memorialize OCC's ability to take actions reasonably

necessary to mitigate any effects to its operations; and (iii) require such Clearing Member to provide a Reconnection Attestation and Checklist. While the proposed changes would require Clearing Members to incur additional costs, including to complete and submit the Reconnection Attestation and Checklist, OCC does not believe the proposed changes would present an undue burden on Clearing Members. Clearing Members are already subject to the notification and reporting requirements in OCC's By-Laws and the Rules that require, among other things, that Clearing Members provide OCC with such documents and information as OCC may require from time to time.¹⁹ Standardizing the form and contents of the proposed submissions would reduce the potential uncertainty and time required to demonstrate an acceptable response to a Security Incident. Additionally, the proposed changes would not unfairly inhibit access to OCC's services or disadvantage or favor any particular user in relationship to another user. Such changes would apply to all Clearing Members consistently and thus would not provide any Clearing Member with a competitive advantage over any other Clearing Member as the requirements would be uniform. As described above, given OCC's position in the marketplace, OCC believes it is prudent to enhance its management of Security Incidents as detailed in the proposal, so that OCC's own information and data systems remain protected against cyberattacks. For the foregoing reasons, OCC believes that the proposed rule change is in the public interest, would be consistent with the requirements of the Act applicable to clearing agencies, and would not impact or impose a burden on competition.

(C) Clearing Agency's Statement on Comments on the Proposed Rule Change Received From Members, Participants or Others

Written comments were not and are not intended to be solicited with respect to the proposed rule change and none have been received.

III. Date of Effectiveness of the Proposed Rule Change and Timing for Commission Action

Within 45 days of the date of publication of this notice in the **Federal Register** or within such longer period up to 90 days (i) as the Commission may designate if it finds such longer period

¹³ *Id.*

¹⁴ 17 CFR 240.17Ad-22(e)(17)(i).

¹⁵ *Id.*

¹⁶ 17 CFR 240.17Ad-22(e)(17)(ii).

¹⁷ *Id.*

¹⁸ 15 U.S.C. 78q-1(b)(3)(I).

¹⁹ See Article V, Section 1, Interpretation and Policy .07 of the By-Laws and Rules 201(b), 215, 216, 217(b), 303, 306, 308 and 310(a)-(c).

to be appropriate and publishes its reasons for so finding or (ii) as to which the self-regulatory organization consents, the Commission will:

(A) by order approve or disapprove such proposed rule change, or

(B) institute proceedings to determine whether the proposed rule change should be disapproved.

The proposal shall not take effect until all regulatory actions required with respect to the proposal are completed.

IV. Solicitation of Comments

Interested persons are invited to submit written data, views and arguments concerning the foregoing, including whether the proposed rule change is consistent with the Act. Comments may be submitted by any of the following methods:

Electronic Comments

- Use the Commission's internet comment form (<http://www.sec.gov/rules/sro.shtml>); or
- Send an email to rule-comments@sec.gov. Please include File Number SR-OCC-2023-003 on the subject line.

Paper Comments

- Send paper comments in triplicate to Vanessa Countryman, Secretary, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549-1090.

All submissions should refer to File Number SR-OCC-2023-003. This file number should be included on the subject line if email is used. To help the Commission process and review your comments more efficiently, please use only one method. The Commission will post all comments on the Commission's internet website (<http://www.sec.gov/rules/sro.shtml>). Copies of the submission, all subsequent amendments, all written statements with respect to the proposed rule change that are filed with the Commission, and all written communications relating to the proposed rule change between the Commission and any person, other than those that may be withheld from the public in accordance with the provisions of 5 U.S.C. 552, will be available for website viewing and printing in the Commission's Public Reference Room, 100 F Street, NE, Washington, DC 20549, on official business days between the hours of 10:00 a.m. and 3:00 p.m. Copies of such filing also will be available for inspection and copying at the principal office of OCC and on OCC's website at <https://www.theocc.com/Company->

Information/Documents-and-Archives/By-Laws-and-Rules.

All comments received will be posted without change. Persons submitting comments are cautioned that we do not redact or edit personal identifying information from comment submissions. You should submit only information that you wish to make available publicly.

All submissions should refer to File Number SR-OCC-2023-003 and should be submitted on or before April 26, 2023.

For the Commission, by the Division of Trading and Markets, pursuant to delegated authority.²⁰

Sherry R. Haywood,

Assistant Secretary.

[FR Doc. 2023-07004 Filed 4-4-23; 8:45 am]

BILLING CODE 8011-01-P

SECURITIES AND EXCHANGE COMMISSION

[Release No. 34-97224; File No. SR-ICEEU-2023-009]

Self-Regulatory Organizations; ICE Clear Europe Limited; Notice of Filing of Proposed Rule Change Relating to Amendments of the Investment Management Procedures

March 30, 2023.

Pursuant to Section 19(b)(1) of the Securities Exchange Act of 1934 ("Act"),¹ and Rule 19b-4 thereunder,² notice is hereby given that on March 23, 2023, ICE Clear Europe Limited ("ICE Clear Europe" or the "Clearing House") filed with the Securities and Exchange Commission ("Commission") the proposed rule changes described in Items I, II and III below, which Items have been primarily prepared by ICE Clear Europe. The Commission is publishing this notice to solicit comments on the proposed rule change from interested persons.

I. Clearing Agency's Statement of the Terms of Substance of the Proposed Rule Change

ICE Clear Europe Limited ("ICE Clear Europe" or the "Clearing House") proposes to modify its Investment Management Procedures³ (the "Investment Management Procedures" or the "Procedures") to change the maximum maturities for certain

investments made with amounts held by the Clearing House as regulatory capital.

II. Clearing Agency's Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change

In its filing with the Commission, ICE Clear Europe included statements concerning the purpose of and basis for the proposed rule change and discussed any comments it received on the proposed rule change. The text of these statements may be examined at the places specified in Item IV below. ICE Clear Europe has prepared summaries, set forth in sections (A), (B), and (C) below, of the most significant aspects of such statements.

(A) *Clearing Agency's Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change*

(a) Purpose

ICE Clear Europe is proposing to amend the Investment Management Procedures in the Table of Authorised Investments and Concentration Limits for ICEU's Regulatory Capital (the "Table") to change the maximum maturity of certain investments in sovereign and government agency bonds. In particular, the maximum maturity on the purchase of U.S. Sovereign Bonds, UK Sovereign Bonds, EU Sovereign Bonds, U.S. Government Agency Bonds, UK Government Agency Bonds, and EU Government Agency Bonds would be amended from 90 days to 13 months. The amendments would align the maximum maturity for such investments with the existing maximum maturity for permitted investments in the same instrument that are made with cash provided by Clearing Members ("CMs") (e.g., as margin or guaranty fund contribution) and the Clearing House's own contribution to the guaranty fund. By extending the maximum maturity, ICE Clear Europe would have the flexibility to invest its regulatory capital in longer term sovereign and government bonds. ICE Clear Europe believes that such flexibility is important in light of current and expected market conditions, including to assist ICE Clear Europe in avoiding having to invest or reinvest in shorter duration instruments during potential periods of market volatility, such as those that may arise in connection with U.S. debt ceiling developments.

(b) Statutory Basis

ICE Clear Europe believes that the proposed amendments to the Investment Management Procedures are consistent with the requirements of

²⁰ 17 CFR 200.30-3(a)(12).

¹ 15 U.S.C. 78s(b)(1).

² 17 CFR 240.19b-4.

³ Capitalized terms used but not defined herein have the meanings specified in the ICE Clear Europe Clearing Rules and the Investment Management Procedures.

Section 17A of the Act⁴ and the regulations thereunder applicable to it. In particular, Section 17A(b)(3)(F) of the Act⁵ requires, among other things, that the rules of a clearing agency be designed to promote the prompt and accurate clearance and settlement of securities transactions and, to the extent applicable, derivative agreements, contracts, and transactions, the safeguarding of securities and funds in the custody or control of the clearing agency or for which it is responsible, and the protection of investors and the public interest.

The proposed changes to the Investment Management Procedures are designed to align the maximum maturity for certain investments made with ICE Clear Europe's regulatory capital with the maximum maturity for investments of other funds by the Clearing House (specifically, cash provided by Clearing Members and the Clearing House's own contribution to the guaranty fund). Although regulatory capital serves a different purpose from default resources, ICE Clear Europe believes that the same principles of capital preservation and maintaining high levels of liquidity are appropriate for all cash managed by the Clearing House. The current maximum maturities for investments in sovereign and government bonds for regulatory capital creates an unnecessary limitation compared to Clearing Member cash and the Clearing House guaranty fund contributions. The current limitation may subject regulatory capital investments to short-term volatility and reinvestment risk that could be avoided in appropriate cases through having the flexibility to invest in longer dated, but still high quality and liquid, instruments. ICE Clear Europe does not believe it is necessary for the maximum maturity for investments of its regulatory capital to be more restrictive than for its other investments of cash. ICE Clear Europe believes that, as with investments of Clearing Member cash and Clearing House guaranty fund contributions, investments in qualifying sovereign and agency bonds with an up-to 13 month maturity would nonetheless have acceptable credit, market and liquidity risks that can be managed by the Clearing House. Moreover, the Clearing House would then have the same tools and ability to manage its regulatory capital as it would its CM cash and Clearing House guaranty fund contributions. (In addition, the general investment consideration under the

existing Procedures that investments have a variety of maturity dates would continue to apply.) Having a consistent set of investment and maturity requirements would also simplify the Clearing House investment process. Accordingly, ICE Clear Europe believes that the Investment Management Procedures, as amended, are consistent with the safeguarding of funds and securities in the custody or control of the clearing agency or for which it is responsible. For the same reasons, the amendments are also consistent with the protection of investors and the public interest. As such, ICE Clear Europe believes the amendments are consistent with the requirements of Section 17A(b)(3)(F) of the Act.⁶

Rule 17A-22(e)(16) requires a covered clearing agency to "establish, implement, maintain and enforce written policies and procedures reasonably designed to, as applicable [. . .] safeguard its own and its participants' assets, minimize the risk of loss and delay in access to these assets, and invest such assets in instruments with minimal credit, market and liquidity risks."⁷ As discussed above, the amendments to the Investment Management Procedures are intended to align the maximum maturities for certain investments made with ICE Clear Europe's own regulatory capital with the maximum maturities for investments in the same assets when made with Clearing Member cash or the Clearing House's own contribution to the guaranty fund. ICE Clear Europe does not believe it is necessary to distinguish between the two types of investments in terms of maximum maturity. As revised, the Procedures will limit investment of Clearing House cash of all varieties to instruments with minimal credit, market and liquidity risks, consistent with the manner in which Clearing Member cash and Clearing House guaranty fund contributions are currently invested. As such, the revised Investment Management Procedures would continue to help enable the Clearing House to safeguard such assets and minimize the risk of loss and delay in access to such assets, consistent with the requirements of Rule 17Ad-22(e)(16).⁸

Rule 17Ad-22(e)(15) requires a covered clearing agency to "establish, implement, maintain and enforce written policies and procedures reasonably designed to, as applicable [. . .] hold liquid net assets funded by

equity [. . .] which [. . .] shall be of high quality and sufficiently liquid to allow the covered clearing agency to meet its current and projected operating expenses under a range of scenarios, including in adverse market conditions."⁹ As set forth above, ICE Clear Europe believes the revisions to the maximum maturity for investments of its own capital will result in investments in assets with minimal credit, market and liquidity risks, consistent with other investments made by the Clearing House. The current investment profile is conservative, allowing for investment only in the highest rated securities, and this would not be affected by the proposed changes. For similar reasons, ICE Clear Europe believes that under the revised Investment Management Procedures, such investments of its capital will be of sufficient high quality and liquidity to permit the Clearing House to meet its operating expenses, even in adverse market conditions. As a result, in ICE Clear Europe's view, the amendments are consistent with the requirements of Rule 17Ad-22(e)(15).¹⁰

(B) Clearing Agency's Statement on Burden on Competition

ICE Clear Europe does not believe the proposed amendments would have any impact, or impose any burden, on competition not necessary or appropriate in furtherance of the purposes of the Act. The changes are being proposed in order to update the Investment Management Procedures to align maturity requirements for investment of the Clearing House's capital. The amendments are not intended to impose new requirements on Clearing Members, and will not affect the investment of cash provided by Clearing Members. The terms of clearing are not otherwise changing. ICE Clear Europe does not believe that proposed amendments would adversely affect competition among Clearing Members or other market participants or affect the ability of market participants to access clearing generally. Therefore, ICE Clear Europe does not believe the proposed rule change imposes any burden on competition that is inappropriate in furtherance of the purposes of the Act.

(C) Clearing Agency's Statement on Comments on the Proposed Rule Change Received From Members, Participants or Others

Written comments relating to the proposed amendment has not been

⁴ 15 U.S.C. 78q-1.

⁵ 15 U.S.C. 78q-1(b)(3)(F).

⁶ 15 U.S.C. 78q-1(b)(3)(F).

⁷ 17 CFR 240.17Ad-22(e)(16).

⁸ 17 CFR 240.17Ad-22(e)(16).

⁹ 17 CFR 240.17Ad-22(e)(15)(B).

¹⁰ 17 CFR 240.17Ad-22(e)(15)(B).

solicited or received by ICE Clear Europe. ICE Clear Europe will notify the Commission of any comments received with respect to the proposed rule change.

III. Date of Effectiveness of the Proposed Rule Change and Timing for Commission Action

Within 45 days of the date of publication of this notice in the **Federal Register** or within such longer period up to 90 days (i) as the Commission may designate if it finds such longer period to be appropriate and publishes its reasons for so finding or (ii) as to which the self-regulatory organization consents, the Commission will:

- (A) by order approve or disapprove such proposed rule change, or
- (B) institute proceedings to determine whether the proposed rule change should be disapproved.

IV. Solicitation of Comments

Interested persons are invited to submit written data, views, and arguments concerning the foregoing, including whether the proposed rule change is consistent with the Act. Comments may be submitted by any of the following methods:

Electronic Comments

- Use the Commission's internet comment form (<http://www.sec.gov/rules/sro.shtml>) or
- Send an email to rule-comments@sec.gov. Please include File Number SR-ICEEU-2023-009 on the subject line.

Paper Comments

- Send paper comments in triplicate to Secretary, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549-1090. All submissions should refer to File Number SR-ICEEU-2023-009. This file number should be included on the subject line if email is used. To help the Commission process and review your comments more efficiently, please use only one method. The Commission will post all comments on the Commission's internet website (<http://www.sec.gov/rules/sro.shtml>). Copies of the submission, all subsequent amendments, all written statements with respect to the proposed rule change, that are filed with the Commission, and all written communications relating to the proposed rule change between the Commission and any person, other than those that may be withheld from the public in accordance with the provisions of 5 U.S.C. 552, will be available for website viewing and printing in the Commission's Public

Reference Room, 100 F Street NE, Washington, DC 20549, on official business days between the hours of 10:00 a.m. and 3:00 p.m. Copies of such filings will also be available for inspection and copying at the principal office of ICE Clear Europe and on ICE Clear Europe's website at <https://www.theice.com/clear-europe/regulation>.

All comments received will be posted without change. Persons submitting comments are cautioned that we do not redact or edit personal identifying information from comment submissions. You should submit only information that you wish to make available publicly. All submissions should refer to File Number SR-ICEEU-2023-009 and should be submitted on or before April 26, 2023.

For the Commission, by the Division of Trading and Markets, pursuant to delegated authority.¹¹

Sherry R. Haywood,
Assistant Secretary.

[FR Doc. 2023-07006 Filed 4-4-23; 8:45 am]

BILLING CODE 8011-01-P

DEPARTMENT OF STATE

[Public Notice 12036]

Listening Session on Modernizing the Columbia River Treaty Regime

ACTION: Notice of meeting.

SUMMARY: The Department of State will hold a virtual listening session, on April 19, 2023, to discuss the modernization of the Columbia River Treaty (CRT) regime.

DATES: The session will be held on Wednesday, April 19, 2023, from 8 p.m.–9:30 p.m. ET (5 p.m.–6:30 p.m. PT).

ADDRESSES: The session will be held virtually.

FOR FURTHER INFORMATION CONTACT: Office of Canadian Affairs, Department of State, (202) 647-2170, ColumbiaRiverTreaty@state.gov.

SUPPLEMENTARY INFORMATION: This listening session is part of the Department's public engagement on the modernization of the CRT regime. (Per 22 U.S.C. 2651a and 2656) The session is open to the public. To register, go to: https://statedept.zoomgov.com/webinar/register/WN_XKI6Hk8TRn-n8xOAnHPA-g. Requests for reasonable accommodation should be made to the email listed above, on or before April 9, 2023. The Department will consider

requests made after that date, but might not be able to accommodate them. More information about the meeting, including call-in information, can be found at <https://www.state.gov/virtual-listening-session-following-the-16th-round-of-negotiations-to-modernize-the-columbia-river-treaty-regime/> or by emailing the email address listed above. Questions can be submitted in advance at ColumbiaRiverTreaty@state.gov for consideration.

Authority: 22 U.S.C. 2651a, 2656; 5 U.S.C. 552.

Jennifer L. Savage,

Director, Office of Canadian Affairs,
Department of State.

[FR Doc. 2023-07000 Filed 4-4-23; 8:45 am]

BILLING CODE 4710-29-P

DEPARTMENT OF STATE

[Public Notice 11871]

Exchange Visitor Program

ACTION: Notice of Temporary Waiver and Modification of Certain Regulatory Requirements.

SUMMARY: In accordance with the General Provisions of the Exchange Visitor Program regulations, the Department's Assistant Secretary for Educational and Cultural Affairs waives and modifies certain regulatory requirements with respect to a temporary educational and cultural exchange program established pursuant to an arrangement between the Government of the United States of America and the Government of Ukraine. This arrangement allows the Department to extend Special Student Relief to eligible Ukrainian students in the United States on J-1 visas to help mitigate the adverse impact on them resulting from the full-scale Russian invasion of Ukraine that began on February 24, 2022.

DATES: This action was effective on August 18, 2022, and will remain in effect until October 23, 2023, unless the U.S. Government unilaterally ends the arrangement early or the U.S. Government and the Government of Ukraine together extend its termination date. The Department will publish a document in the **Federal Register** if the termination date is changed.

FOR FURTHER INFORMATION CONTACT: Nicole Elkon, Deputy Assistant Secretary, Private Sector Exchange at 2200 C Street NW, SA-5, 5th Floor, Washington, DC 20522 or via email at JExchanges@state.gov. or phone (202) 826-4364.

¹¹ 17 CFR 200.30-3(a)(12).

SUPPLEMENTARY INFORMATION: On February 24, 2022, Russian military forces invaded Ukraine, resulting in the destruction of infrastructure and the disruption of daily life. Many exchange visitors from Ukraine dependent upon financial support originating in their home country have limited or no access to funds. Others may have difficulty returning home. To ameliorate hardship arising from lack of financial support and to facilitate these students' continued studies in the United States, in accordance with the Exchange Visitor Program Regulations, located in 22 CFR part 62, the Department's Assistant Secretary for Educational and Cultural Affairs has waived and/or modified certain provisions in § 62.23 with respect to an educational and cultural exchange program established pursuant to an arrangement between the Government of the United States of America and the Government of Ukraine. The Department is establishing this temporary program to offer "Special Student Relief" to eligible Ukrainian exchange visitors in the College and University category. As described in detail below and with respect to Special Student Relief for eligible Ukrainian students, the Department temporarily waives and/or modifies the application of selected portions of the following sections of regulations governing the College and University Student category of the Exchange Visitor Program: Full Course of Study (§ 62.23(e)), Student Employment (§ 62.23(g), and Duration (§ 62.23(h)).

Individuals eligible for Special Student Relief, like those eligible for Temporary Protective Status (TPS), must have continuously resided in the United States since April 11, 2022. Special Student Relief with respect to program status and employment for J-1 Ukrainian students does not apply to Federal Work-Study jobs.

Regulations at § 62.23(e) enumerate the circumstances under which students (except student interns) are exempt from the "full course of study" requirement as defined in § 62.2. Because those circumstances do not include exigent circumstances such as war as an articulated exemption from the full course of study requirement, the Department temporarily waives § 62.23(e) for eligible Ukrainian students.

Regulations at § 62.23(g) enumerate the conditions that students (except student interns) must meet to engage in employment. With respect to Special Student Relief, the Department temporarily waives all subsections of § 62.23(g) except (g)(2)(i) and (iv). By retaining § 62.23(g)(2)(i), Ukrainian

students are required to remain in good academic standing at the post-secondary accredited academic institutions at which they are registered. By modifying § 62.23(g)(2)(iv), sponsors may grant advanced, written employment approval to last beyond the twelve months that the provision currently allows, *i.e.*, for the duration of the arrangement between the United States and Ukraine. Waiver and modification of these provisions allow eligible Ukrainian students to work on- or off-campus, for more than 20 hours a week, and for longer than twelve months.

Regulations at § 62.23(h) enumerate the conditions that exchange visitors must meet to retain their authorization to participate in the Exchange Visitor Program. For purposes of Special Student Relief, the Department modifies § 62.23(h)(1)(i)(A) to allow eligible Ukrainian students to pursue course work equivalent to half of the full course of study requirement as defined in § 62.2 and further explained in paragraph (e) of § 62.23. The Department similarly modifies § 62.23(h)(2)(i)(A) to allow eligible Ukrainian students to participate half-time in a prescribed course of study. In other words, degree-seeking students may limit their course work to half of their academic institutions' definition of a full-course of study. Similarly, non-degree-seeking students may reduce participation in their academic programs from full- to part-time.

The Department notes that the establishment of Special Student Relief does not alter the rules and requirements of accredited academic institutions. If, for example, an institution does not allow part-time participation in non-degree academic programs, students must negotiate flexible conditions with their institutions to overcome such rules and requirements. The temporary waiver and modification of Exchange Visitor Program regulations only address conditions that eligible Ukrainian exchange visitors must meet to be in status and comply with Exchange Visitor Program eligibility requirements.

Responsible Officers of academic institutions may authorize Special Student Relief for college and university students in J-1 status whose means of financial support from Ukraine has been disrupted, reduced, or eliminated due to the Russian invasion if they have continuously resided in the United States since April 11, 2022, and meet the reduced course load requirements set forth above. To authorize on-campus or off-campus employment for these students, Responsible Officers should update the students' records in the

Student and Exchange Visitor Information System (SEVIS) by notating the following text in the "Remarks" field: "Special Student Relief work authorization granted until October 19, 2023." To authorize a reduced course load due to such employment, Responsible Officers should also note the "Comment" field in the SEVIS record with the following text: "reduced course load authorized." Responsible Officers should monitor students at the start of each term to confirm that students seeking to reduce their course loads intend to work more than 20 hours a week or that students who availed themselves of reduced course loads intend to continue to work more than 20 hours a week.

If the arrangement between the United States and Ukraine is terminated early or extended, Responsible Officers should update the Remarks field accordingly. Exchange visitors participating according to the waived and/or modified provisions at the time the arrangement ends may continue their current employment and course load through the end of the academic term during which the arrangement ends.

Lee Satterfield,

Assistant Secretary, Bureau of Educational and Cultural Affairs, Department of State.

[FR Doc. 2023-07021 Filed 4-4-23; 8:45 am]

BILLING CODE 4710-05-P

DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

[Docket No. FAA-2023-0100]

Agency Information Collection Activities: Requests for Comments; Clearance of a Renewed Approval of Information Collection: Application for Employment With the Federal Aviation Administration

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Notice and request for comments.

SUMMARY: In accordance with the Paperwork Reduction Act of 1995, FAA invites public comments about our intention to request the Office of Management and Budget (OMB) approval to renew an information collection. The **Federal Register** notice with a 60-day comment period soliciting comments on the following collection of information was published on January 24, 2023. The collection involves an automated application process for employment with the Federal Aviation

Administration. Applicants access an online form that is presented with requests for certain information. The information collected is necessary to determine basic eligibility for employment and potential eligibility for Veteran's Preference, Veteran's Readjustment Act, and People with Disability appointments. In addition, there are specific occupation questions that assist the FAA Office of Human Resource Management (AHR) in determining candidates' qualifications in order that the best-qualified candidates are hired for the many FAA occupations.

DATES: Written comments should be submitted by May 5, 2023.

ADDRESSES: Written comments and recommendations for the proposed information collection should be sent within 30 days of publication of this notice to www.reginfo.gov/public/do/PRAMain. Find this particular information collection by selecting "Currently under 30-day Review—Open for Public Comments" or by using the search function.

FOR FURTHER INFORMATION CONTACT: Toni Main-Valentin by email at: toni.main-valentin@faa.gov; phone: 405-954-0870.

SUPPLEMENTARY INFORMATION:

Public Comments Invited: You are asked to comment on any aspect of this information collection, including (a) Whether the proposed collection of information is necessary for FAA's performance; (b) the accuracy of the estimated burden; (c) ways for FAA to enhance the quality, utility and clarity of the information collection; and (d) ways that the burden could be minimized without reducing the quality of the collected information.

OMB Control Number: 2120-0597.

Title: Application for Employment with the Federal Aviation Administration.

Form Numbers: Not applicable (electronic submission).

Type of Review: Renewal of an information collection.

Background:

The **Federal Register** notice with a 60-day comment period soliciting comments on the following collection of information was published on January 24, 2023 (88 FR 4280). Under the provisions of Public Law 104-50, the Federal Aviation Administration (FAA) is given the authority and the responsibility for developing and implementing its own personnel system without regard to most of the provisions of title 5, United States Code, exceptions being those concerning veteran's preference and various benefits.

The Office of Personnel Management (OPM) developed a suite of forms for use in automated employment processes: all under a single OMB approval. The FAA office of Human Resource Management, Human Resources (AHR) has the same OMB approval for its automated application for employment. By automating processes for employment application and the evaluation of candidates, AHR continues to markedly improve the service it provides to the public as well as its ability to locate and hire the best-qualified applicants. This automated process provides applicants the capability to receive on-line results immediately upon submitting their application questionnaires.

The Agency is requesting certain information necessary to determine basic eligibility for employment and potential eligibility for Veteran's Preference, Veteran's Readjustment Act, and People with Disability appointments. In addition, occupation specific questions assist AHR in determining candidates' qualifications in order that the best-qualified candidates are hired for the many FAA occupations. The system currently in use for this collection is the FAA Automated Vacancy Information Access Tool for Online Referral (AVIATOR). This system cannot be directly accessed. Applicants are transferred to the AVIATOR system from OPM's USAJOBS website during the application process.

Respondents: Over 180,000 U.S. citizens identified as applicants for employment with the Federal Aviation Administration.

Frequency: On occasion/as interested.

Estimated Average Burden per Response: 180,000 hours.

Approximately 180,000 respondents will complete an application form on an as needed basis. Based on this sample size, it will take the average applicant approximately 1 hour to read the instructions and complete the form.

Estimated Total Annual Burden: The estimated total burden is 180,000 hours annually.

Issued in Washington, DC, on March 31, 2023.

Alpha O Woodson-Smith,

Information Technology Project Manager, Finance and Management (AFN), Information and Technology Services (AIT), Enterprise Program Management Service (AEM-320).

[FR Doc. 2023-07062 Filed 4-4-23; 8:45 am]

BILLING CODE 4910-13-P

DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

Petition for Exemption; Summary of Petition Received; AMAC Aerospace Switzerland AG

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Notice of petition for exemption received; reopening of comment period.

SUMMARY: This notice contains a summary of a petition seeking relief from specified requirements of Federal Aviation Regulations. On February 14, 2023, the FAA published in the **Federal Register** a notice of petition for exemption received from AMAC Aerospace Switzerland AG, and requested public comments. The Association of Flight Attendants and the Air Line Pilots Association, International requested additional time to comment on the exemption proposal. The purpose of this notice is to reopen the comment period to improve the public's awareness of, and participation in, the FAA's exemption process. Neither publication of this notice nor the inclusion or omission of information in the summary is intended to affect the legal status of the petition or its final disposition.

DATES: Comments on this petition must identify the petition docket number and must be received on or before April 19, 2023.

ADDRESSES: Send comments identified by docket number FAA-2022-1802 using any of the following methods:

- *Federal eRulemaking Portal:* Go to <http://www.regulations.gov> and follow the online instructions for sending your comments electronically.

- *Mail:* Send comments to Docket Operations, M-30; U.S. Department of Transportation (DOT), 1200 New Jersey Avenue SE, Room W12-140, West Building Ground Floor, Washington, DC 20590-0001.

- *Hand Delivery or Courier:* Take comments to Docket Operations in Room W12-140 of the West Building Ground Floor at 1200 New Jersey Avenue SE, Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays.

- *Fax:* Fax comments to Docket Operations at 202-493-2251.

Privacy: In accordance with 5 U.S.C. 553(c), DOT solicits comments from the public to better inform its rulemaking process. DOT posts these comments, without edit, including any personal information the commenter provides, to <http://www.regulations.gov>, as described in the system of records

notice (DOT/ALL-14 FDMS), which can be reviewed at <http://www.dot.gov/privacy>.

Docket: Background documents or comments received may be read at <http://www.regulations.gov> at any time. Follow the online instructions for accessing the docket or go to the Docket Operations in Room W12-140 of the West Building Ground Floor at 1200 New Jersey Avenue SE, Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays.

FOR FURTHER INFORMATION CONTACT:

Deana Stedman, AIR-612, Federal Aviation Administration, 2200 South 216th Street, phone and fax 206-231-3187, email deana.stedman@faa.gov.

This notice is published pursuant to 14 CFR 11.85.

Issued in Washington, DC, on March 30, 2023.

James David Foltz,

Acting Manager, Strategic Policy Management, Policy and Innovation Division, Aircraft Certification Service.

Petition for Exemption

Docket No.: FAA-2022-1802.

Petitioner: AMAC Aerospace Switzerland AG.

Section(s) of 14 CFR Affected:

§§ 25.562(a), 25.785(b), 25.785(h)(2), 25.785(j), 25.791(a), 25.807(e), 25.811(d)(1), 25.812(b)(1)(i) and (ii), 25.813(c)(2)(ii), and 25.858.

Description of Relief Sought:

Petitioner is seeking relief from the listed design requirements in order to support a supplemental type certificate (STC) application for a Boeing Model 737-8 airplane. The proposed STC is for the installation of an executive-style interior with multiple rooms.

[FR Doc. 2023-07025 Filed 4-4-23; 8:45 am]

BILLING CODE 4910-13-P

DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

Notice of Opportunity for Public Comment on a Proposed Change of Airport Property Land Use From Aeronautical to Non-Aeronautical Use at Tulsa International Airport, Tulsa, OK

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Notice.

SUMMARY: The FAA is considering a request from the Tulsa Airport Improvement Trust to change approximately 241.72 acres, located on the east side of the airport bordered by North Mingo Road, 46th Street and

Mingo Valley Expressway, from aeronautical use to non-aeronautical use and to authorize the conversion of the airport property.

DATES: Comments must be received on or before May 5, 2023.

ADDRESSES: Send comments on this document to Mr. Glenn Boles, Federal Aviation Administration, Arkansas/Oklahoma Airports District Office Manager, 10101 Hillwood Parkway, Fort Worth, TX 76177. Email: Glenn.A.Boles@faa.gov.

FOR FURTHER INFORMATION CONTACT: Ms. Alexis Higgins, Chief Executive Officer of Tulsa Airports Improvement Trust, 7777 East Apache, Suite A217, Tulsa, OK 74115, telephone 918-838-5001; or Mr. Glenn Boles, Federal Aviation Administration, Arkansas/Oklahoma Airports District Office Manager, 10101 Hillwood Parkway, Fort Worth, TX 76177, telephone (817) 222-5639. Email: Glenn.A.Boles@faa.gov.

Documents reflecting this FAA action may be reviewed at the above locations.

SUPPLEMENTARY INFORMATION: The proposal consists of three parcels of land that were originally acquired under the following Federal grants: Airport Development Aid Program (ADAP) No. 6-40-0099-015 in 1978 and Airport Improvement Program (AIP) No. 3-40-0099-073-2009 in 2009.

The land comprising these parcels is outside the forecasted need for aviation development and is not needed for indirect or direct aeronautical use. The Airport wishes to develop this land for compatible non-aeronautical use. The Airport will retain ownership of this land and ensure the protection of part 77 surfaces and compatible land use. The income from the conversion of these parcels will benefit the aviation community by reinvestment in the airport.

Approval does not constitute a commitment by the FAA to financially assist in the conversion of the subject airport property nor a determination of eligibility for grant-in-aid funding from the FAA. The disposition of proceeds from the conversion of the airport property will be in accordance with FAA's Policy and Procedures Concerning the Use of Airport Revenue, published in the **Federal Register** on February 16, 1999. In accordance with section 47107(h) of title 49, United States Code, this notice is required to be published in the **Federal Register** 30 days before modifying the land-use assurance that requires the property to be used for an aeronautical purpose.

Issued in Fort Worth, TX.

D. Cameron Bryan,

Acting Director, Airports Division, FAA, Southwest Region.

[FR Doc. 2023-06997 Filed 4-4-23; 8:45 am]

BILLING CODE P

DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

[Summary Notice No. PE-2023-08]

Petition for Exemption; Summary of Petition Received; The Boeing Company

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Notice of petition for exemption received.

SUMMARY: This notice contains a summary of a petition seeking relief from specified requirements of Federal Aviation Regulations. The purpose of this notice is to improve the public's awareness of, and participation in, the FAA's exemption process. Neither publication of this notice nor the inclusion or omission of information in the summary is intended to affect the legal status of the petition or its final disposition.

DATES: Comments on this petition must identify the petition docket number and must be received on or before April 25, 2023.

ADDRESSES: Send comments identified by docket number FAA-2022-0920 using any of the following methods:

- *Federal eRulemaking Portal:* Go to <http://www.regulations.gov> and follow the online instructions for sending your comments electronically.
- *Mail:* Send comments to Docket Operations, M-30; U.S. Department of Transportation (DOT), 1200 New Jersey Avenue SE, Room W12-140, West Building Ground Floor, Washington, DC 20590-0001.

- *Hand Delivery or Courier:* Take comments to Docket Operations in Room W12-140 of the West Building Ground Floor at 1200 New Jersey Avenue SE, Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays.

- *Fax:* Fax comments to Docket Operations at 202-493-2251.

Privacy: In accordance with 5 U.S.C. 553(c), DOT solicits comments from the public to better inform its rulemaking process. DOT posts these comments, without edit, including any personal information the commenter provides, to <http://www.regulations.gov>, as described in the system of records

notice (DOT/ALL-14 FDMS), which can be reviewed at <http://www.dot.gov/privacy>.

Docket: Background documents or comments received may be read at <http://www.regulations.gov> at any time. Follow the online instructions for accessing the docket or go to the Docket Operations in Room W12-140 of the West Building Ground Floor at 1200 New Jersey Avenue SE, Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays.

FOR FURTHER INFORMATION CONTACT:

Deana Stedman, AIR-612, Federal Aviation Administration, 2200 South 216th Street, Des Moines, WA 98198, phone and fax 206-231-3187, email deana.stedman@faa.gov.

This notice is published pursuant to 14 CFR 11.85.

Issued in Washington, DC, on March 31, 2023.

James David Foltz,

Acting Manager, Strategic Policy Management, Policy and Innovation Division, Aircraft Certification Service.

Petition for Exemption

Docket No.: FAA-2022-0920.

Petitioner: The Boeing Company.

Section(s) of 14 CFR Affected:

§§ 25.901(c), 25.981(a)(3), 25.1309(b), (d)(1), and (d)(2).

Description of Relief Sought: The Boeing Company is seeking relief from 14 CFR 25.901(c) at amendment 25-46, 25.981(a)(3) at amendment 25-102, and 25.1309(b), (d)(1), and (d)(2) at amendment 25-41 for the Fuel Quantity Indication System (FQIS) wiring separation for the main fuel tanks. The relief sought will allow earlier planned type design changes to the center fuel tank FQIS fuselage wiring installation on Model 777-200 and -300 series airplanes prior to line number 562, to address the unsafe condition identified within airworthiness directive (AD) 2020-18-12.

[FR Doc. 2023-07112 Filed 4-4-23; 8:45 am]

BILLING CODE 4910-13-P

DEPARTMENT OF TRANSPORTATION

Federal Highway Administration

Federal Transit Administration

Supplemental Environmental Impact Statement for the Interstate Bridge Replacement Program

AGENCY: Federal Highway Administration (FHWA) and Federal Transit Administration (FTA), USDOT.

ACTION: Notice.

SUMMARY: The FHWA and FTA are issuing this notice to advise other Federal, State, and local agencies, Tribes, and the public that a Supplemental Environmental Impact Statement (SEIS) will be prepared in accordance with the National Environmental Policy Act (NEPA) for the Interstate Bridge Replacement (IBR) Program for proposed highway and high-capacity transit improvements between Portland, Oregon, and Vancouver, Washington, across the Columbia River in the Interstate 5 (I-5) corridor, including the interstate bridge replacement and addressing changes that have occurred since the I-5 Columbia River Crossing (CRC) Project's 2011 Record of Decision (ROD).

FOR FURTHER INFORMATION CONTACT:

For FHWA: Thomas Goldstein, PE, Federal Highway Administration, 530 Center Street NE, Suite 420, Salem, OR 97301; *Telephone:* (503) 316-2545.

For FTA: Jeff Horton, Federal Transit Administration, Region 10, 915 Second Avenue, Suite 3192, Seattle, WA 98174; *Telephone:* (206) 220-4463.

For the IBR Program (ODOT/WSDOT): Chris Regan, IBR Environmental Manager, Interstate Bridge Replacement Program, 500 East Broadway, Suite 200, Vancouver, WA 98660; *Telephone:* (360) 556-7135.

SUPPLEMENTARY INFORMATION: The FHWA and FTA, as Federal joint lead agencies, the Oregon Department of Transportation (ODOT), the Washington State Department of Transportation (WSDOT), Metro, Southwest Washington Regional Transportation Council (RTC), Tri-County Metropolitan Transportation District of Oregon (TriMet), and Clark County Public Transportation Benefit Area Authority (C-TRAN), as local joint lead agencies, intend to prepare a SEIS for the IBR Program for proposed highway and high-capacity transit improvements between Portland, Oregon, and Vancouver, Washington, across the Columbia River in the I-5 corridor. Federal cooperating agencies in the preparation of the SEIS will be the National Oceanic and Atmospheric Administration National Marine Fisheries Service, National Park Service, U.S. Army Corps of Engineers, U.S. Coast Guard (USCG), and U.S. Environmental Protection Agency. This analysis includes the interstate bridge replacement and addresses changes that have occurred since the 2011 CRC Project's ROD.

The IBR Program builds on previous studies conducted for the CRC Project between 2005 and 2013. As identified in the CRC Project's ROD, the Selected

Alternative (referred to as the Locally Preferred Alternative (LPA)) included: (1) two new bridges to replace the existing, functionally obsolete lift span bridges over the Columbia River; (2) improvements to seven I-5 interchanges (from south to north: Victory Boulevard, Marine Drive, Hayden Island, SR 14, Mill Plain Boulevard, Fourth Plain Boulevard and SR 500) and related enhancements to the local street network; (3) improvements to the existing I-5 mainline bridge over the North Portland Harbor; (4) bicycle and pedestrian improvements throughout the corridor, including a multi-use path that would allow users to travel from north Portland into downtown Vancouver and destinations farther north; (5) extension of light rail transit from the Expo Center in Portland to Clark College in Vancouver and associated transit improvements; and (6) transportation demand and system management measures, including the use of tolls subject to the authority of the Washington and Oregon Transportation Commissions. After the CRC Project's ROD was published, two NEPA re-evaluations were prepared: one to increase the height of the Columbia River bridges, and another to evaluate a phased construction plan. Neither of these re-evaluations found it necessary to prepare a SEIS.

In 2014, ODOT and WSDOT suspended the CRC Project due to lack of funding needed to complete design and construction. In 2019, ODOT and WSDOT reinitiated the CRC Project as the IBR Program. The needs identified in the CRC Purpose and Need statement are still pertinent to the IBR Program. As a result, the Purpose and Need statement for the IBR Program remains the same as in the CRC Project's 2011 Final EIS and ROD. On December 29, 2021, FHWA and FTA completed a re-evaluation concluding that, due to changes in the physical environment, community priorities, and regulations that have occurred since the 2011 CRC Project ROD, and potential design changes or refinements to the CRC Selected Alternative, the IBR Program may result in new or changed significant impacts that were not evaluated in the CRC Project's Final EIS and ROD. Therefore, pursuant to 23 CFR 771.130(a), FHWA and FTA have determined that a SEIS is necessary to identify and disclose any new significant impacts and mitigation associated with the IBR Program.

The CRC Project's EIS, ROD, and two re-evaluations, the Purpose and Need statement, and the 2021 re-evaluation for the IBR Program are available on the

IBR Program website at CRC Environmental Documentation.

The IBR Program SEIS will incorporate the CRC Project's NEPA analyses and other relevant information, as appropriate. The focus of the IBR Program SEIS will be limited to areas and issues that have resulted in changes to impacts and mitigation, including the following: proposed modifications to the bridge design, interchanges and lane configurations, and transit options; changes in existing conditions; safety considerations; and updated regulations/policies and permitting requirements, including USCG bridge clearance requirements. The IBR Program SEIS will provide updated information on the affected environment, environmental consequences, and mitigation measures for a modified LPA; coordination activities and input from Federal, State, and local agencies; consultation with Tribes; and public involvement. The SEIS will follow the same process and format as the CRC Project's EIS, except that in accordance with 23 CFR 771.130(d), additional scoping is not required. Per 40 CFR 1506.13, the SEIS will follow Council on Environmental Quality (CEQ) regulations that were in effect when the original Notice of Intent was published for the CRC Project on September 27, 2005.

The IBR Program has and will continue to offer extensive opportunities for public, agency, and tribal involvement, building on past NEPA compliance and associated outreach. The IBR Program has established a Community Advisory Group, Equity Advisory Group, and Executive Steering Group that meet regularly to provide input on changes since the CRC Project EIS and ROD, and to develop strategies for the IBR Program to address those changes.

Public involvement is a critical component of the IBR Program and will occur throughout the SEIS process in compliance with NEPA and other applicable environmental laws, Executive Orders, regulations, and policies. One or more public hearing(s) will be held during the public comment period following the publication of the Draft SEIS. The Draft SEIS will be made available for public, agency, and Tribe review and comment prior to the public hearing. After public review of the Draft SEIS, FHWA, FTA, ODOT, WSDOT, Metro, RTC, TriMet, and C-TRAN anticipate issuing a combined Final SEIS/ROD pursuant to 23 U.S.C. 139(n)(2) and 23 CFR 771.124.

Authority: 42 U.S.C. 4321 *et seq.*; 23 U.S.C. 139.

Issued on: March 28, 2023.

Ralph J. Rizzo,

FHWA Division Administrator, Olympia, WA.

Keith Lynch,

FHWA Division Administrator, Salem, OR.

Susan K. Fletcher,

Acting FTA Regional Administrator, Seattle, WA.

[FR Doc. 2023-07052 Filed 4-4-23; 8:45 am]

BILLING CODE 4910-RY-P

DEPARTMENT OF TRANSPORTATION

National Highway Traffic Safety Administration

[Docket No. NHTSA-2023-0016]

Request for Comments; CISS Expansion

AGENCY: National Highway Traffic Safety Administration (NHTSA), DOT.

ACTION: Notice and request for comments.

SUMMARY: On November 15, 2021, Congress passed the Bipartisan Infrastructure Law (BIL). Under § 24108(e) Congress authorizes the Secretary of Transportation to enhance the collection of crash data by upgrading the Crash Investigation Sampling System (CISS) to include—(1) additional program sites; (2) an expanded scope that includes all crash types; and (3) on-scene investigation protocols. The NHTSA is conducting a comprehensive review of the Crash Investigation Sampling System (CISS) sample design and data collection methods as part of a major effort to upgrade CISS. Users of CISS and other crash data may comment as to the future utility of current CISS, recommend ways to upgrade current CISS, and indicate their anticipated data needs. All comments should be submitted via Docket number NHTSA-2023-0016.

DATES: Comments must be submitted on or before June 5, 2023.

ADDRESSES: You may submit comments identified by the Docket No. NHTSA-2023-0016 through any of the following methods:

- *Electronic submissions:* Go to the Federal eRulemaking Portal at <http://www.regulations.gov>. Follow the online instructions for submitting comments.

- *Fax:* (202) 493-2251.

- *Mail or Hand Delivery:* Docket Management, U.S. Department of Transportation, 1200 New Jersey Avenue SE, West Building, Room W12-140, Washington, DC 20590, between 9 a.m. and 5 p.m., Monday through Friday, except on Federal holidays. To be sure someone is there to help you,

please call (202) 366-9322 before coming.

Instructions: All submissions must include the agency name and docket number for this notice. Note that all comments received will be posted without change to <http://www.regulations.gov>, including any personal information provided. Please see the Privacy Act heading below.

Privacy Act: Anyone can search the electronic form of all comments received into any of our dockets by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor union, etc.). You may review DOT's complete Privacy Act Statement in the **Federal Register** published on April 11, 2000 (65 FR 19477-78) or you may visit <https://www.transportation.gov/privacy>.

Docket: For access to the docket to read background documents or comments received, go to <http://www.regulations.gov> or the street address listed above. Follow the online instructions for accessing the dockets via internet.

FOR FURTHER INFORMATION CONTACT: For questions relating to the redesign effort, please contact Tina Morgan, National Center for Statistics and Analysis, NHTSA, telephone: (202) 366-9253, email: tina.morgan@dot.gov. She may also be reached at 1200 New Jersey Avenue SE, NSA-010, Washington, DC 20590.

SUPPLEMENTARY INFORMATION:

Title: Data Review for the upgrade of Crash Investigation Sampling System (CISS).

Background: NHTSA is undertaking an effort to upgrade the Crash Investigation Sampling System (CISS) by adding data collection sites, expanding the scope of crashes investigated and using on-scene investigation protocols.

CISS collects crash data on a nationally representative sample of crashes involving at least one passenger vehicle—cars, light trucks, sport utility vehicles, and vans—towed from the scene. CISS collects real-world crash data that identifies the primary factors related to crashes and their injury outcome. CISS data is used throughout the world by stakeholders, researchers, manufacturers, other Federal agencies, and safety advocates for making vehicles and highways safer. The data enables stakeholders to make informed regulatory, program, and policy decisions regarding vehicle design and traffic safety.

The CISS began implementation in 2015 and by 2018 was collecting crash

data from thirty-two (32) fully operational sites. The current scope of crashes in CISS is limited to crashes involving at least one passenger vehicle towed from the scene. There are very few crashes in CISS involving a non-motorist, motorcyclist or large vehicle. CISS investigates about 4,000 crashes annually making it sometimes difficult to identify new or emerging crash trends and containing an adequate number of rare crashes or crashes involving a non-motorist, motorcycle, large vehicle, or a vehicle with new technology for meaningful analysis. However, the original sample was designed to be flexible and scalable to accommodate different types of crashes and increase the number of data collection sites without redesigning the site sample. NHTSA plans to utilize these capabilities to increase the number of data collection sites and types of crashes included in CISS. These changes will increase the number of crashes investigated annually, reduce variance of key estimates, and expand the current scope of crashes.

The current CISS investigation process selects crashes to be investigated usually 3 to 7 days after the crash. Then crash technicians locate, visit, measure, and photograph the crash scene; locate, inspect, and photograph vehicles; conduct a telephone or personal interview in specific crashes with the involved individuals or surrogate (another person who can provide occupant or crash information, such as parents of a minor, or a parent or spouse for the deceased individual); and obtain and record injury information received from various medical data sources. From the time of the crash to the time of investigation, critical evidence from the scene can be destroyed, altered or removed, vehicles can be hard to locate or repaired, and people involved tend to forget information related to the crash. To obtain this critical information, on-scene or rapid response investigations protocols would be required. On-scene protocols involve crash investigators arriving at the scene of the crashes before the crash scene is cleared allowing investigators to collect critical evidence and interview drivers or witnesses while the crash is still fresh. Rapid response protocols are where crash investigators arrive at the scene of the crash 1–2 days after the crash.

NHTSA is pursuing data improvement initiatives that will enhance the amount of data collected and the quality of the data collected in CISS as authorized by BIL.

This effort includes the following major objectives:

- Add more data collection sites to increase the number of crashes collected and reduce the variance of estimates,
- Expand the scope of crashes investigated to collect real-world data for crashes involving other types of vehicles and non-motorists (pedestrian, pedalcyclist, etc.); and

- Utilize rapid response investigation protocols to collect data sooner than the current method to reduce the loss of critical information needed from the scene, vehicle and people involved.

In order to meet these objectives, NHTSA invites stakeholders to comment on the types of crashes to include in CISS, propose new data elements for new crash types, make suggestions on the improving timeliness of investigation protocols or notification and identification of crashes, and make any other suggestions they feel NHTSA should consider in an attempt to improve crash data collection.

For more information about CISS can be reviewed on NHTSA's websites: <https://www.nhtsa.gov/crash-data-systems/crash-investigation-sampling-system>. Current CISS data elements, coding instructions, and descriptive materials can be reviewed on NHTSA's website at: <https://crashstats.nhtsa.dot.gov/#!/PublicationList/110> and the CISS crash viewer at: <https://crashviewer.nhtsa.dot.gov/CISS/SearchIndex>.

Chou-Lin Chen,

Associate Administrator for the National Center for Statistics and Analysis.

[FR Doc. 2023–07071 Filed 4–4–23; 8:45 am]

BILLING CODE P

DEPARTMENT OF TRANSPORTATION

Pipeline and Hazardous Materials Safety Administration

[Docket No. PHMSA–2023–0009]

Safety of Underground Natural Gas Storage Public Meeting

AGENCY: Pipeline and Hazardous Materials Safety Administration (PHMSA), DOT.

ACTION: Notice of a public meeting.

SUMMARY: This notice announces that PHMSA will host a two-day public meeting titled: “Safety of Underground Natural Gas Storage Public Meeting” in Broomfield, Colorado. PHMSA is hosting this meeting as part of its core mission to improve safety through better communications between PHMSA and its stakeholders. The purpose of the public meeting is to share important safety information with the public and

industry, as well as gather input to inform future rulemaking decisions.

DATES: The public meeting and forum will be held May 16–17, 2023, from 8 a.m. to 4 p.m. (MT). Persons who wish to attend the meeting are asked to register no later than April 21, 2023. Individuals requiring accommodations, such as sign language interpretation or other aids, are asked to notify Kimberly Harrigan at K.Harrigan.ctr@dot.gov no later than April 21, 2023. For additional information, please see the **ADDRESSES** section of this notice.

ADDRESSES: The public meeting will be held at the Renaissance Boulder Flatiron Hotel, 500 Flatiron Boulevard, Broomfield, Colorado. The agenda and instructions on how to attend are available on the meeting website at <https://primis.phmsa.dot.gov/meetings/MtgHome.mtg?mtg=164>.

Presentations: Presentations from the public meeting will be available on the meeting website no later than five business days following the meeting.

Submitting Comments: Persons who wish to submit written comments may submit them to the docket in one of the following ways:

E-Gov Website: <https://www.regulations.gov>. This site allows the public to enter comments on any **Federal Register** notice issued by any agency. Follow the online instructions for submitting comments.

Fax: 1–202–493–2251—The Docket Management Facility, U.S. Department of Transportation will not issue confirmation notices for faxed comments.

Mail: Docket Management Facility, U.S. Department of Transportation, 1200 New Jersey Avenue SE, West Building: Room W12–140, Washington, DC 20590–0001

Hand Delivery: U.S. Department of Transportation, 1200 New Jersey Avenue SE, West Building: Room W12–140, Washington, DC 20590–0001, between 9:00 a.m. and 5:00 p.m. EST Monday through Friday, except federal holidays

Instructions: Identify Docket No. PHMSA–2023–0009 at the beginning of your comments. Internet users may submit comments at <https://www.regulations.gov>. If you submit your comments by mail or hand delivery, submit two copies. If you would like confirmation that PHMSA received your comments, please include a self-addressed stamped postcard that is labeled “Comments on PHMSA–2023–0009.” The docket clerk will date stamp the postcard prior to returning it to you via the U.S. mail.

Note: All comments received will be posted without edits to <https://www.regulations.gov>

www.regulations.gov, including any personal information provided. Please see the Privacy Act heading for more information. Anyone can use the site to search all comments by the name of the submitting individual or, if the comment was submitted on behalf of an association, business, labor union, etc., the name of the signing individual. Therefore, please review the complete U.S. Department of Transportation Privacy Act Statement in the **Federal Register** (65 FR 19477) or the Privacy Notice at <https://www.regulations.gov> before submitting comments.

Privacy Act Statement: In accordance with 5 U.S.C. 553(c), DOT solicits comments from the public regarding certain general notices. DOT posts these comments without edit, including any personal information the commenter provides, to <https://www.regulations.gov>, as described in the system of records notice (DOT/ALL-14 FDMS), which can be reviewed at <https://www.dot.gov/privacy>.

Confidential Business Information: Confidential Business Information (CBI) is commercial or financial information that is both customarily and actually treated as private by its owner. Under the Freedom of Information Act (5 U.S.C. 552), CBI is exempt from public disclosure. If your comments in response to this notice contain commercial or financial information that is customarily treated as private, that you actually treat as private, and that is relevant or responsive to this notice, it is important that you clearly designate the submitted comments as CBI. Pursuant to 49 CFR 190.343, you may ask PHMSA to provide confidential treatment to information you give to the Agency by taking the following steps: (1) mark each page of the original document submission containing CBI as "Confidential;" (2) send PHMSA a copy of the original document with the CBI deleted along with the original, unaltered document; and (3) explain why the information you are submitting is CBI. Submissions containing CBI should be sent to Catherine Washabaugh, DOT, PHMSA, 1200 New Jersey Avenue SE, Washington, DC 20590-0001. Also, submissions containing CBI can be emailed to Catherine Washabaugh by encrypted email at Catherine.Washabaugh@dot.gov. Any CBI PHMSA receives that is not specifically designated as CBI will be placed in the public docket.

Docket: For access to the docket or to read background documents or comments, go to

<https://www.regulations.gov>. Follow the online instructions for accessing the dockets. Alternatively, this information

is available by visiting DOT at 1200 New Jersey Avenue SE, West Building: Room W12-140, Washington, DC 20590-0001, between 9:00 a.m. and 5:00 p.m. ET Monday through Friday, except federal holidays.

FOR FURTHER INFORMATION CONTACT: Catherine Washabaugh by email at Catherine.Washabaugh@dot.gov, or phone (816) 728-7945.

SUPPLEMENTARY INFORMATION:

I. Background

The underground natural gas storage regulations have been in place for five years. Operators are now experienced in operating under these regulations. The meeting will bring federal and state regulators, emergency responders, industry, underground natural gas storage operators, and interested members of the public together to participate in understanding, enhancing, and shaping the future of underground natural gas storage safety. The meeting will provide a forum for discussion of multiple topics related to underground natural gas storage including: regulatory review, inspection processes, frequently asked question, jurisdictional coverage, incorporation by reference of American Petroleum Institute's Recommended Practices 1170 and 1171, general enforcement processes, common operator challenges, well annulus monitoring and exceedances, surface and subsurface safety valves, best practices, and lessons learned from incidents.

PHMSA's mission is to protect people and the environment by advancing the safe transportation of energy products and other hazardous materials that are essential to our daily lives. Part of this mission includes preventing the release of natural gas, which releases methane into the atmosphere. PHMSA is pursuing the DOT Strategic Goals of Safety, Economic Strength and Global Competitiveness, Equity, Climate & Sustainability, Transformation, and Organizational Excellence in effort to profile these goals during the public meeting.

Public Participation

The meeting will be open to the public. Members of the public who wish to attend are requested to register on the meeting website and include their names and organization affiliation (see **ADDRESSES**). PHMSA is committed to providing all participants with equal access to these meetings.

PHMSA is not always able to publish a notice in the **Federal Register** quickly enough to provide timely notification regarding last minute changes that

impact a previously announced meeting. Therefore, individuals should check the meeting website listed in the **ADDRESSES** section of this notice regarding any possible changes.

Issued in Washington, DC, on March 31, 2023, under authority delegated in 49 CFR 1.97.

Alan K. Mayberry,

Associate Administrator for Pipeline Safety.

[FR Doc. 2023-07072 Filed 4-4-23; 8:45 am]

BILLING CODE 4910-60-P

DEPARTMENT OF TRANSPORTATION

Pipeline and Hazardous Materials Safety Administration

[PHMSA-2019-0098]

Lithium Battery Air Safety Advisory Committee; Notice of Public Meeting

AGENCY: Pipeline and Hazardous Materials Safety Administration (PHMSA), U.S. Department of Transportation (DOT).

ACTION: Notice of public meeting.

SUMMARY: This notice announces a meeting of the Lithium Battery Air Safety Advisory Committee (Committee).

DATES: The meeting will be held on April 20, 2023, from 9 a.m. to 5:30 p.m. EDT. Requests to attend the meeting must be sent by April 5, 2023, to the point of contact identified in the **FOR FURTHER INFORMATION CONTACT** section. Persons requesting to speak during the meeting must submit a written copy of their remarks to DOT by April 5, 2023. Requests to submit written materials to be reviewed during the meeting must be received no later than April 5, 2023.

ADDRESSES: The meeting will be held at DOT Headquarters, West Building, 1200 New Jersey Avenue SE, Washington, DC 20590-0001. A remote participation option will also be available and the meeting will be webcast. Specific details on location and access to this meeting will be posted on the Committee website located at: <https://www.phmsa.dot.gov/hazmat/rulemakings/lithium-battery-safety-advisory-committee>. The E-Gov website is located at <https://www.regulations.gov>. Mailed written comments intended for the Committee should be sent to Docket Management Facility, U.S. Department of Transportation (DOT), 1200 New Jersey Avenue SE, West Building, Room W12-140, Washington, DC 20590-0001.

FOR FURTHER INFORMATION CONTACT: Steven Webb or Aaron Wiener, PHMSA, U.S. Department of Transportation.

Telephone: 202-366-8553. Email: *lithiumbatteryFACA@dot.gov*. Any committee-related request should be sent to the email address listed in this section.

SUPPLEMENTARY INFORMATION:

I. Background

The Lithium Battery Air Safety Advisory Committee was created under the Federal Advisory Committee Act (FACA, Pub. L. 92-463), in accordance with Section 333(d) of the FAA Reauthorization Act of 2018 (Pub. L. 115-254).

II. Agenda

The meeting agenda will address the following duties of the Committee as specifically outlined in Section 333(d) of the FAA Reauthorization Act of 2018:

(a) Facilitate communication among manufacturers of lithium batteries and products containing lithium batteries, air carriers, and the federal government.

(b) Discuss the effectiveness and the economic and social impacts of lithium battery transportation regulations.

(c) Provide the Secretary with information regarding new technologies and transportation safety practices.

(d) Provide a forum to discuss Departmental activities related to lithium battery transportation safety.

(e) Advise and recommend activities to improve the global enforcement of U.S. regulations and the International Civil Aviation Organization (ICAO) Technical Instructions relevant to air transportation of lithium batteries, and the effectiveness of those regulations.

(f) Provide a forum for feedback on potential positions to be taken by the U.S. at international forums.

(g) Guide activities to increase awareness of relevant requirements.

(h) Review methods to decrease the risk posed by undeclared hazardous materials.

A final agenda will be posted on the Lithium Battery Air Safety Advisory Committee website at least 15 days in advance of the meeting.

III. Public Participation

The meeting will be open to the public. DOT is committed to providing equal access to this meeting for all participants. If you need alternative formats or services because of a disability, such as sign language, interpretation, or other ancillary aids, please contact the person listed in the **FOR FURTHER INFORMATION CONTACT** section no later than April 5, 2023. To accommodate as many speakers as possible, time for each commenter may be limited. There will be five minutes allotted for oral comments from members of the public joining the meeting. Individuals wishing to reserve speaking time during the meeting must submit a request at the time of registration, as well as the name, address, and organizational affiliation of the proposed speaker. If the number of registrants requesting to make statements is greater than can be reasonably accommodated during the meeting, PHMSA may conduct a lottery to determine the speakers. Speakers are requested to submit a written copy of their prepared remarks for inclusion in the meeting records and for circulation to Lithium Battery Air Safety Advisory Committee members. All prepared remarks submitted on time will be accepted and considered as part of the record. Any member of the public may present a written statement to the committee at any time. Copies of the meeting minutes and committee presentations will be available on the Lithium Battery Air Safety Advisory Committee website. Presentations will also be posted on the E-Gov website in docket number [PHMSA-2019-0098], within 30 days following the meeting.

Written comments: Persons who wish to submit written comments on the meetings may submit them to docket [PHMSA-2019-0098] in the following ways:

1. *E-Gov Website:* This site allows the public to enter comments on any **Federal Register** notice issued by any agency.

2. *Mail:* Dockets Management System; U.S. Department of Transportation,

Dockets Operations, M-30, Ground Floor, Room W12-140, 1200 New Jersey Avenue SE, Washington, DC 20590-0001.

Instructions: Identify the docket number [PHMSA-2019-0098] at the beginning of your comments. Note that all comments received will be posted without change to the E-Gov website, including any personal information provided. Anyone can search the electronic form of all comments received into any of our dockets by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor union, etc.). Therefore, consider reviewing DOT's complete Privacy Act Statement in the **Federal Register** published on April 11, 2000, (65 FR 19477), or view the Privacy Notice on the E-Gov website before submitting comments.

Docket: For docket access or to read background documents or comments, go to the E-Gov website at any time or visit the DOT dockets facility listed in the **ADDRESSES** category, between 9:00 a.m. and 5:00 p.m., Monday through Friday, except federal holidays.

If you wish to receive confirmation of receipt of your written comments, please include a self-addressed, stamped postcard with the following statement: "Comments on [PHMSA-2019-0098]." The docket clerk will date stamp the postcard prior to returning it to you via U.S. mail.

Privacy Act Statement

DOT may solicit comments from the public regarding certain general notices. DOT posts these comments, without edit, including any personal information the commenter provides, to the E-Gov website, as described in the system of records notice (DOT/ALL-14 FDMS).

Issued in Washington, DC, on March 31, 2023.

William S. Schoonover,

Associate Administrator for Hazardous Materials Safety, Pipeline and Hazardous Materials Safety Administration.

[FR Doc. 2023-07102 Filed 4-4-23; 8:45 am]

BILLING CODE 4910-9X-P



FEDERAL REGISTER

Vol. 88

Wednesday,

No. 65

April 5, 2023

Part II

Securities and Exchange Commission

17 CFR Parts 232, 240, 242, et al.

Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents; Proposed Rule

SECURITIES AND EXCHANGE COMMISSION

17 CFR Parts 232, 240, 242 and 249

[Release No. 34–97142; File No. S7–06–23]

RIN 3235–AN15

Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents

AGENCY: Securities and Exchange Commission.

ACTION: Proposed rule.

SUMMARY: The Securities and Exchange Commission (“Commission”) is proposing a new rule and form and amendments to existing recordkeeping rules to require broker-dealers, clearing agencies, major security-based swap participants, the Municipal Securities Rulemaking Board, national securities associations, national securities exchanges, security-based swap data repositories, security-based swap dealers, and transfer agents to address cybersecurity risks through policies and procedures, immediate notification to the Commission of the occurrence of a significant cybersecurity incident and, as applicable, reporting detailed information to the Commission about a significant cybersecurity incident, and public disclosures that would improve transparency with respect to cybersecurity risks and significant cybersecurity incidents. In addition, the Commission is proposing amendments to existing clearing agency exemption orders to require the retention of records that would need to be made under the proposed cybersecurity requirements. Finally, the Commission is proposing amendments to address the potential availability to security-based swap dealers and major security-based swap participants of substituted compliance in connection with those requirements.

DATES: Comments should be received on or before June 5, 2023.

ADDRESSES: Comments may be submitted by any of the following methods:

Electronic Comments

- Use the Commission’s internet comment form (<https://www.sec.gov/rules/submitcomments.htm>); or
- Send an email to rule-comments@sec.gov. Please include File Number S7–06–23 on the subject line.

Paper Comments

- Send paper comments to Secretary, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549–1090.

All submissions should refer to File Number S7–06–23. The file number should be included on the subject line if email is used. To help the Commission process and review your comments more efficiently, please use only one method of submission. The Commission will post all comments on the Commission’s website (<https://www.sec.gov/rules/proposed.shtml>). Comments are also available for website viewing and printing in the Commission’s Public Reference Room, 100 F Street NE, Washington, DC 20549, on official business days between the hours of 10 a.m. and 3 p.m. Operating conditions may limit access to the Commission’s Public Reference Room. All comments received will be posted without change; the Commission does not edit personal identifying information from submissions. You should submit only information that you wish to make available publicly.

Studies, memoranda, or other substantive items may be added by the Commission or staff to the comment file during this rulemaking. A notification of the inclusion in the comment file of any such materials will be made available on the Commission’s website. To ensure direct electronic receipt of such notifications, sign up through the “Stay Connected” option at www.sec.gov to receive notifications by email.

FOR FURTHER INFORMATION CONTACT: Randall W. Roy, Deputy Associate Director and Nina Kostyukovsky, Special Counsel, Office of Broker-Dealer Finances (with respect to the proposed cybersecurity rule and form and the aspects of the proposal unique to broker-dealers); Matthew Lee, Assistant Director and Stephanie Park, Senior Special Counsel, Office of Clearance and Settlement (with respect to aspects of the proposal unique to clearing agencies and security-based swap data repositories); John Guidroz, Assistant Director and Russell Mancuso, Special Counsel, Office of Derivatives Policy (with respect to aspects of the proposal unique to major security-based swap participants and security-based swap dealers); Michael E. Coe, Assistant Director and Leah Mesfin, Special Counsel, Office of Market Supervision (with respect to aspects of the proposal unique to national securities associations and national securities exchanges); Moshe Rothman, Assistant Director, Office of Clearance and Settlement (with respect to aspects of

the proposal unique to transfer agents) at (202) 551–5500, Division of Trading and Markets; and Dave Sanchez, Director, Adam Wendell, Deputy Director, and Adam Allongamento, Special Counsel, Office of Municipal Securities (with respect to aspects of the proposal unique to the Municipal Securities Rulemaking Board) at (202) 551–5680, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549–7010.

SUPPLEMENTARY INFORMATION: The Commission is proposing to add the following new rule and form under the Securities Exchange Act of 1934 (“Exchange Act”): (1) 17 CFR 242.10 (“Rule 10”); and (2) 17 CFR 249.642 (“Form SCIR”). The Commission also is proposing related amendments to the following rules: (1) 17 CFR 232.101; (2) 17 CFR 240.3a71–6; (3) 17 CFR 240.17a–4; (4) 17 CFR 240.17Ad–7; (5) 17 CFR 240.18a–6; and (6) 17 CFR 240.18a–10. Further, the Commission is proposing to amend certain orders that exempt clearing agencies from registration.

Commission reference	CFR citation (17 CFR)
Regulation S–T	§ 232.101
Rule 3a71–6	§ 240.3a71–6
Rule 17a–4	§ 240.17a–4
Rule 17Ad–7	§ 240.17Ad–7
Rule 18a–6	§ 240.18a–6
Rule 18a–10	§ 240.18a–10
Rule 10	§ 242.10
Form SCIR	§ 249.624

Table of Contents

- I. Introduction
 - A. Cybersecurity Risk Poses a Threat the U.S. Securities Markets
 - 1. In General
 - 2. Critical Operations of Market Entities Are Exposed to Cybersecurity Risk
 - B. Overview of the Proposed Cybersecurity Requirements
- II. Discussion of Proposed Cybersecurity Rule
 - A. Definitions
 - 1. “Covered Entity”
 - 2. “Cybersecurity Incident”
 - 3. “Significant Cybersecurity Incident”
 - 4. “Cybersecurity Threat”
 - 5. “Cybersecurity Vulnerability”
 - 6. “Cybersecurity Risk”
 - 7. “Information”
 - 8. “Information Systems”
 - 9. “Personal Information”
 - 10. Request for Comment
 - B. Proposed Requirements for Covered Entities
 - 1. Cybersecurity Risk Management Policies and Procedures
 - 2. Notification and Reporting of Significant Cybersecurity Incidents
 - 3. Disclosure of Cybersecurity Risks and Incidents
 - 4. Filing Parts I and II of Proposed Form SCIR in EDGAR Using a Structured Data Language

5. Recordkeeping
- C. Proposed Requirements for Non-Covered Broker-Dealers
1. Cybersecurity Policies and Procedures, Annual Review, Notification, and Recordkeeping
2. Request for Comment
- D. Cross-Border Application of the Proposed Cybersecurity Requirements to SBS Entities
1. Background on the Cross-Border Application of Title VII Requirements
2. Proposed Entity-Level Treatment
3. Availability of Substituted Compliance
- E. Amendments to Rule 18a–10
1. Proposal
2. Request for Comment
- F. Market Entities Subject to Regulation SCI, Regulation S–P, Regulation ATS, and Regulation S–ID
1. Discussion
2. Request for Comment
- G. Cybersecurity Risk Related to Crypto Assets
- III. General Request for Comment
- IV. Economic Analysis
- A. Introduction
- B. Broad Economic Considerations
- C. Baseline
1. Cybersecurity Risks and Current Relevant Regulations
2. Market Structure
- D. Benefits and Costs of Proposed Rule 10, Form SCIR, and Rule Amendments
1. Benefits and Costs of the Proposals to the U.S. Securities Markets
2. Policies and Procedures and Annual Review Requirements for Covered Entities
3. Regulatory Reporting of Cybersecurity Incidents by Covered Entities
4. Public Disclosure of Cybersecurity Risks and Significant Cybersecurity Incidents
5. Record Preservation and Maintenance by Covered Entities
6. Policies and Procedures, Annual Review, Immediate Notification of Significant Cybersecurity Incidents, and Record Preservation Requirements for Non-Covered Broker-Dealers
7. Substituted Compliance for Non-U.S. SBS Entities
- E. Effects on Efficiency, Competition, and Capital Formation
- F. Reasonable Alternatives
1. Alternatives to the Policies and Procedures Requirements of Proposed Rule 10
2. Alternatives to the Requirements of Proposed Form SCIR and Related Notification and Disclosure Requirements of Proposed Rule 10
3. General Request for Comment
- V. Paperwork Reduction Act Analysis
- A. Summary of Collections of Information
1. Proposed Rule 10
2. Form SCIR
3. Rules 17a–4, 17ad–7, 18a–6 and Clearing Agency Exemption Orders
4. Substituted Compliance (Rule 3a71–6)
- B. Proposed Use of Information
- C. Respondents
1. Broker-Dealers
2. Clearing Agencies
3. The MSRB
4. National Securities Exchanges and National Securities Associations
5. SBS Entities
6. SBSDRs
7. Transfer Agents
- D. Total Initial and Annual Reporting Burdens
1. Proposed Rule 10
2. Form SCIR
3. Rules 17a–4, 17ad–7, 18a–6, and Clearing Agency Exemption Orders (and Existing Rules 13n–7 and 17a–1)
4. Substituted Compliance (Rule 3a71–6)
- E. Collection of Information is Mandatory
- F. Confidentiality of Responses to Collection of Information
- G. Retention Period for Recordkeeping Requirements
- H. Request for Comment
- VI. Initial Regulatory Flexibility Act Analysis
- A. Reasons for, and Objectives of, Proposed Action
1. Proposed Rule 10 and Parts I and II of Proposed Form SCIR
2. Rules 17a–4, 17ad–7, 18a–6 and Clearing Agency Exemption Orders
- B. Legal Basis
- C. Small Entities Subject to Proposed Rule, Form SCIR, and Recordkeeping Rule Amendments
1. Broker-Dealers
2. Clearing Agencies
3. The MSRB
4. National Securities Exchanges and National Securities Associations
5. SBS Entities
6. SBSDRs
7. Transfer Agents
- D. Reporting, Recordkeeping, and Other Compliance Requirements
1. Proposed Rule 10 and Parts I and II of Proposed Form SCIR
2. Rules 17a–4, 17ad–7, and 18a–6
- E. Duplicative, Overlapping, or Conflicting Federal Rules
1. Proposed Rule 10 and Parts I and II of Proposed Form SCIR
2. Rules 17a–4, 17ad–7, 18a–6 and Clearing Agency Exemption Orders
- F. Significant Alternatives
1. Broker-Dealers
2. Clearing Agencies
3. The MSRB
4. National Securities Exchanges and National Securities Associations
5. SBS Entities
6. SBSDRs
7. Transfer Agents
- G. Request for Comment
- VII. Small Business Regulatory Enforcement Fairness Act
- VIII. Statutory Authority

I. Introduction

A. Cybersecurity Risk Poses a Threat to the U.S. Securities Markets

1. In General

Cybersecurity risk has been described as “an effect of uncertainty on or within information and technology.”¹ This risk

¹ See the National Institute of Standards and Technology (“NIST”), U.S. Department of Commerce, *Computer Security Resource Center Glossary*, available at <https://csrc.nist.gov/glossary> (“NIST Glossary”) (definition of “cybersecurity risk”). The NIST Glossary consists of terms and

can lead to “the loss of confidentiality, integrity, or availability of information, data, or information (or control) systems and [thereby to] potential adverse impacts to organizational operations (*i.e.*, mission, functions, image, or reputation) and assets, individuals, other organizations, and the Nation.”² The U.S. Financial Stability Oversight Counsel (“FSOC”) in its 2021 annual report stated that a destabilizing cybersecurity incident could potentially threaten the stability of the U.S. financial system through at least three channels:

- First, the incident could disrupt a key financial service or utility for which there is little or no substitute. This could include attacks on central banks; exchanges; sovereign and subsovereign creditors, including U.S. state and local governments; custodian banks; payment clearing and settlement systems; or other firms or services that lack substitutes or are sole service providers.
- Second, the incident could compromise the integrity of critical

definitions extracted verbatim from NIST’s cybersecurity and privacy-related publications (*i.e.*, Federal Information Processing Standards (FIPS), NIST Special Publications (SPs), and NIST Internal/Interagency Reports (IRs)) and from the Committee on National Security Systems (CNSS) Instruction CNSSI–4009. The NIST Glossary may be expanded to include relevant terms in external or supplemental sources, such as applicable laws and regulations. The Cybersecurity Enhancement Act of 2014 (“CEA”) updated the role of NIST to include identifying and developing cybersecurity risk frameworks for voluntary use by critical infrastructure owners and operators. The CEA required NIST to identify “a prioritized, flexible, repeatable, performance based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks.” See 15 U.S.C. 272(e)(1)(A)(iii). In response, NIST has published the *Framework for Improving Critical Infrastructure Cybersecurity* (“NIST Framework”). See also NIST, *Integrating Cybersecurity and Enterprise Risk Management (ERM)* (Oct. 2020), available at <https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8286.pdf> (“All types of organizations, from corporations to federal agencies, face a broad array of risks. For federal agencies, the Office of Management and Budget (OMB) Circular A–11 defines risk as ‘the effect of uncertainty on objectives’. The effect of uncertainty on enterprise mission and business objectives may then be considered an ‘enterprise risk’ that must be similarly managed. . . . Cybersecurity risk is an important type of risk for any enterprise.”) (footnotes omitted).

² See NIST Glossary (definition of “cybersecurity risk”). See also The Board of the International Organization of Securities Commissions (“IOSCO”), *Cyber Security in Securities Markets—An International Perspective* (Apr. 2016), available at <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf> (“IOSCO Cybersecurity Report”) (“In essence, cyber risk refers to the potential negative outcomes associated with cyber attacks. In turn, cyber attacks can be defined as attempts to compromise the confidentiality, integrity and availability of computer data or systems.”) (footnote omitted).

data. Accurate and usable information is critical to the stable functioning of financial firms and the system; if such data is corrupted on a sufficiently large scale, it could disrupt the functioning of the system. The loss of such data also has privacy implications for consumers and could lead to identity theft and fraud, which in turn could result in a loss of confidence.

- Third, a cybersecurity incident that causes a loss of confidence among a broad set of customers or market participants could cause customers or participants to question the safety or liquidity of their assets or transactions, and lead to significant withdrawal of assets or activity.³

The U.S. securities markets are part of the *Financial Services Sector*, one of the sixteen critical infrastructure sectors “whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.”⁴ These markets are over \$100 trillion in total size, and more than a trillion dollars’ worth of transactions flow through them each day. For example, the market capitalization of the U.S. equities market was valued at \$49 trillion as of the first quarter of 2022,⁵ and as of May 2022, the average daily trading dollar volume in the U.S. equities market was \$659 billion.⁶ The market capitalization of the U.S. fixed income market was valued at \$52.9 trillion as of the fourth quarter of 2021,⁷ and as of May 2022, the average daily trading dollar volume in the U.S. fixed income market was \$897.8 billion.⁸

³ FSOC, *Annual Report (2021)*, at 168, available at <https://home.treasury.gov/system/files/261/FSOC2021AnnualReport.pdf> (“FSOC 2021 Annual Report”).

⁴ Cybersecurity and Infrastructure Security Agency (“CISA”), U.S. Department of Homeland Security, *Critical Infrastructure Sectors*, available at <https://www.cisa.gov/critical-infrastructure-sectors>. See also Presidential Policy Directive—Critical Infrastructure Security and Resilience, Presidential Policy Directive, PPD–21 (Feb. 12 2013).

⁵ See Securities Industry and Financial Markets Association (“SIFMA”), *Research Quarterly: Equities* (Apr. 27, 2022), available at <https://www.sifma.org/resources/research/research-quarterly-equities/>.

⁶ See SIFMA, *US Equity and Related Statistics* (June 1, 2022), available at <https://www.sifma.org/resources/research/us-equity-and-related-securities-statistics/>.

⁷ See SIFMA, *Research Quarterly: Fixed Income—Outstanding* (Mar. 14, 2022), available at <https://www.sifma.org/resources/research/research-quarterly-fixed-income-outstanding/>.

⁸ See SIFMA, *US Fixed Income Securities Statistics* (June 9, 2022), available at <https://www.sifma.org/resources/research/us-fixed-income-securities-statistics/>.

The sizes of these markets are indicative of the central role they play in the U.S. economy in terms of the flow of capital, including the savings of individual investors who are increasingly relying on them to, for example, build wealth to fund their retirement, purchase a home, or pay for college for themselves or their family. Therefore, it is critically important to the U.S. economy, investors, and capital formation that the U.S. securities markets function in a fair, orderly, and efficient manner.⁹

The fair, orderly, and efficient operation of the U.S. securities markets depends on different types of entities performing various functions to support, among other things, disseminating market information, underwriting securities issuances, making markets in securities, trading securities, providing liquidity to the securities markets, executing securities transactions, clearing and settling securities transactions, financing securities transactions, recording and transferring securities ownership, maintaining custody of securities, paying dividends and interest on securities, repaying principal on securities investments, supervising regulated market participants, and monitoring market activities. Collectively, these functions are performed by entities regulated by the Commission: broker-dealers, broker-dealers that operate an alternative trading system (“ATS”), clearing agencies, major security-based swap participants (“MSBSPs”), the Municipal Securities Rulemaking Board (“MSRB”), national securities associations, national securities exchanges, security-based swap data repositories (“SBSDRs”), security-based swap dealers (“SBSDs” or collectively with MSBSPs, “SBS Entities”), and transfer agents (collectively, “Market Entities”).¹⁰

To perform their functions, Market Entities rely on an array of electronic information, communication, and computer systems (or similar systems) (“information systems”) and networks of interconnected information systems. While Market Entities have long relied on information systems to perform their various functions, the acceleration of technical innovation in recent years has exponentially expanded the role these systems play in the U.S. securities

markets.¹¹ This expansion has been driven by the greater efficiencies and lower costs that can be achieved through the use of information systems.¹² It also has been driven by newer entrants (financial technology (Fintech) firms) that have developed business models that rely heavily on information systems (e.g., applications on mobile devices) to provide services to investors and other participants in the securities markets and more established Market Entities adopting the use of similar technologies.¹³ The COVID–19 pandemic also has contributed to the greater reliance on information systems.¹⁴

¹¹ See, e.g., Bank of International Settlements, Erik Feyen, Jon Frost, Leonardo Gambacorta, Harish Natarajan, and Mathew Saal, *Fintech and the digital transformation of financial services: implications for market structure and public policy*, BIS Papers No. 117 (July 2021), available at <https://www.bis.org/publ/bppdf/bispap117.pdf> (“BIS Papers 117”) (“Significant technology advances have taken place in two key areas that have contributed to the current wave of technology-based finance:” Increased connectivity . . . [and] Low-cost computing and data storage . . .”).

¹² *Id.* (“Technology has reduced the costs of, and need for, much of the traditional physical infrastructure that drove fixed costs for the direct financial services provider . . . Financial intermediaries can reduce marginal costs through technology-enabled automation and ‘straight through’ processing, which are accelerating with the expanded use of data and [artificial intelligence]-based processes. Digital innovation can also help to overcome spatial (geographical) barriers, and even to bridge differences across legal jurisdictions . . .”). See also United Nations, Office for Disaster Risk Reduction, Constantine Toregas and Joost Santos, *Cybersecurity and its cascading effect on societal systems* (2019), available at <https://www.undrr.org/publication/cybersecurity-and-its-cascading-effect-societal-systems> (“Cybersecurity and its Cascading Effect on Societal Systems”) (“Modern society has benefited from the additional efficiency achieved by improving the coordination across interdependent systems using information technology (IT) solutions. IT systems have significantly contributed to enhancing the speed of communication and reducing geographic barriers across consumers and producers, leading to a more efficient and cost-effective exchange of products and services across an economy.”).

¹³ BIS Papers 117 (“Internet and mobile technology have rapidly increased the ability to transfer information and interact remotely, both between businesses and directly to the consumer. Through mobile and smartphones, which are near-ubiquitous, technology has increased access to, and the efficiency of, direct delivery channels and promises lower-cost, tailored financial services . . . Incumbents large and small are embracing digital transformation across the value chain to compete with fintechs and big techs. Competitive pressure on traditional financial institutions may force even those that are lagging to transform or risk erosion of their customer base, income, and margins.”).

¹⁴ *Id.* (“The COVID–19 pandemic has accelerated the digital transformation. In particular, the need for digital connectivity to replace physical interactions between consumers and providers, and in the processes that produce financial services, will be even more important as economies, financial services providers, businesses and individuals navigate the pandemic and the eventual post-COVID–19 world.”). See also McKinsey & Company, *How Covid–19 has pushed companies*

⁹ The Commission’s tripartite mission is to: (1) protect investors; (2) maintain, fair, orderly, and efficient markets; and (3) facilitate capital formation. See, e.g., Commission, *Our Goals*, available at <https://www.sec.gov/our-goals>.

¹⁰ Currently, there are no MSBSPs registered with the Commission.

This increased reliance on information systems by Market Entities has caused a corresponding increase in their cybersecurity risk.¹⁵ This risk can be caused by the actions of external threat actors, including organized or individual threat actors seeking financial gain, nation states conducting espionage operations, or individuals engaging in protest, acting on grudges or personal offenses, or seeking thrills.¹⁶

over the technology tipping point—and transformed business forever (Oct. 5, 2020), available at <https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever/> (noting that due to the COVID-19 pandemic, “companies have accelerated the digitization of their customer and supply-chain interactions and of their internal operations by three to four years [and] the share of digital or digitally enhanced products in their portfolios has accelerated by a shocking seven years”).

¹⁵ See, e.g., Financial Services Information Sharing and Analysis Center (“FS-ISAC”), *Navigating Cyber 2022* (Mar. 2022), available at www.fsisac.com/navigatingcyber2022-report (detailing cyber threats that emerged in 2021 and predictions for 2022); Danny Brando, Antonis Kotidis, Anna Kovner, Michael Lee, and Stacey L. Schreft, *Implications of Cyber Risk for Financial Stability*, FEDS Notes, Washington: Board of Governors of the Federal Reserve System (May 12, 2022), available at <https://doi.org/10.17016/2380-7172.3077> (“Implications of Cyber Risk for Financial Stability”) (“Cyber risk in the financial system has grown over time as the system has become more digitized, as evidenced by the increase in cyber incidents. That growth has brought to light unique features of cyber risk and the potentially greater scope for cyber events to affect financial stability.”); United States Government Accountability Office (“GAO”), *Critical Infrastructure Protection: Treasury Needs to Improve Tracking of Financial Sector Cybersecurity Risk Mitigation Efforts*, GAO-20-631 (Sept. 2020), available at <https://www.gao.gov/assets/gao-20-631.pdf> (“GAO Cybersecurity Report”) (“The federal government has long identified the financial services sector as a critical component of the nation’s infrastructure. The sector includes commercial banks, securities brokers and dealers, and providers of the key financial systems and services that support these functions. Altogether, the sector holds about \$108 trillion in assets and faces a variety of cybersecurity-related risks. Key risks include (1) an increase in access to financial data through information technology service providers and supply chain partners; (2) a growth in sophistication of malware—software meant to do harm—and (3) an increase in interconnectivity via networks, the cloud, and mobile applications.”); Cybersecurity and its Cascading Effect on Societal Systems (“Nonetheless, IT dependence has also exposed critical infrastructure and industry systems to a myriad of cyber security risks, ranging from accidental causes, technological glitches, to malevolent willful attacks.”).

¹⁶ See, e.g., Verizon, *Data Breach Investigations Report* (2022) available at <https://www.verizon.com/business/resources/Tba/reports/dbir/2022-data-breach-investigations-report-dbir.pdf> (“Verizon DBIR”) (finding that 73% of the data breaches analyzed in the report were caused by external actors). The Verizon DBIR is an annual report that analyzes cyber security incidents (defined as a security event that compromises the integrity, confidentiality or availability of an information asset) and breaches (defined as an incident that results in the confirmed disclosure—

Internal threat actors (e.g., disgruntled employees or employees seeking financial gain) also can be sources of cybersecurity risk.¹⁷ Threat actors may target Market Entities because they handle financial assets or proprietary information about financial assets and transactions.¹⁸ In addition to threat actors, errors of employees, service providers, or business partners can create cybersecurity risk (e.g., mistakenly exposing confidential or personal information by, for example, sending it through an unencrypted email to unintended recipients).¹⁹

Another factor increasing the cybersecurity risk to Market Entities is the growing sophistication of the tactics, techniques, and procedures employed by threat actors.²⁰ This trend is further

not just potential exposure—of data to an unauthorized party). To perform the analysis, data about the cybersecurity incidents included in the report are catalogued using the Vocabulary for Event Recording and Incident Sharing (VERIS). VERIS is a set of metrics designed to provide a common language for describing security incidents in a structured and repeatable manner. More information about VERIS is available at: <http://veriscommunity.net/index.html>. See also Microsoft, *Microsoft Digital Defense Report* (Oct. 2021), available at <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFli> (“Microsoft Report”) (“The last year has been marked by significant historic geopolitical events and unforeseen challenges that have changed the way organizations approach daily operations. During this time, nation state actors have largely maintained their operations at a consistent pace while creating new tactics and techniques to evade detection and increase the scale of their attacks”).

¹⁷ See, e.g., Verizon DBIR (finding that 18% of the data breaches analyzed in the report were caused by internal actors). *But see id.* (“Internal sources accounted for the fewest number of incidents (18 percent), trailing those of external origin by a ratio of four to one. The relative infrequency of data breaches attributed to insiders may be surprising to some. It is widely believed and commonly reported that insider incidents outnumber those caused by other sources. While certainly true for the broad range of security incidents, our caseload showed otherwise for incidents resulting in data compromise. This finding, of course, should be considered in light of the fact that insiders are adept at keeping their activities secret.”).

¹⁸ See, e.g., GAO Cybersecurity Report (“The financial services sector faces significant risks due to its reliance on sophisticated technologies and information systems, as well as the potential monetary gain and economic disruption that can occur by attacking the sector”); IOSCO Cybersecurity Report (“[T]he financial sector is one of the prime targets of cyber attacks. It is easy to understand why: the sector is ‘where the money is’ and it can represent a nation or be a symbol of capitalism for some politically motivated activists.”).

¹⁹ See Verizon DBIR (finding that error (defined as anything done (or left undone) incorrectly or inadvertently) as one of action types leading to cybersecurity incidents and breaches).

²⁰ See, e.g., Bank of England, *CBEST Intelligence-Led Testing: Understanding Cyber Threat Intelligence Operations* (Version 2.0), available at <https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/understanding-cyber-threat-intelligence-operations.pdf> (“Bank of England CBEST Report”)

exacerbated by the ability of threat actors to purchase tools to engage in cyber-crime.²¹ Threat actors employ a number of tactics to cause harmful cybersecurity incidents.²² One tactic is the use of malicious software (“malware”) that is uploaded into a computer system and used by threat actors to compromise the confidentiality of information stored or operations performed (e.g., monitoring key strokes) on the system or the integrity or availability of the system (e.g., command and control attacks where a threat actor is able to infiltrate a system to install malware to enable it to remotely send commands to infected devices).²³ There are a number of different forms of malware, including adware, botnets, rootkit, spyware, Trojans, viruses, and worms.²⁴

(“The threat actor community, once dominated by amateur hackers, has expanded to include a broad range of professional threat actors, all of whom are strongly motivated, organised and funded. They include: state-sponsored organisations stealing military, government and commercial intellectual property; organised criminal gangs committing theft, fraud and money laundering which they perceive as low risk and high return; non-profit hacktivists and for-profit mercenary organisations attempting to disrupt or destroy their own or their client’s perceived enemies.”); Microsoft Report (“Sophisticated cybercriminals are also still working for governments conducting espionage and training in the new battlefield”).

²¹ See, e.g., Microsoft Report (“Through our investigations of online organized crime networks, frontline investigations of customer attacks, security and attack research, nation state threat tracking, and security tool development, we continue to see the cybercrime supply chain consolidate and mature. It used to be that cybercriminals had to develop all the technology for their attacks. Today they rely on a mature supply chain, where specialists create cybercrime kits and services that other actors buy and incorporate into their campaigns. With the increased demand for these services, an economy of specialized services has surfaced, and threat actors are increasing automation to drive down their costs and increase scale.”).

²² See, e.g., Financial Industry Regulatory Authority (“FINRA”), *Common Cybersecurity Threats*, available at: www.finra.org/rules-guidance/guidance/common-cybersecurity-threats (“FINRA Common Cybersecurity Threats”) (summarizing common cybersecurity threats faced by broker-dealers to include phishing, imposter websites, malware, ransomware, distributed denial-of-service attacks, and vendor breaches, among others).

²³ See CISA, *Malware Tip Card*, available at https://www.cisa.gov/sites/default/files/publications/Malware_1.pdf (“CISA Malware Tip Card”) (“Malware, short for ‘malicious software,’ includes any software (such as a virus, Trojan, or spyware) that is installed on your computer or mobile device. The software is then used, usually covertly, to compromise the integrity of your device. Most commonly, malware is designed to give attackers access to your infected computer. That access may allow others to monitor and control your online activity or steal your personal information or other sensitive data.”).

²⁴ See, e.g., CISA Malware Tip Card (“Adware [is] a type of software that downloads or displays unwanted ads when a user is online or redirects search requests to certain advertising websites. Botnets [are] networks of computers infected by

Continued

A second tactic is a variation of malware known as “ransomware.”²⁵ In this scheme, the threat actor encrypts the victim’s data making it unusable and then demands payment to decrypt it.²⁶ Ransomware schemes have become more prevalent with the widespread adoption and use of crypto assets.²⁷ It is a common tactic used against the financial sector.²⁸ Commission staff has observed that this tactic has increasingly

malware and controlled remotely by cybercriminals, usually for financial gain or to launch attacks on websites or networks. Many botnets are designed to harvest data, such as passwords, Social Security numbers, credit card numbers, and other personal information . . . Rootkit [is] a type of malware that opens a permanent “back door” into a computer system. Once installed, a rootkit will allow additional viruses to infect a computer as various hackers find the vulnerable computer exposed and compromise it. Spyware [is] a type of malware that quietly gathers a user’s sensitive information (including browsing and computing habits) and reports it to unauthorized third parties. Trojan [is] a type of malware that disguises itself as a normal file to trick a user into downloading it in order to gain unauthorized access to a computer. Virus [is] a program that spreads by first infecting files or the system areas of a computer or network router’s hard drive and then making copies of itself. Some viruses are harmless, others may damage data files, and some may destroy files entirely. Worm [is] a type of malware that replicates itself over and over within a computer.”).

²⁵ See CISA, Ransomware 101, available at <https://www.cisa.gov/stopransomware/ransomware-101> (“Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid. In recent years, ransomware incidents have become increasingly prevalent among the Nation’s state, local, tribal, and territorial (SLTT) government entities and critical infrastructure organizations.”).

²⁶ See, e.g., Federal Bureau of Investigation (“FBI”), *Internet Crime Report (2021)*, available at https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf (“FBI Internet Crime Report”) (“Ransomware is a type of malicious software, or malware, that encrypts data on a computer, making it unusable. A malicious cyber criminal holds the data hostage until the ransom is paid. If the ransom is not paid, the victim’s data remains unavailable. Cyber criminals may also pressure victims to pay the ransom by threatening to destroy the victim’s data or to release it to the public.”).

²⁷ See, e.g., Institute for Security and Technology, *Combating Ransomware: A Comprehensive Framework For Action: Key Recommendations from the Ransomware Task Force* (Apr. 2021), available at <https://securityandtechnology.org/ransomware-taskforce/report> (“The explosion of ransomware as a lucrative criminal enterprise has been closely tied to the rise of Bitcoin and other cryptocurrencies, which use distributed ledgers, such as blockchain, to track transactions.”).

²⁸ See, e.g., FBI Internet Crime Report (stating that it received 649 complaints that indicated organizations in the sixteen U.S. critical infrastructure sectors were victims of a ransomware attack, with the financial sector being the source of the second largest number of complaints).

been employed against certain Market Entities.²⁹

Another group of tactics are various social engineering schemes. In a social engineering attack, the threat actor uses social skills to convince an individual to provide access or information that can be used to access an information system.³⁰ “Phishing” is a variation of a social engineering attack in which an email is used to convince an individual to provide information (e.g., personal or account information or log-in credentials) that can be used to gain unauthorized access to an information system.³¹ Threat actors also use websites to perform phishing attacks.³² “Spear phishing” is a variation of phishing that targets a specific individual or group.³³ “Vishing” and

²⁹ See, Office of Compliance, Inspections and Examinations (now the Division of Examinations (“EXAMS”)), Commission, Risk Alert, *Cybersecurity: Ransomware Alert* (July 10, 2020), available at <https://www.sec.gov/files/Risk%20Alert%20-%20Ransomware.pdf> (“EXAMS Ransomware Risk Alert”) (observing an apparent increase in sophistication of ransomware attacks on Commission registrants, including broker-dealers). Any staff statements represent the views of the staff. They are not a rule, regulation, or statement of the Commission. Furthermore, the Commission has neither approved nor disapproved their content. These staff statements, like all staff statements, have no legal force or effect: they do not alter or amend applicable law; and they create no new or additional obligations for any person.

³⁰ See, e.g., CISA, *Security Tip (ST04-014)—Avoiding Social Engineering and Phishing Attacks*, available at <https://www.cisa.gov/uscert/ncas/tips/ST04-014> (“CISA Security Tip (ST04-014)”).

³¹ See, e.g., CISA Security Tip (ST04-014); Microsoft Report (“Phishing is the most common type of malicious email observed in our threat signals. These emails are designed to trick an individual into sharing sensitive information, such as usernames and passwords, with an attacker. To do this, attackers will craft emails using a variety of themes, such as productivity tools, password resets, or other notifications with a sense of urgency to lure a user to click on a link.”).

³² See, e.g., Microsoft Report (“The phishing web pages used in these attacks may utilize malicious domains, such as those purchased and operated by the attacker, or compromised domains, where the attacker abuses a vulnerability in a legitimate website to host malicious content. The phishing sites frequently copy well-known, legitimate login pages, such as Office 365 or Google, to trick users into inputting their credentials. Once the user inputs their credentials, they will often be redirected to a legitimate final site—such as the real Office 365 login page—leaving the user unaware that actors have obtained their credentials. Meanwhile, the entered credentials are stored or sent to the attacker for later abuse or sale.”).

³³ See, e.g., U.S. Office of the Director of National Intelligence, *Spear Phishing and Common Cyber Attacks*, available at https://www.dni.gov/files/NCSC/documents/campaign/Counterintelligence_Tips_Spearphishing.pdf (“ODNI Spear Phishing Alert”) (“A spear phishing attack is an attempt to acquire sensitive information or access to a computer system by sending counterfeit messages that appear to be legitimate. ‘Spear phishing’ is a type of phishing campaign that targets a specific person or group and often will include information known to be of interest to the target, such as current events or financial documents. Like other social

“smishing” are variations of social engineering that use phone communications or text messages, respectively, for this purpose.³⁴ These social engineering tactics also are used to deceive the recipient of an electronic communication (e.g., an email or text message) to open a link or attachment in the communication that uploads malware on to the recipient’s information systems.³⁵

In addition to malware and social engineering, threat actors may try to circumvent or thwart the information system’s logical security mechanisms (i.e., to “hack” the system).³⁶ There are many variations of hacking.³⁷ One tactic is a “brute force” attack in which the threat actor attempts to determine an unknown value (e.g., log-in credentials) using an automated process that tries a large number of possible values.³⁸ The Commission staff has observed that a variation of this tactic has increasingly been employed by threat actors against certain Market Entities to access their customers’ accounts.³⁹ The ability of

engineering attacks, spear phishing takes advantage of our most basic human traits, such as a desire to be helpful, provide a positive response to those in authority, a desire to respond positively to someone who shares similar tastes or views, or simple curiosity about contemporary news and events.”).

³⁴ See, e.g., CISA Security Tip (ST04-014).

³⁵ See, e.g., ODNI Spear Phishing Alert (“The goal of spear phishing is to acquire sensitive information such as usernames, passwords, and other personal information. When a link in a phishing email is opened, it may open a malicious site, which could download unwanted information onto a user’s computer. When the user opens an attachment, malicious software may run which could compromise the security posture of the host. Once a connection is established, the attacker is able to initiate actions that could compromise the integrity of your computer, the network it resides on, and data.”).

³⁶ See Verizon DBIR (definition of “hacking”); see also NIST Glossary (defining a “hacker” as an “unauthorized user who attempts to or gains access to an information system”).

³⁷ See, e.g., Web Application Security Consortium, *WASC Threat Classification: Version 2.00* (1/1/2010), available at https://projects.webappsec.org/f/WASC-TC-v2_0.pdf (“WASC Classification Report”).

³⁸ See, e.g., WASC Classification Report (“The most common type of a brute force attack in web applications is an attack against log-in credentials. Since users need to remember passwords, they often select easy to memorize words or phrases as passwords, making a brute force attack using a dictionary useful. Such an attack attempting to log-in to a system using a large list of words and phrases as potential passwords is often called a ‘word list attack’ or a ‘dictionary attack.’”).

³⁹ See EXAMS, Commission, Risk Alert, *Cybersecurity: Safeguarding Client Accounts against Credential Compromise* (Sept. 15, 2020), available at <https://www.sec.gov/files/Risk%20Alert%20-%20Credential%20Compromise.pdf> (“EXAMS Safeguarding Client Accounts Risk Alert”) (“The Office of Compliance Inspections and Examinations (‘OCIE’) has observed in recent examinations an increase in the number of cyberattacks against SEC-registered investment advisers (‘advisers’) and brokers and dealers (‘broker-

threat actors to hack into information systems can be facilitated by vulnerabilities in information systems, including for example the software run on the systems.⁴⁰

Threat actors also cause harmful cybersecurity incidents through denial-of-service (“DoS”) attacks.⁴¹ This type of attack may involve botnets or compromised servers sending “junk” data or messages to an information system that a Market Entity uses to provide services to investors, market participants, or other Market Entities causing the system to fail or be unable to process operations in a timely manner. DoS attacks are a commonly used tactic.⁴²

The tactics, techniques, and procedures employed by threat actors

dealers,’ and together with advisers, ‘registrants’ or ‘firms’) using credential stuffing. Credential stuffing is an automated attack on web-based user accounts as well as direct network login account credentials. Cyber attackers obtain lists of usernames, email addresses, and corresponding passwords from the dark web and then use automated scripts to try the compromised user names and passwords on other websites, such as a registrant’s website, in an attempt to log in and gain unauthorized access to customer accounts.”)

⁴⁰ See, e.g., CISA, *Alert (AA22-117A): 2021 Top Routinely Exploited Vulnerabilities*, available at <https://www.cisa.gov/uscert/ncas/alerts/aa22-117a> (“CISA 2021 Vulnerability Report”) (“Globally, in 2021, malicious cyber actors targeted internet-facing systems, such as email servers and virtual private network (VPN) servers, with exploits of newly disclosed vulnerabilities. For most of the top exploited vulnerabilities, researchers or other actors released proof of concept (POC) code within two weeks of the vulnerability’s disclosure, likely facilitating exploitation by a broader range of malicious actors. To a lesser extent, malicious cyber actors continued to exploit publicly known, dated software vulnerabilities—some of which were also routinely exploited in 2020 or earlier. The exploitation of older vulnerabilities demonstrates the continued risk to organizations that fail to patch software in a timely manner or are using software that is no longer supported by a vendor.”). To address this risk, CISA maintains a Known Exploited Vulnerability (KEV) catalogue that identifies known vulnerabilities. See, e.g., CISA, *Reducing The Significant Risk of Known Exploited Vulnerabilities*, available at <https://www.cisa.gov/known-exploited-vulnerabilities> (“CISA strongly recommends all organizations review and monitor the KEV catalog and prioritize remediation of the listed vulnerabilities to reduce the likelihood of compromise by known threat actors.”).

⁴¹ See CISA, *Security Tip (ST04-015)—Understanding Denial-of-Service Attacks*, available at <https://www.cisa.gov/uscert/ncas/tips/ST04-015> (“A denial-of-service (DoS) attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious threat actor. Services affected may include email, websites, online accounts (e.g., banking), or other services that rely on the affected computer or network. A denial-of-service condition is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users. DoS attacks can cost an organization both time and money while their resources and services are inaccessible.”).

⁴² See Verizon DBIR (finding that DoS attacks represented 46% of the total cybersecurity incidents analyzed).

can impact the information systems a Market Entity operates directly (e.g., a web application or email system).⁴³ They also can adversely impact the Market Entity and its information systems through its connection to information systems operated by third parties such as service providers (e.g., cloud service providers), business partners, customers, counterparties, members, registrants, or users.⁴⁴ Further, the tactics, techniques, and procedures employed by threat actors can adversely impact the Market Entity and its information systems through its connection to information systems operated by utilities or central platforms to which the Market Entity is connected (e.g., a securities exchange, securities trading platform, securities clearing agency, or a payment processor).⁴⁵

If cybersecurity risk materializes into a significant cybersecurity incident, a Market Entity may lose its ability to perform a key function causing harm to the Market Entity, investors, or other market participants. Moreover, given the interconnectedness of Market Entities’ information systems, a significant cybersecurity incident at one Market Entity has the potential to spread to other Market Entities in a cascading process that could cause widespread disruptions threatening the fair, orderly, and efficient operation of the U.S. securities markets.⁴⁶ Further, the

⁴³ See, e.g., Verizon DBIR (finding that the top assets breached in cyber security incidents are servers hosting web applications and emails, and stating that because they are “internet-facing” they “provide a useful venue for attackers to slip through the organization’s ‘perimeter’”).

⁴⁴ See, e.g., Ponemon Institute LLC, *The Cost of Third-Party Cybersecurity Risk Management* (Mar. 2019), available at <https://info.cybergix.com/ponemon-report> (“Third-party breaches remain a dominant security challenge for organizations, with over 63% of breaches linked to a third party.”).

⁴⁵ See, e.g., Financial Markets Authority, New Zealand, *Market Operator Obligations Targeted Review—NZX* (January 2021), available at <https://www.fma.govt.nz/assets/Reports/Market-Operator-Obligations-Targeted-Review-NZX.pdf> (“New Zealand FMA Report”) (describing an August 2020 cybersecurity incident at New Zealand’s only regulated financial product market that caused a trading halt of approximately four days).

⁴⁶ See, e.g., Implications of Cyber Risk for Financial Stability (“Cyber shocks can lead to losses hitting many firms at the same time because of correlated risk exposures (sometimes called the popcorn effect), such as when firms load the same malware-infected third-party software update.”); The Bank for International Settlements, Committee on Payments and Market Infrastructures (“CPMI”) and IOSCO, *Guidance on cyber resilience for financial market infrastructures* (June 2016), available at <https://www.bis.org/cpmi/publ/d146.pdf> (“[T]here is a broad range of entry points through which a [financial market intermediary (“FMI”)] could be compromised. As a result of their interconnectedness, cyber attacks could come through an FMI’s participants, linked FMIs, service providers, vendors and vendor products. . . . Because an FMI’s systems and processes are often

disruption of a Market Entity that provides critical services to other Market Entities through connected information systems could cause cascading disruptions to those other Market Entities to the extent they cannot obtain those critical services from another source.⁴⁷

A significant cybersecurity incident also can result in unauthorized access to and use of personal, confidential, or proprietary information.⁴⁸ In the case of personal information, this can cause harm to investors and others whose personal information was accessed or used (e.g., identity theft).⁴⁹ This could lead to theft of investor assets. In the case of confidential or proprietary information, this can cause harm to the business of the person whose proprietary information was accessed or used (e.g., public exposure of trading positions or business strategies) or provide the unauthorized user with an unfair advantage over other market participants (e.g., trading based on confidential business information). Unauthorized access to proprietary information also can lead to theft of a Market Entity’s valuable intellectual property.

Cybersecurity incidents affecting Market Entities can cause substantial harm to other market participants, including investors. For example, significant cybersecurity incidents caused by malware can cause the loss of the Market Entity’s data, or the data of other market participants.⁵⁰ These

interconnected with the systems and processes of other entities within its ecosystem, in the event of a large-scale cyber incident it is possible for an FMI to pose contagion risk (i.e., propagation of malware or corrupted data) to, or be exposed to contagion risk from, its ecosystem.”).

⁴⁷ See, e.g., Implications of Cyber Risk for Financial Stability (“And the interconnectedness of the financial system means that an event at one or more firms may spread to others (the domino effect). For example, a cyber event at a single bank can disrupt the bank’s ability to send payments and have cascading effects on other banks’ liquidity and operations.”).

⁴⁸ See, e.g., Bank of England CBEST Report (“One class of targeted attack is Computer Network Exploitation (CNE) where the goal is to steal (or exfiltrate) confidential information from the target. This is effectively espionage in cyberspace or, in information security terms, compromising confidentiality.”).

⁴⁹ The NIST Glossary defines “identity fraud or theft” as “all types of crime in which someone wrongfully obtains and uses another person’s personal data in some way that involves fraud or deception, typically for economic gain.”

⁵⁰ CISA, *Cyber Essentials Starter Kit—The Basics for Building a Culture of Cyber Readiness* (Spring 2021), available at https://www.cisa.gov/sites/default/files/publications/Cyber%20Essentials%20Starter%20Kit_03.12.2021_508_0.pdf (“CISA Cyber Essentials Starter Kit”) (“Malware is designed to spread quickly. A lack of defense against it can completely corrupt, destroy or render your data inaccessible.”).

incidents also can lead to business disruptions that are not just costly to the Market Entity but also the other market participants that rely on the Market Entity's services.

A Market Entity also may incur substantial remediation costs due to a significant cybersecurity incident.⁵¹ For example, the incident may result in reimbursement to other market participants for cybersecurity-related losses and payment for their use of identity protection services. A Market Entity's failure to protect itself adequately against a significant cybersecurity incident also may increase its insurance premiums. In addition, a significant cybersecurity incident may expose a Market Entity to litigation costs (e.g., to defend lawsuits brought by individuals whose personal information was stolen), regulatory scrutiny, reputational damage, and, if a result of a compliance failure, penalties. Finally, a sufficiently severe significant cybersecurity incident could cause the failure of a Market Entity. Given the interconnectedness of Market Entities, a significant cybersecurity incident that degrades or disrupts the critical functions of one Market Entity could cause harm to other Market Entities (e.g., by cutting off their access to a critical service such as securities clearance or by exposing them to the same malware that degraded or disrupted the critical functions of the first Market Entity). This could lead to market-wide outages that compromise the fair, orderly, and efficient functioning of the U.S. securities markets.

For these reasons, the Commission is proposing new rule requirements that are designed to protect the U.S. securities markets and investors in these markets from the threat posed by cybersecurity risks.⁵²

⁵¹ See, e.g., IBM Security, *Cost of Data Breach Report 2022*, available at <https://www.ibm.com/security/data-breach> (noting the average cost of a data breach in the financial industry is \$5.97 million); FBI Internet Crime Report (noting that cybercrime victims lost approximately \$6.9 billion in 2021).

⁵² The Commission has pending proposals to address cybersecurity risk with respect to investment advisers, investment companies, and public companies. See *Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies*, Release Nos. 33-11028, 34-94917, IA-5956, IC-34497 (Feb. 9, 2022) [87 FR 13524, (Mar. 9, 2022)] ("Investment Management Cybersecurity Release"); *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, Release Nos. 33-11038, 34-94382, IC-34529 (Mar. 9, 2022) [87 FR 16590 (Mar. 23, 2022)]. In addition, as discussed in more detail below in section II.F. of this release, the Commission is proposing to amend Regulation SCI (17 CFR 242.1000 through 1007) and Regulation S-P (17 CFR 248.1 through

2. Critical Operations of Market Entities Are Exposed to Cybersecurity Risk

The fair, orderly, and efficient operation of the U.S. securities markets depends on Market Entities performing various functions without disruption. Market Entities rely on information systems and networks of interconnected information systems to perform their functions. This exposes them to the harms that can be caused by threat actors using the tactics, techniques, and procedures discussed above (among others) and by errors of employees or third-party service providers (among others). The GAO has stated that the primary cybersecurity risks identified by financial sector firms are: (1) internal

248.30) concurrent with this release. See *Regulation Systems Compliance and Integrity*, Release No. 34-97143 (Mar. 15, 2023) (File No. S7-07-23) ("Regulation SCI 2023 Proposing Release"); *Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information*, Release Nos. 34-97141, IA-6262, IC-34854 (Mar. 15, 2023) (File No. S7-05-23) ("Regulation S-P 2023 Proposing Release"). The Commission encourages commenters to review the proposals with respect to Regulation SCI and Regulation S-P to determine whether they might affect their comments on this proposing release. See also section II.F. of this release (seeking specific comment on how the proposals in this release would interact with Regulation SCI and Regulation S-P as they currently exist and would be amended). Further, the Commission has reopened the comment period for the Investment Management Cybersecurity Release to allow interested persons additional time to analyze the issues and prepare their comments in light of other regulatory developments, including the proposed rules and amendments regarding this proposal, the Regulation SCI 2023 Proposing Release and the Regulation S-P 2023 Proposing Release that the Commission should consider in connection with the Investment Management Cybersecurity Release. See *Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies; Reopening of Comment Period*, Release Nos. 33-11167, 34-97144, IA-6263, IC-34855 (Mar. 15, 2023), [88 FR 16921 (Mar. 31, 2023)]. The Commission encourages commenters to review the Investment Management Cybersecurity Release and the comments on that proposal to determine whether they might affect their comments on this proposing release. The comments on the Investment Management Cybersecurity Release are available at: <https://www.sec.gov/comments/s7-04-22/s70422.htm>. Lastly, the Commission also proposed rules and amendments regarding an investment adviser's obligations with respect to outsourcing certain categories of "covered functions," including cybersecurity. See *Outsourcing by Investment Advisers*, Release No. IA-6176 (Oct. 26, 2022), [87 FR 68816 (Nov. 16, 2022)]. The Commission encourages commenters to review that proposal to determine whether it might affect comments on this proposing release.

actors;⁵³ (2) malware;⁵⁴ (3) social engineering;⁵⁵ and (4) interconnectivity.⁵⁶ As discussed below, a significant cybersecurity incident can cause serious harm to Market Entities and others who use their services or are connected to them through information systems and, if severe enough, negatively impact the fair, orderly, and efficient operations of the U.S. securities markets.

a. Common Uses of Information Systems by Market Entities

Market Entities need accurate and accessible books and records, among other things, to manage and conduct their operations, manage and mitigate their risks, monitor the progress of their business, track their financial condition, prepare financial statements, prepare regulatory filings, and prepare tax returns. Increasingly, these records are made and preserved on information systems.⁵⁷ These recordkeeping information systems also store personal, confidential, and proprietary business information about the Market Entity and its customers, counterparties, members, registrants, or users.

The complexity and scope of these books and records systems ranges from ones used by large Market Entities that comprise networks of systems that track thousands of different types of daily transactions (e.g., securities trades and movements of assets) to ones used by small Market Entities comprising off-

⁵³ See GAO Cybersecurity Report ("Risks due to insider threats involve careless, poorly trained, or disgruntled employees or contractors hired by an organization who may intentionally or inadvertently introduce vulnerabilities or malware into information systems. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. Results of insider threats can include data destruction and account compromise.").

⁵⁴ *Id.* ("The risk of malware exploits impacting the [financial] sector has increased as malware exploits have grown in sophistication").

⁵⁵ *Id.* ("The financial services sector is at risk due to social engineering attacks, which include a broad range of malicious activities accomplished through human interaction that enable attackers to gain access to sensitive data by convincing a legitimate, authorized user to give them their credentials and/or other personal information").

⁵⁶ *Id.* ("Interconnectivity involves interdependencies throughout the financial services sector and the sharing of data and information via networks, the cloud, and mobile applications. Organizations in the financial services sector utilize data aggregation hubs and cloud service providers, and new financial technologies such as algorithms based on consumers' data and risk preferences to provide digital services for investment and financial advice.").

⁵⁷ Some Market Entities may store certain or all of their records in paper format. This discussion pertains to recordkeeping systems that store records electronically on information systems.

the-shelf accounting software and computer files on a desktop computer. In either case, the impact on the confidentiality, integrity, or availability of the information system being compromised as a consequence of a significant cybersecurity incident can be devastating to the Market Entity and its customers, counterparties, members, registrants or users. For example, it could cause the Market Entity to cease operations or allow threat actors to use personal information about the customers of the Market Entity to steal their identities.

Market Entities also use information systems so that their employees can communicate with each other and with external persons. These include email, text messaging, and virtual meeting applications. The failure of these information systems as a result of a significant cybersecurity incident can seriously disrupt the Market Entity's ability to carry out its functions. Moreover, these outward facing information systems are vectors that threat actors use to cause harmful cybersecurity incidents by, for example, tricking an employee through social engineering into downloading malware in an attachment to an email.

b. Broker-Dealers

Broker-dealers perform a number of functions in the U.S. securities markets, including underwriting the issuance of securities for publicly and privately held companies, making markets in securities, brokering securities transactions, dealing securities, operating an ATS, executing securities transactions, clearing and settling securities transactions, and maintaining custody of securities for investors. Some broker-dealers may perform multiple functions; whereas others may perform a single function. Increasingly, these functions are performed through the use of information systems. For example, broker-dealers use information systems to connect to securities exchanges, ATSs, and other securities markets in order to transmit purchase and sell orders. Broker-dealers also use information systems to connect to clearing agencies or clearing broker-dealers to transmit securities settlement instructions and transfer funds. They use information systems to communicate and transact with other broker-dealers. In addition, they use information systems to provide securities services to investors, including information systems that investors use to access their securities accounts and transmit orders to purchase or sell securities.

Depending on the functions undertaken by a broker-dealer, a significant cybersecurity incident could affect customers, including retail investors. For example, a significant cybersecurity incident could result in the broker-dealer experiencing a systems outage, which in turn could leave customers unable to purchase or sell securities held in their account and the broker-dealer unable to trade for itself. In addition, broker-dealers maintain records and information related to their customers that include personal information, such as names, addresses, phone numbers, employer information, tax identification information, bank information, and other detailed and individualized information related to broker-dealer obligations under applicable statutory and regulatory provisions.⁵⁸ If personal information held by a broker-dealer is accessed or stolen by unauthorized users, it could result in harm (e.g., identity theft or conversion of financial assets) to many individuals, including retail investors.

Further, a significant cybersecurity incident at a broker-dealer could provide a gateway for threat actors to attack the self-regulatory organizations ("SROs")—such as national securities exchanges and registered clearing agencies—ATSs, and other broker-dealers to which the firm is connected through information systems and networks of interconnected information systems.⁵⁹ This could cause a cascading effect where a significant cybersecurity incident initially impacting one broker-dealer spreads to other Market Entities. Moreover, the information systems that link a broker-dealer to other Market Entities, its customers, and other service providers are vectors that expose the broker-dealer to cybersecurity risk arising from threats that originate in information systems outside the broker-dealer's control.

In addition, some broker-dealers operate ATSs. An ATS is a trading system for securities that meets the definition of "exchange" under federal

securities laws but is not required to register with the Commission as a national securities exchange if it complies with the conditions to an exemption provided under Regulation ATS, which includes registering as a broker-dealer.⁶⁰ Registering as a broker-dealer requires becoming a member of an SRO, such as FINRA, and membership in FINRA subjects an ATS to FINRA's rules and oversight. Since Regulation ATS was adopted in 1998, ATSs' operations have increasingly relied on complex automated systems to bring together buyers and sellers for various securities, which include—for example—electronic limit order books and auction mechanisms. These developments have made ATSs significant sources of orders and trading interest for securities. ATSs employ information systems to accept, store, and match orders pursuant to pre-programmed methods and to communicate the execution of these orders for trade reporting purposes and for clearance and settlement of the transactions. ATSs, in particular ATSs that are "NMS Stock ATSs,"⁶¹ use information systems to connect to various trading centers in order to receive market data that ATSs use to price and execute orders that are entered on the ATS. A significant cybersecurity incident could disrupt the ATS's critical infrastructure and significantly impede the ability of the ATS to (among other things): (1) receive market data; (2) accept, price, and match orders; or (3) report transactions. This, in turn, could negatively impact the ability of ATS subscribers to trade and execute the orders of their investors or purchase certain securities at favorable or predictable prices or in a timely manner to the extent the ATS provides

⁶⁰ 17 CFR 242.300 through 242.304. Exchange Act Rule 3a1-1(a)(2) exempts from the definition of "exchange" under Section 3(a)(1) of the Exchange Act an organization, association, or group of persons that complies with Regulation ATS. See 17 CFR 240.3a1-1(a)(2). Regulation ATS requires an ATS to, among other things, register as a broker-dealer, file a Form ATS with the Commission to notice its operations, and establish written safeguards and procedures to protect subscribers' confidential trading information. See 17 CFR 242.301(b)(1), (2), and (10), respectively. The broker-dealer operator of the ATS controls all aspects of the ATS's operations and is legally responsible for its operations and for ensuring that the ATS complies with applicable federal securities laws and the rules and regulations thereunder, including Regulation ATS. See *Regulation of NMS Stock Alternative Trading Systems*, Exchange Act Release No. 83663 (July 18, 2018) [83 FR 38768, 38819-20 (Aug. 7, 2018)] ("Regulation of NMS Stock Alternative Trading Systems Release").

⁶¹ See 17 CFR 242.300(k) (defining the term "NMS Stock ATS").

⁵⁸ See, e.g., 17 CFR 240.17a-3(a)(17) (requiring broker-dealers to make account records of the customer's or owner's name, tax identification number, address, telephone number, date of birth, employment status, annual income, net worth, and the account's investment objectives). Broker-dealers also must comply with relevant anti-money laundering (AML) laws, rules, orders, and guidance. See, e.g., Commission, *Anti-Money Laundering (AML) Source Tool for Broker-Dealers*, (May 16, 2022), available at <https://www.sec.gov/about/offices/ocie/amlsourcetool>.

⁵⁹ Section 3(a)(26) of the Exchange Act defines a self-regulatory organization as any national securities exchange, registered securities association, registered clearing agency, or (with limitations) the MSRB. See 15 U.S.C. 78c(a)(26).

liquidity to the market for those securities.

c. Clearing Agencies

Clearing agencies are broadly defined in the Exchange Act and undertake a variety of functions.⁶² An entity that meets the definition of a “clearing agency” is required to register with the Commission or obtain from the Commission an exemption from registration prior to performing the functions of a clearing agency.⁶³

Two common functions of registered clearing agencies are operating as a central counterparty (“CCP”) or a central securities depository (“CSD”). Registered clearing agencies that provide these services are “covered clearing agencies” under Commission regulations.⁶⁴ A CCP acts as the buyer to every seller and the seller to every buyer, providing a trade guaranty with respect to transactions submitted for clearing by the clearing agency’s participants.⁶⁵ A CSD acts as a depository for handling securities, whereby all securities of a particular class or series of any issuer deposited within the system are treated as fungible. Market Entities may use a CSD to transfer, loan, or pledge securities by bookkeeping entry without the physical delivery of certificates. A CSD also may permit or facilitate the settlement of securities transactions more generally.⁶⁶ Currently, all clearing agencies registered with the Commission that are actively providing clearance and settlement services are covered clearing agencies.⁶⁷

Registered clearing agencies also are SROs under section 19 of the Exchange Act, and their proposed rules are subject to Commission review and published for notice and comment. While certain types of proposed rules are effective upon filing, others are subject to Commission approval before they can go into effect.

Additionally, section 17A(b)(1) of the Exchange Act provides the Commission with authority to exempt a clearing agency or any class of clearing agencies (“exempt clearing agencies”) from any provision of section 17A or the rules or regulations thereunder.⁶⁸ An exemption may be effected by rule or order, upon the Commission’s own motion or upon application, and conditionally or unconditionally.⁶⁹ The Commission has provided exemptions from registration as a clearing agency for clearing agencies that provide matching services.⁷⁰ Matching services centrally

but conduct no clearance or settlement operations. *See Self-Regulatory Organizations; The Boston Stock Clearing Corporation; Notice of Filing and Immediate Effectiveness of Proposed Rule Change To Amend the Articles of Organization and By-Laws*, Exchange Act Release No. 63629 (Jan. 3, 2011) [76 FR 1473, 1474 (Jan. 10, 2011)] (“BSECC Notice”); *Self-Regulatory Organizations; Stock Clearing Corporation of Philadelphia; Notice of Filing and Immediate Effectiveness of Proposed Rule Change Relating to the Suspension of Certain Provisions Due to Inactivity*, Exchange Act Release No. 63268 (Nov. 8, 2010) [75 FR 69730, 69731 (Nov. 15, 2010)] (“SCCP Notice”).

⁶² 15 U.S.C. 78q–1(b)(1). *See also* 15 U.S.C. 78mm (providing the Commission with general exemptive authority).

⁶³ *See* 15 U.S.C. 78q–1(b)(1). The Commission’s exercise of authority to grant exemptive relief must be consistent with the public interest, the protection of investors, and the purposes of Section 17A of the Exchange Act, including the prompt and accurate clearance and settlement of securities transactions and the safeguarding of securities and funds.

⁶⁴ *See Global Joint Venture Matching Services—US, LLC; Order Granting Exemption from Registration as a Clearing Agency*, Exchange Act Release No. 44188 (Apr. 17, 2001) [66 FR 20494 (Apr. 23, 2001)] (granting an exemption to provide matching services to Global Joint Venture Matching Services US LLC, now known as DTCC ITP Matching U.S. LLC) (“DTCC ITP Matching Order”); *Bloomberg STP LLC; SS&C Technologies, Inc.; Order of the Commission Approving Applications for an Exemption From Registration as a Clearing Agency*, Exchange Act Release No. 76514 (Nov. 25, 2015) [80 FR 75388 (Dec. 1, 2015)] (granting an exemption to provide matching services to each of Bloomberg STP LLC and SS&C Technologies, Inc.) (“BSTP SS&C Order”). In addition, on July 1, 2011, the Commission published a conditional, temporary exemption from clearing agency registration for entities that perform certain post-trade processing services for security-based swap transactions. *See Order Pursuant to Section 36 of the Securities Exchange Act of 1934 Granting Temporary Exemptions From Clearing Agency Registration Requirements Under Section 17A(b) of the Exchange Act for Entities Providing Certain Clearing Services for Security-Based Swaps*, Exchange Act Release No. 34–64796 (July 1, 2011) [76 FR 39963 (July 7, 2011)]. The order facilitated the Commission’s identification of entities that

match trade information between a broker-dealer and its institutional customer. The Commission also has provided exemptions for non-U.S. clearing agencies to perform the functions of a clearing agency with respect to transactions of U.S. participants involving U.S. government and agency securities.⁷¹

Registered and exempt clearing agencies rely on information systems to perform the functions described above. Given their central role, the information systems operated by clearing agencies are critical to the operations of the U.S. securities markets. For registered clearing agencies, in particular, these information systems include those that set and calculate margin obligations and other charges, perform netting and calculate payment obligations, facilitate the movement of funds and securities, or effectuate end-of-day settlement.

operate in that area and that accordingly may fall within the clearing agency definition. Recently, the Commission indicated that the 2011 Temporary Exemption may no longer be necessary. *See Rules Relating to Security-Based Swap Execution and Registration and Regulation of Security-Based Swap Execution Facilities*, Release No. 34–94615 (Apr. 6, 2022) [87 FR 28872, 28934 (May 11, 2022)] (stating that the “Commission preliminarily believes that, if it adopts a framework for the registration of [security-based swap execution facilities (“SBSEFs”)], the 2011 Temporary Exemption would no longer be necessary because entities carrying out the functions of SBSEFs would be able to register with the Commission as such, thereby falling within the exemption from the definition of ‘clearing agency’ in existing Rule 17Ad–24.”).

⁷¹ *See Euroclear Bank SA/NV; Order of the Commission Approving an Application To Modify an Existing Exemption From Clearing Agency Registration*, Exchange Act Release No. 79577 (Dec. 16, 2016) [81 FR 93994 (Dec. 22, 2016)] (providing an exemption to Euroclear Bank SA/NV (successor in name to Morgan Guaranty Trust Company of NY)) (“Euroclear Bank Order”); *Self-Regulatory Organizations; Cedel Bank; Order Approving Application for Exemption From Registration as a Clearing Agency*, Exchange Act Release No. Release No. 38328 (Feb. 24, 1997) [62 FR 9225 (Feb. 28, 1997)] (providing an exemption to Clearstream Banking, S.A. (successor in name to Cedel Bank, société anonyme, Luxembourg)) (“Clearstream Banking Order”). Furthermore, pursuant to the Commission’s statement on CCPs in the European Union (“EU”) authorized under the European Markets Infrastructure Regulation (“EMIR”), an EU CCP may request an exemption from the Commission where it has determined that the application of Commission requirements would impose unnecessary, duplicative, or inconsistent requirements in light of EMIR requirements to which it is subject. *See Statement on Central Counterparties Authorized under the European Markets Infrastructure Regulation Seeking to Register as a Clearing Agency or to Request Exemptions from Certain Requirements Under the Securities Exchange Act of 1934*, Exchange Act Release No. 34–90492 (Nov. 23, 2020) [85 FR 76635, 76639 (Nov. 30, 2020)], <https://www.govinfo.gov/content/pkg/FR-2020-11-30/pdf/FR-2020-11-30.pdf> (stating that in seeking an exemption, an EU CCP could provide “a self-assessment . . . [to] explain how the EU CCP’s compliance with EMIR corresponds to the requirements in the Exchange Act and applicable SEC rules thereunder, such as Rule 17Ad–22 and Regulation SCI.”).

⁶² *See* 15 U.S.C. 78c(a)(23)(A).

⁶³ *See* 15 U.S.C. 78q–1(b); 17 CFR 240.17Ab2–1.

⁶⁴ *See* 17 CFR 240.17Ad–22. *See also Standards for Covered Clearing Agencies*, Exchange Act Release No. 78961 (Sept. 28, 2016) [81 FR 70786, 70793 (Oct. 13, 2016)] (“CCA Standards Adopting Release”). As discussed below, some clearing agencies operate pursuant to Commission exemptions from registration.

⁶⁵ *See* 17 CFR 240.17Ad–22 (“Rule 17Ad–22”); *Definition of “Covered Clearing Agency”*, Exchange Act Release No. 88616 (Apr. 9, 2020) [85 FR 28853, 28855–56 (May 14, 2020)] (“CCA Definition Adopting Release”).

⁶⁶ *See* 15 U.S.C. 78c(a)(23)(A); 17 CFR 240.17Ad–22; *CCA Definition Adopting Release*, 81 FR at 28856.

⁶⁷ The active covered clearing agencies are: (1) The Depository Trust Company (“DTC”); (2) Fixed Income Clearing Corporation (“FICC”); (3) National Securities Clearing Corporation (“NSCC”); (4) Intercontinental Exchange, Inc. (“ICE”) Clear Credit LLC (“ICC”); (5) ICE Clear Europe Limited (“ICEEU”); (6) The Options Clearing Corporation (“Options Clearing Corp.”); and (7) LCH SA. Certain clearing agencies are registered with the Commission but are not covered clearing agencies. *See CCA Standards Adopting Release*, 81 FR at 70793. In particular, although subject to paragraph (d) of Rule 17Ad–22, the Boston Stock Exchange Clearing Corporation (“BSECC”) and Stock Clearing Corporation of Philadelphia (“SCCP”) are currently registered with the Commission as clearing agencies

Certain exempt clearing agencies (e.g., Euroclear and Clearstream) may provide CSD functions like covered clearing agencies while other exempt clearing agencies (e.g., DTCC ITP) may not provide such functions. Nonetheless, any entity that falls within the definition of a clearing agency centralizes technology functions in a manner that increases its potential to become a single point of failure in the case of a significant cybersecurity incident.⁷²

The technology behind clearing agency information systems is subject to growing innovation and interconnectedness, with multiple clearing agencies sharing links among their systems and with the systems of other Market Entities. This growing interconnectivity means that a significant cybersecurity incident at a registered clearing agency could, for example, prevent it from acting timely to carry out its functions, which, in turn, could negatively impact other Market Entities that utilize the clearing agency's services.⁷³ Further, a significant cybersecurity incident at a registered or exempt clearing agency could provide a gateway for threat actors to attack the members of the clearing agency and other financial institutions that connect to it through information systems. Moreover, the information systems that link the clearing agency to its members are vectors that expose the clearing agency to cybersecurity risk.

The records stored by clearing agencies on their information systems include proprietary information about their members, including confidential business information (e.g., information about the financial condition of the members used by the clearing agency to manage credit risk). Each clearing

agency also is required to keep all records made or received by it in the course of its business and in the conduct of its self-regulatory activity. A significant cybersecurity incident at a clearing agency could lead to the improper use of this information to harm the members (e.g., public exposure of confidential financial information) or provide the unauthorized user with an unfair advantage over other market participants (e.g., trading based on confidential business information). Moreover, a disruption to a registered clearing agency's operations as a result of a significant cybersecurity incident could interfere with its ability to perform its responsibilities as an SRO (e.g., interrupting its oversight of clearing member activities for compliance with its rules and the federal securities laws), and, therefore, materially impact the fair, orderly, and efficient functioning of the U.S. securities markets.

d. The Municipal Securities Rulemaking Board

The MSRB is an SRO that serves as a regulator of the U.S. municipal securities market with a mandate to protect municipal securities investors, municipal entities, obligated persons, and the public interest.⁷⁴ Pursuant to the Exchange Act, the MSRB shall propose and adopt rules with respect to transactions in municipal securities effected by broker-dealers and municipal securities dealers and with respect to advice provided to or on behalf of municipal entities or obligated persons by broker-dealers, municipal securities dealers, and municipal advisors with respect to municipal financial products, the issuance of municipal securities, and solicitations of municipal entities or obligated persons undertaken by broker-dealers, municipal securities dealers, and municipal advisors.⁷⁵ Pursuant to the Exchange Act, the MSRB's rules shall be designed to prevent fraudulent and manipulative acts and practices, to promote just and equitable principles of trade, to foster cooperation and coordination with persons engaged in regulating, clearing, settling, processing, information with respect to, and facilitating transactions in municipal securities and municipal financial products, to remove impediments to and perfect the mechanism of a free and open market in municipal securities and municipal products, and in general, to

protect investors, municipal entities, obligated persons, and the public interest.⁷⁶ As an SRO, the MSRB's proposed rules are subject to Commission review and published for notice and comment. While certain types of proposed rules are effective upon filing, others are subject to Commission approval before they can go into effect.

The MSRB relies on information systems to carry out its mission regulating broker-dealers, municipal securities dealers, and municipal advisors. For example, the MSRB operates the Electronic Municipal Market Access website ("EMMA"). EMMA provides transparency to the U.S. municipal bond market by disclosing free information on virtually all municipal bond offerings, including real-time trade prices, bond disclosure documents, and certain market statistics.⁷⁷ The MSRB also provides data to the Commission, broker-dealer examining authorities, and banking supervisors to assist in their examination and enforcement efforts involving participants in the municipal securities markets. The MSRB also maintains other data on the U.S. municipal securities markets. This data can be used by the public and others to understand better these markets. The MSRB is also required to keep all records made or received by it in the course of its business and in the conduct of its self-regulatory activity.

A significant cybersecurity incident could disrupt the operation of EMMA and could negatively impact the fair, orderly, and efficient operation of the U.S. municipal securities market. For example, the loss or corruption of transparent price information could cause investors to stop purchasing or selling municipal securities or negatively impact the ability of investors to liquidate or purchase municipal securities at favorable or predictable prices or in a timely manner. In addition, the unauthorized access or use of personal or proprietary

⁷² See generally Board of Governors of the Federal Reserve System ("Federal Reserve Board"), Commission, Commodity Futures Trading Commission ("CFTC"), *Risk Management of Designated Clearing Entities* (July 2011), available at <https://www.federalreserve.gov/publications/other-reports/files/risk-management-supervision-report-201107.pdf> (report to the Senate Committees on Banking, Housing, and Urban Affairs and Agriculture, Nutrition, and Forestry and the House Committees on Financial Services and Agriculture stating that a designated clearing entity ("DCE") "faces two types of non-financial risks—operational and legal—that may disrupt the functioning of the DCE. . . . DCEs face operational risk from both internal and external sources, including human error, system failures, security breaches, and natural or man-made disasters.").

⁷³ See also EXAMS, Commission, *Staff Report on the Regulation of Clearing Agencies* (Oct. 1, 2020), available at <https://www.sec.gov/files/regulation-clearing-agencies-100120.pdf> (staff stating that "consolidation among providers of clearance and settlement services concentrates clearing activity in fewer providers and has increased the potential for providers to become single points of failure.").

⁷⁴ See 15 U.S.C. 78o-4. Information about the MSRB and its functions is available at: www.msrb.org.

⁷⁵ See 15 U.S.C. 78o-4(b)(2).

⁷⁶ See 15 U.S.C. 78o-4(b)(2)(C).

⁷⁷ Broker-dealers, and municipal securities dealers that trade municipal securities are subject to transaction reporting obligations under MSRB Rule G-14. EMMA, established by the MSRB in 2009, is currently designated by the Commission as the official repository of municipal securities disclosure providing the public with free access to relevant municipal securities data, and is the central database for information about municipal securities offerings, issuers, and obligors. Additionally, the MSRB's Real-Time Transaction Reporting System ("RTRS"), with limited exceptions, requires broker-dealers and municipal securities dealers to submit transaction data to the MSRB within 15 minutes of trade execution, and such near real-time post-trade transaction data can be accessed through the MSRB's EMMA website.

information of the persons who are registered with the MSRB could cause them harm through identity theft or the disclosure of confidential business information.

Further, a significant cybersecurity incident impacting the MSRB could provide a gateway for threat actors to attack registrants that connect to the MSRB through information systems and networks of interconnected information systems. Moreover, the information systems that link the MSRB to its registrants are vectors that expose the MSRB to cybersecurity risk.

e. National Securities Associations

A national securities association is an SRO created to regulate broker-dealers and the off-exchange broker-dealer market.⁷⁸ Currently, FINRA is the only national securities association registered under section 15A of the Exchange Act. As a national securities association, FINRA must have rules for its members that, among other things, are designed to prevent fraudulent and manipulative acts and practices, to promote just and equitable principles of trade, to foster cooperation and coordination with persons engaged in regulating, clearing, settling, or processing information with respect to (and facilitating transactions in) securities, to remove impediments to and perfect the mechanism of a free and open market and a national market system, and, in general, to protect investors and the public interest.⁷⁹ FINRA's rules also must provide for discipline of its members for violations of any provision of the Exchange Act, Exchange Act rules, the rules of the MSRB, or its own rules.⁸⁰ A national securities association is an SRO under section 19 of the Exchange Act, and its proposed rules are subject to Commission review and are published for notice and comment. While certain types of proposed FINRA rules are effective upon filing, others are subject to Commission approval before they can go into effect.

FINRA also performs other functions of vital importance to the U.S. securities markets. It developed and operates the Trade Reporting and Compliance Engine ("TRACE"), which facilitates the mandatory reporting of over-the-counter transactions in eligible fixed-income

securities.⁸¹ In addition, FINRA operates the Trade Reporting Facility ("TRF"). FINRA members report over-the-counter transactions in national market system ("NMS") stocks to the TRF, which are then included in publicly disseminated consolidated equity market data pursuant to an NMS plan.⁸² Further, pursuant to plans declared effective by the Commission under Exchange Act Rule 17d-2 ("Rule 17d-2"),⁸³ FINRA frequently acts as the sole SRO with regulatory responsibility with respect to certain applicable laws, rules, and regulations for its members that are also members of other SROs (e.g., national securities exchanges).⁸⁴ Some of these Rule 17d-2 plans facilitate the conduct of market-wide surveillance, including for insider trading.⁸⁵ The disruption of these FINRA activities by a significant cybersecurity incident could interfere with its ability to carry out its regulatory responsibilities (e.g., disclosing confidential information pertaining to its surveillance of trading activity), and,

⁸¹ FINRA members are subject to transaction reporting obligations under FINRA Rule 6730. This rule requires FINRA members to report transactions in TRACE-Eligible Securities, which the rule defines to include a range of fixed-income securities.

⁸² In addition, FINRA operates the Alternative Display Facility ("ADF"), which allows members to display quotations and report trades in NMS stocks. Although there are currently no users of the ADF, FINRA has issued a pre-quotation notice advising that a new participant intends to begin using the ADF, subject to regulatory approval. See *Self-Regulatory Organizations; Financial Industry Regulatory Authority, Inc.; Notice of Filing of a Proposed Rule Change Relating to Alternative Display Facility New Entrant*, Exchange Act Release No. 96550 (Dec. 20, 2022) [87 FR 79401 (Dec. 27, 2022)].

⁸³ 17 CFR 240.17d-2. Pursuant to a plan declared effective by the Commission under Rule 17d-2, the Commission relieves an SRO of those regulatory responsibilities allocated by the plan to another SRO.

⁸⁴ See, e.g., *Program for Allocation of Regulatory Responsibilities Pursuant to Rule 17d-2; Notice of Filing and Order Approving and Declaring Effective an Amended Plan for the Allocation of Regulatory Responsibilities Between the Financial Industry Regulatory Authority, Inc. and MEMX LLC*, Exchange Act Release No. 96101 (Oct. 18, 2022) [87 FR 64280 (Oct. 24, 2022)].

⁸⁵ See, e.g., *Program for Allocation of Regulatory Responsibilities Pursuant to Rule 17d-2; Notice of Filing and Order Approving and Declaring Effective an Amendment to the Plan for the Allocation of Regulatory Responsibilities Among Cboe BZX Exchange, Inc., Cboe BYX Exchange, Inc., NYSE Chicago, Inc., Cboe EDGA Exchange, Inc., Cboe EDGX Exchange, Inc., Financial Industry Regulatory Authority, Inc., MEMX LLC, MIAX PEARL, LLC, Nasdaq BX, Inc., Nasdaq PHLX LLC, The Nasdaq Stock Market LLC, NYSE National, Inc., New York Stock Exchange LLC, NYSE American LLC, NYSE Arca, Inc., Investors' Exchange LLC, and Long-Term Stock Exchange, Inc. Relating to the Surveillance, Investigation, and Enforcement of Insider Trading Rules*, Exchange Act Release No. 89972 (Sept. 23, 2020) [85 FR 61062 (Sept. 29, 2020)].

therefore, materially impact the fair, orderly, and efficient functioning of the U.S. securities markets.

FINRA uses other information systems to perform its responsibilities as an SRO. For example, it operates a number of information systems that its members use to make regulatory filings.⁸⁶ These systems include the FINRA's eFOCUS system through which its broker-dealer members file periodic (monthly or quarterly) confidential financial and operational reports.⁸⁷ FINRA Gateway is another information system that it uses as a compliance portal for its members to file and access information. A disruption of FINRA's business operations caused by a significant cybersecurity incident could disrupt its ability to carry out its responsibilities as an SRO (e.g., by disrupting its oversight of broker-dealer activities for compliance with its rules and the federal securities laws or its review of broker-dealers' financial condition), and could therefore materially impact the fair, orderly, and efficient functioning of the U.S. securities markets.

Further, a significant cybersecurity incident at FINRA could provide a gateway for threat actors to attack members that connect to it through information systems and networks of interconnected information systems. Moreover, the information systems that link FINRA to its members are vectors that expose FINRA to cybersecurity risk.

Additionally, the records stored by FINRA on its information systems include proprietary information about its members, including confidential business information (e.g., information about the operational and financial condition of its broker-dealer members) and confidential personal information about registered persons affiliated with member firms. FINRA also is required to keep all records made or received by it in the course of its business and in the conduct of its self-regulatory activity. A significant cybersecurity incident at FINRA could lead to the improper use of this information to harm the members

⁸⁶ Further information about these filing systems is available at: <https://www.finra.org/filing-reporting/regulatory-filing-systems>.

⁸⁷ The eFOCUS system provides firms with the capability to electronically submit their Financial and Operational Combined Uniform Single (FOCUS) Reports to FINRA. FINRA member broker-dealers are required to prepare and submit FOCUS reports pursuant to Exchange Rule 17a-5 (17 CFR 240.17a-5) ("Rule 17a-5") and FINRA's FOCUS Report filing plan. See, e.g., *Self-Regulatory Organizations; Notice of Filing and Order Granting Accelerated Approval of Proposed Rule Change by the National Association of Securities Dealers, Inc. Relating to the Association's FOCUS Filing Plan*, Exchange Act Release No. 36780, (Jan. 26, 1996) [61 FR 3743 (Feb. 1, 1996)].

⁷⁸ See 15 U.S.C. 78o-3(a); *Exemption for Certain Exchange Members*, Exchange Act Release No. 95388 (July 29, 2022) [87 FR 49930 (Aug. 12, 2022)] (proposing amendments to national securities association membership exemption for certain exchange members).

⁷⁹ See 15 U.S.C. 78o-3(b)(6).

⁸⁰ See 15 U.S.C. 78o-3(b)(7).

(e.g., public exposure of confidential financial information) or their registered persons (e.g., public exposure of personal information). Further, it could provide the unauthorized user with an unfair advantage over other market participants (e.g., trading based on confidential financial information about its members).

f. National Securities Exchanges

Under the Exchange Act, an “exchange” is any organization, association, or group of persons, whether incorporated or unincorporated, that constitutes, maintains, or provides a market place or facilities for bringing together purchasers and sellers of securities or for otherwise performing with respect to securities the functions commonly performed by a stock exchange (as that term is generally understood), and includes the market place and the market facilities maintained by that exchange.⁸⁸ Section 5 of the Exchange Act⁸⁹ requires an organization, association, or group of persons that meets the definition of “exchange” under section 3(a)(1) of the Exchange Act, unless otherwise exempt, to register with the Commission as a national securities exchange pursuant to section 6 of the Exchange Act. Registered

national securities exchanges also are SROs, and must comply with regulatory requirements applicable to both national securities exchanges and SROs.⁹⁰ Section 6 of the Exchange Act requires, among other things, that the rules of a national securities exchange be designed to prevent fraudulent and manipulative acts and practices; to promote just and equitable principles of trade; to foster cooperation and coordination with persons engaged in facilitating transactions in securities; to remove impediments to, and perfect the mechanism of, a free and open market and a national market system; and, in general, to protect investors and the public interest; and that the rules of a national securities exchange not be designed to permit unfair discrimination between customers, issuers, brokers, or dealers.⁹¹ As SROs under section 19 of the Exchange Act, the proposed rules of national securities exchanges are subject to Commission review and are published for notice and comment.⁹² While certain types of proposed exchange rules are effective upon filing, others are subject to Commission approval before they can go into effect.

National securities exchanges use information systems to operate their marketplaces and facilities for bringing together purchasers and sellers of securities. In particular, national securities exchanges rely on automated, complex, and interconnected information systems for trading, routing, market data, regulatory, and surveillance purposes. They also use information systems to connect to members, other national securities exchanges, plan processors, and clearing agencies to facilitate order routing, trading, trade reporting, and the clearing of securities transactions. They also provide quotation, trade reporting, and regulatory information to the securities information processors to ensure that current market data information is available to market participants.⁹³ A

significant cyber security incident at a national securities exchange could disrupt or disable its ability to provide these market functions, causing broader disruptions to the securities markets.⁹⁴ For example, a significant cyber security incident could severely impede the ability to trade securities, or could disrupt the public dissemination of consolidated market data, impacting investors and the maintenance of fair, orderly, and efficient markets. In addition, the information systems that link national securities exchanges to their members are vectors that expose the exchange to cybersecurity risk.

Similarly, proprietary market data systems of exchanges are widely used and relied upon by a wide swath of market participants for detailed information about quoting and trading activity on an exchange. A significant cybersecurity incident that disrupts the availability or integrity of these feeds could have a significant impact on the trading of securities because market participants may withdraw from trading without access to current quotation and trade information. This could interfere with the maintenance of fair, orderly, and efficient markets.

National securities exchanges also use information systems to perform their

⁸⁸ See 15 U.S.C. 78c(a)(1). Exchange Act Rule 3b-16 (“Rule 3b-16”) defines terms used in the statutory definition of “exchange” under section 3(a)(1) of the Exchange Act. Under paragraph (a) of Rule 3b-16, an organization, association, or group of persons is considered to constitute, maintain, or provide such a marketplace or facilities if they “[bring] together the orders for securities of multiple buyers and sellers” and use “established non-discretionary methods (whether by providing a trading facility or by setting rules) under which such orders interact with each other, and the buyers and sellers entering such orders agree to the terms of a trade.” See 17 CFR 240.3b-16(a). In January 2022, the Commission: (1) proposed amendments to Rule 3b-16 to include systems that offer the use of non-firm trading interest and provide communication protocols to bring together buyers and sellers of securities; (2) re-proposed amendments to Regulation ATS for ATSs that trade government securities or repurchase and reverse repurchase agreements on government securities; (3) re-proposed amendments to Regulation SCI to apply to ATSs that meet certain volume thresholds in U.S. Treasury securities or in a debt security issued or guaranteed by a U.S. executive agency or government-sponsored enterprise; and (4) proposed amendments to, among other things, Form ATS-N, Form ATS-R, Form ATS, and the fair access rule under Regulation ATS. See *Amendments Regarding the Definition of “Exchange” and Alternative Trading Systems (ATSs) That Trade U.S. Treasury and Agency Securities, National Market System (NMS) Stocks, and Other Securities*, Exchange Act Release No. 94062 (Jan. 26, 2022) [87 FR 15496 (Mar. 18, 2022)] (“Amendments Regarding the Definition of ‘Exchange’ and ATSs Release”). The Commission encourages commenters to review that proposal with respect to ATSs and the comments on that proposal to determine whether they might affect comments on this proposing release.

⁸⁹ 15 U.S.C. 78e.

⁹⁰ See, e.g., 15 U.S.C. 78f and 78s.

⁹¹ See 15 U.S.C. 78f(b)(5).

⁹² See 15 U.S.C. 78s.

⁹³ The national securities exchanges will provide quotation, trade reporting, and regulatory information to competing consolidators and self-aggregators after the market data infrastructure rules have been implemented. See *Market Data Infrastructure*, Exchange Act Release No. 90610 (Dec. 9, 2020) [86 FR 18596 (Apr. 9, 2021)] (“MDI Adopting Release”). In July 2012, the Commission adopted Rule 613 of Regulation NMS, which required national securities exchanges and national securities associations (the “Participants”) to jointly develop and submit to the Commission a national market system plan to create, implement, and maintain a consolidated audit trail (the “CAT”). See *Consolidated Audit Trail*, Exchange Act Release No. 67457 (July 18, 2012) [77 FR 45722 (Aug. 1, 2012)];

17 CFR 242.613. In November 2016, the Commission approved the national market system plan required by Rule 613 (the “CAT NMS Plan”). See *Joint Industry Plan; Order Approving the National Market System Plan Governing the Consolidated Audit Trail*, Exchange Act Release No. 78318 (Nov. 15, 2016) [81 FR 84696 (Nov. 23, 2016)] (the “CAT NMS Plan Approval Order”). The Participants conduct the activities related to the CAT in a Delaware limited liability company, Consolidated Audit Trail, LLC (the “Company”). The Participants jointly own on an equal basis the Company. As such, the CAT’s Central Repository is a facility of each of the Participants. See *CAT NMS Plan Approval Order*, 81 FR at 84758. It would also qualify as an “information system” of each national securities exchange and each national securities association under proposed Rule 10. FINRA CAT, LLC—a wholly-owned subsidiary of FINRA—has entered into an agreement with the Company to act as the plan processor for the CAT. However, because the CAT System is operated by FINRA CAT, LLC on behalf of the national securities exchanges and FINRA, the Participants remain ultimately responsible for the performance of the CAT and its compliance with any statutes, rules, and regulations. The goal of the CAT NMS Plan is to create a modernized audit trail system that provides regulators with more timely access to a more comprehensive set of trading data, thus enabling regulators to more efficiently and effectively analyze and reconstruct broad-based market events, conduct market analysis in support of regulatory decisions, and to conduct market surveillance, investigations, and other enforcement activities. The CAT accepts data that are submitted by the Participants and broker-dealers, as well as data from certain market data feeds like SIP and OPRA.

⁹⁴ See, e.g., New Zealand FMA Report (describing an August 2020 cybersecurity incident at New Zealand’s only regulated financial product market that caused a trading halt of approximately four days).

responsibilities as SROs. In particular, exchanges employ market-regulation systems to assist with obligations such as enforcing their rules and the federal securities laws with respect to their members. A disruption of a national securities exchange's business operations caused by a significant cybersecurity incident could disrupt its ability to carry out its regulatory responsibilities as an SRO and, therefore, materially impact the fair, orderly, and efficient functioning of the U.S. securities markets.

Each exchange also is required to keep all records made or received by it in the course of its business and in the conduct of its self-regulatory activity. The records stored by national securities exchanges on their information systems include proprietary information about their members, including confidential business information (e.g., information about the financial condition of their members). The records also include information relating to trading, routing, market data, and market surveillance, among other areas.⁹⁵ A significant cybersecurity incident at a national securities exchange could lead to the improper use of this information to harm exchange members (e.g., public exposure of confidential financial information) or provide the unauthorized user with an unfair advantage over other market participants (e.g., trading based on confidential business information).

g. Security-Based Swap Data Repositories

Title VII of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Title VII of the Dodd-Frank Act"), enacted in 2010, provided for a comprehensive, new regulatory framework for swaps and security-based swaps, including regulatory reporting and public dissemination of transactions in security-based swaps.⁹⁶ In 2015, the Commission established a regulatory framework for SBSDRs to provide improved transparency to regulators and help facilitate price discovery and efficiency in the SBS market.⁹⁷ Under this framework,

⁹⁵ For example, as discussed above, the national securities exchanges and FINRA jointly operate the CAT System, which collects and stores information relating market participants, and their order and trading activities.

⁹⁶ Public Law 111–203, 124 Stat. 1376 (2010), section 761(a) (adding Exchange Act section 3(a)(75) (defining SBSDR)) and section 763(i) (adding Exchange Act section 13(n)) (establishing a regulatory regime for SBSDRs).

⁹⁷ See *Security-Based Swap Data Repository Registration, Duties, and Core Principles*, Exchange Act Release No. 74246 (Feb. 11, 2015) [80 FR 14438 (Mar. 19, 2015)] ("SBSDR Adopting Release");

SBSDRs are registered securities information processors and disseminators of market data in the security-based swap market,⁹⁸ thereby supporting the Dodd-Frank Act's goal of public dissemination for all security-based swaps to enhance price discovery to market participants.⁹⁹ The collection and dissemination of security-based swap data by SBSDRs provide transparency in the security-based swap market for regulators and market participants.

In addition, as centralized repositories for security-based swap transaction data that is used by regulators, SBSDRs provide an important infrastructure assisting relevant authorities in performing their market oversight.¹⁰⁰ Data maintained by SBSDRs can assist regulators in addressing market abuses, performing supervision, and resolving issues and positions if an institution fails.¹⁰¹ SBSDRs are required to collect and maintain accurate security-based swap transaction data so that relevant authorities can access and analyze the data from secure, central locations, thereby putting the regulators in a better position to monitor for potential market abuse and risks to financial stability.¹⁰² SBSDRs also have the potential to reduce operational risk and enhance operational efficiency, such as by maintaining transaction records that would help counterparties to ensure

Regulation SBSR—Reporting and Dissemination of Security-Based Swap Information, Exchange Act Release No. 74244 (Feb. 11, 2015) [80 FR 14563 (Mar. 19, 2015)] ("SBSR Adopting Release").

⁹⁸ See 17 CFR 242.909 ("A registered security-based swap data repository shall also register with the Commission as a securities information processor on Form SDR"); see also Form SDR ("With respect to an applicant for registration as a security-based swap data repository, Form SDR also constitutes an application for registration as a securities information processor.").

⁹⁹ See, e.g., SBSDR Adopting Release, 80 FR at 14604.

¹⁰⁰ See *Security-Based Swap Data Repository Registration, Duties, and Core Principles*, Exchange Act Release No. 63347 (Nov. 19, 2010) [75 FR 77306, 77307 (Dec. 10, 2010)], corrected at 75 FR 79320 (Dec. 20, 2010) and 76 FR 2287 (Jan. 13, 2011) ("SBSDR Proposing Release") ("The data maintained by an [SBSDR] may also assist regulators in (i) preventing market manipulation, fraud, and other market abuses; (ii) performing market surveillance, prudential supervision, and macroprudential (systemic risk) supervision; and (iii) resolving issues and positions after an institution fails.").

¹⁰¹ See SBSDR Proposing Release at 77307.

¹⁰² See SBSDR Adopting Release, 80 FR at 14440 (stating that "[SBSDRs] are required to collect and maintain accurate [security-based swap] transaction data so that relevant authorities can access and analyze the data from secure, central locations, thereby putting them in a better position to monitor for potential market abuse and risks to financial stability.").

that their records reconcile on all of the key economic details.

SBSDRs use information systems to perform these functions, including to disseminate market data and provide price transparency in the security-based swap market. They also use information systems to operate centralized repositories for security-based swap data for use by regulators. These information systems provide an important market infrastructure that assists relevant authorities in performing their market oversight.¹⁰³ As discussed above, data maintained by SBSDRs may, for example, assist regulators in addressing market abuses, performing supervision, and resolving issues and positions if an institution fails.

SBSDRs are subject to certain cybersecurity risks that if realized could impede their ability to meet the goals set out in Title VII of the Dodd-Frank Act and the Commission's rules.¹⁰⁴ For example, SBSDRs process and disseminate trade data using information systems. If these information systems suffer from a significant cybersecurity incident, public access to timely and reliable trade data for the derivatives markets could potentially be compromised.¹⁰⁵ Also, if the data stored at an SBSDR is corrupted by a threat actor through a cybersecurity attack, the SBSDR would not be able to provide accurate data to relevant regulatory authorities, which could hinder the oversight of the derivatives markets. Moreover, SBSDRs

¹⁰³ See Committee on Payments and Settlement Systems ("CPSS"), Technical Committee of IOSCO, *Principles for financial markets intermediaries* (Apr. 2012), available at <https://www.bis.org/cpmi/publ/d101a.pdf> ("FMI Principles") (Principle for financial markets intermediaries ("PFMI") 1.14 stating that "[b]y centralising the collection, storage, and dissemination of data, a well-designed [trade repository ("TR")] that operates with effective risk controls can serve an important role in enhancing the transparency of transaction information to relevant authorities and the public, promoting financial stability, and supporting the detection and prevention of market abuse."). In 2014, the CPSS became the Committee on Payments and Market Infrastructures ("CPMI").

¹⁰⁴ See SBSDR Adopting Release, 80 FR at 14450 ("[SBSDRs] themselves are subject to certain operational risks that may impede the ability of [SBSDRs] to meet these goals, and the Title VII regulatory framework is intended to address these risks.").

¹⁰⁵ See FMI Principles (PFMI 1.14, Box 1 stating that "[t]he primary public policy benefits of a TR, which stem from the centralisation and quality of the data that a TR maintains, are improved market transparency and the provision of this data to relevant authorities and the public in line with their respective information needs. Timely and reliable access to data stored in a TR has the potential to improve significantly the ability of relevant authorities and the public to identify and evaluate the potential risks posed to the broader financial system.").

use information systems to receive and maintain personal, confidential, and proprietary information and data. The unauthorized use or access of this information could be used to create unfair business or trading advantages and, in the case of personal information, to steal identities.

Further, a significant cybersecurity incident at an SBSDR could provide a gateway for threat actors to attack Market Entities and others that connect to it through information systems. Moreover, the links established between an SBSDR and other entities, including unaffiliated clearing agencies and other SBSDRs, are vectors that expose the SBSDR to cybersecurity risk arising from threats that originate in information systems outside the SBSDR's control.¹⁰⁶

h. SBS Entities

The SBS Entities covered by the proposed rulemaking are SBSDs and MSBSPs. An SBSD generally refers to any person who: (1) holds itself out as a dealer in security-based swaps; (2) makes a market in security-based swaps; (3) regularly enters into security-based swaps with counterparties as an ordinary course of business for its own account; or (4) engages in any activity causing it to be commonly known in the trade as a dealer or market maker in security-based swaps.¹⁰⁷ An SBSD does not, however, include a person that enters into security-based swaps for such person's own account, either

individually or in a fiduciary capacity, but not as a part of regular business.¹⁰⁸

An MSBSP generally includes any person that is not a security-based swap dealer and that satisfies one of the following three alternative statutory tests: (1) it maintains a "substantial position" in security-based swaps, excluding positions held for hedging or mitigating commercial risk and positions maintained by any employee benefit plan (or any contract held by such a plan) for the primary purpose of hedging or mitigating any risk directly associated with the operation of the plan, for any of the major security-based swap categories determined by the Commission; (2) its outstanding security-based swaps create substantial counterparty exposure that could have serious adverse effects on the financial stability of the U.S. banking system or financial markets; or (3) it is a "financial entity" that is "highly leveraged" relative to the amount of capital it holds (and that is not subject to capital requirements by an appropriate federal banking agency) and maintains a "substantial position" in outstanding security-based swaps in any major category as determined by the Commission.¹⁰⁹ Currently, there are no MSBSPs registered with the Commission.

SBS Entities play (or, in the case of MSBSPs, could play) a critical role in the U.S. security-based swap market.¹¹⁰ SBS Entities rely on information systems to transact in security-based swaps with other market participants, to receive and deliver collateral, to create and maintain books and records, and to obtain market information to update books and records, and manage risk.

A disruption to an SBS Entity's operations caused by a significant cybersecurity incident could have a large negative impact on the U.S. security-based swap market given the concentration of dealers in this market. Further, a disruption in the security-based swap market could negatively impact the broader securities markets by, for example, causing participants to liquidate positions related to, or referenced by, the impacted security-based swaps to mitigate losses to participants' positions or portfolios or due to loss of trading confidence. A disruption in the security-based swap market also could negatively impact the broader securities markets by causing

participants to liquidate the collateral margining the security-based swaps for similar reasons or to cover margin calls. The consequences of a business disruption to an SBS Entity's functions—such as those that may be caused by a significant cybersecurity incident—may be amplified because, unlike many other securities transactions, securities-based swap transactions give rise to an ongoing obligation between transaction counterparties during the life of the transaction.¹¹¹ This means that each counterparty bears the risk of its counterparty's ability to perform under the terms of a security-based swap until the transaction is terminated. A disruption of an SBS Entity's normal business activities because of a significant cybersecurity incident could produce spillover or contagion by negatively affecting the willingness or the ability of market participants to extend credit to each other, and could substantially reduce liquidity and valuations for particular types of financial instruments.¹¹² The security-based swap market is large¹¹³ and thus a disruption of an SBS Entity's operations due to a significant cybersecurity incident could negatively impact sectors of the U.S. economy.¹¹⁴

Further, a significant cybersecurity incident at an SBS Entity could provide a gateway for threat actors to attack the exchanges, SBSDRs, clearing agencies, counterparties, and other SBS Entities to

¹⁰⁶ See FMI Principles (PFMI) at 3.20.20 stating that "[a] TR should carefully assess the additional operational risks related to its links to ensure the scalability and reliability of IT and related resources. A TR can establish links with another TR or with another type of FMI. Such links may expose the linked [financial market infrastructures ("FMIs")] to additional risks if not properly designed. Besides legal risks, a link to either another TR or to another type of FMI may involve the potential spillover of operational risk. The mitigation of operational risk is particularly important because the information maintained by a TR can support bilateral netting and be used to provide services directly to market participants, service providers (for example, portfolio compression service providers), and other linked FMIs." The CPMI and IOSCO issued guidance for cyber resilience for FMIs, including CSDs, securities settlement systems ("SSSs"), CCPs, and trade repositories. See CPMI-IOSCO, *Guidance on cyber resilience for financial market infrastructures* (June 2016), available at <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf>; see also CPMI-IOSCO, *Implementation monitoring of the PFMI: Level 3 assessment on Financial Market Infrastructures' Cyber Resilience* (Nov. 2022), available at <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD723.pdf> (presenting the results of an assessment of the state of cyber resilience (as of February 2021) of FMIs from 29 jurisdictions that participated in the exercise in 2020 to 2022).

¹⁰⁷ See 15 U.S.C. 78c(a)(71); 17 CFR 240.3a71-1 *et seq.*

¹⁰⁸ See 15 U.S.C. 78c(a)(71)(C); 17 CFR 240.3a71-1(b).

¹⁰⁹ See 15 U.S.C. 78c(a)(67); 17 CFR 240.3a67-1 *et seq.*

¹¹⁰ Currently, this role is fulfilled by SBSDs, given there are no MSBSPs registered with the Commission.

¹¹¹ See *Further Definition of "Swap Dealer," "Security-Based Swap Dealer," "Major Swap Participant," "Major Security-Based Swap Participant" and "Eligible Contract Participant"*, Exchange Act Release No. 66868 (Apr. 27, 2012) [77 FR 30596, 30616-17 (May 23, 2012)] ("Further Definition Release") (noting that "[i]n contrast to a secondary market transaction involving equity or debt securities, in which the completion of a purchase or sale transaction can be expected to terminate the mutual obligations of the parties to the transaction, the parties to a security-based swap often will have an ongoing obligation to exchange cash flows over the life of the agreement").

¹¹² See *Cross-Border Security-Based Swap Activities; Re-Proposal of Regulation SBSR and Certain Rules and Forms Relating to the Registration of Security-Based Swap Dealers and Major Security-Based Swap Participants*, Exchange Act Release No. 69490 (May 1, 2013) [78 FR 30967, 30980-81 (May 23, 2013)] ("Cross-Border Proposing Release").

¹¹³ See, e.g., Commission, *Report on Security-Based Swaps Pursuant to Section 13(m)(2) of the Securities Exchange Act of 1934* (July 15, 2022) available at <https://www.sec.gov/files/report-on-security-based-swaps-071522.pdf>.

¹¹⁴ See Cross-Border Proposing Release, 78 FR at 30972 ("The Dodd-Frank Act was enacted, among other reasons, to promote the financial stability of the United States by improving accountability and transparency in the financial system. The 2008 financial crisis highlighted significant issues in the over-the-counter ("OTC") derivatives markets, which . . . are capable of affecting significant sectors of the U.S. economy.") (footnotes omitted).

which the firm is connected through information systems and networks of interconnected information systems. Moreover, the information systems that link SBS Entities to other Market Entities are vectors that expose the SBS Entity to cybersecurity risk arising from threats that originate in information systems outside the SBS Entity's control. SBS Entities also store proprietary and confidential information about their counterparties on their information systems, including financial information they use to perform credit analysis. A significant cybersecurity incident at an SBS Entity could lead to the improper use of this information to harm the counterparties (e.g., public exposure of confidential financial information) or provide the unauthorized user with an unfair advantage over other market participants (e.g., trading based on confidential business information).

i. Transfer Agents

A transfer agent is any person who engages on behalf of an issuer of securities or on behalf of itself as an issuer of securities in (among other functions): (1) tracking, recording, and maintaining the official record of ownership of each issuer's securities; (2) canceling old certificates, issuing new ones, and performing other processing and recordkeeping functions that facilitate the issuance, cancellation, and transfer of those securities; (3) facilitating communications between issuers and registered securityholders; and (4) making dividend, principal, interest, and other distributions to securityholders.¹¹⁵ To perform these functions, transfer agents maintain records and information related to securityholders that may include names, addresses, phone numbers, email addresses, employers, employment history, bank and specific account information, credit card information, transaction histories, securities holdings, and other detailed and individualized information related to the transfer agents' recordkeeping and transaction processing on behalf of issuers. With advances in technology and the expansion of book-entry ownership of securities, transfer agents today increasingly rely on technology and automation to perform the core recordkeeping, processing, and transfer services described above, including the use of computer systems to store, access, and process the information related to securityholders they maintain on behalf

of issuers. A significant cybersecurity incident that impacts these systems could cause harm to investors by, for example, preventing the transfer agent from transferring ownership of securities or preventing investors from receiving dividend, interest, or principal payments.

Further, a significant cybersecurity incident at a transfer agent could provide a gateway for threat actors to attack other Market Entities that connect to it through information systems and networks of interconnected information systems. Moreover, the information systems that link transfer agents to other Market Entities expose the transfer agent to cybersecurity risk arising from threats that originate in information systems outside the transfer agent's control. The records stored by transfer agents on their information systems include proprietary information about securities ownership and corporate actions. A significant cybersecurity incident at a transfer agent could lead to the improper use of this information to harm securities holders (e.g., public exposure of their confidential financial information or the use of that information to steal their identities) or provide the unauthorized user with an unfair advantage over other market participants (e.g., trading based on confidential business information).

B. Overview of the Proposed Cybersecurity Requirements

As discussed above, the U.S. securities markets are part of the critical infrastructure of the United States.¹¹⁶ In this regard, they play a central role in the U.S. economy in terms of facilitating the flow of capital, including the savings of individual investors. The fair, orderly, and efficient operation of the U.S. securities markets depends on Market Entities being able to perform their critical functions, and Market Entities are increasingly relying on information systems and interconnected networks of information systems to perform these functions. These information systems are targets of threat actors. Moreover, Market Entities—as financial institutions—are choice targets for threat actors seeking financial gain or to inflict economic harm. Further, threat actors are using increasingly sophisticated and constantly evolving tactics, techniques, and procedures to attack information systems. In addition to threat actors, cybersecurity risk also can be caused by the errors of employees, service providers, or

business partners. The interconnectedness of Market Entities increases the risk that a significant cybersecurity incident can simultaneously impact multiple Market Entities causing harm to the U.S. securities markets.

For these reasons, it is critically important that Market Entities take steps to protect their information systems and the information residing on those systems from cybersecurity risk. A Market Entity that fails to do so is more vulnerable to succumbing to a significant cybersecurity incident. As discussed above, a significant cybersecurity incident can cause serious harm not only to the Market Entity but also to its customers, counterparties, members, registrants, or users, or to any other market participants (including other Market Entities) that interact with the Market Entity. Therefore, it is vital to the U.S. securities markets and the participants in those markets that *all* Market Entities address cybersecurity risk, which, as discussed above, is increasingly threatening the financial sector.

Consequently, the Commission is proposing new Rule 10 and new Form SCIR to require that Market Entities address cybersecurity risks, to improve the Commission's ability to obtain information about significant cybersecurity incidents impacting Market Entities, and to improve transparency about the cybersecurity risks that can cause adverse impacts to the U.S. securities markets.¹¹⁷ Under proposed Rule 10, certain broker-dealers, the MSRB, and all clearing agencies, national securities associations, national securities exchanges, SBSDRs, SBS Entities, and transfer agents would be defined as a "covered entity" (collectively, "Covered Entities").¹¹⁸

¹¹⁷ In designing the requirements of proposed Rule 10, the Commission considered several cybersecurity sources (which are cited in the relevant sections below), including the NIST Framework, the NIST Glossary, and CISA's *Cyber Essentials Starter Kit* (information about CISA's *Cyber Essentials Starter Kit* is available at: <https://www.cisa.gov/publication/cisa-cyber-essentials>). The Commission also considered definitions in relevant federal statutes including the Federal Information Security Modernization Act of 2014, Public Law 113–283 (Dec. 18, 2014); 44 U.S.C. 3551 *et seq.* ("FISMA") and the Cyber Incident Reporting for Critical Infrastructure Act of 2022, H.R. 2471, 117th Cong. (2021–2022); 6 U.S.C. 681 *et seq.* ("CIRCLA").

¹¹⁸ The following broker-dealers would be Covered Entities: (1) broker-dealers that maintain custody of securities and cash for customers or other broker-dealers ("carrying broker-dealers"); (2) broker-dealers that introduce their customer accounts to a carrying broker-dealer on a fully disclosed basis ("introducing broker-dealers"); (3) broker-dealers with regulatory capital equal to or

¹¹⁵ See *Transfer Agent Regulations*, Exchange Act Release No. 76743 (Dec. 22, 2015) [80 FR 81948, 81949 (Dec. 31, 2015)].

¹¹⁶ See section I.A. of this release (discussing cybersecurity risk and how critical operations of Market Entities are exposed to cybersecurity risk).

Proposed Rule 10 would require all Market Entities (Covered Entities and Non-Covered Entities) to establish, maintain, and enforce written policies and procedures that are reasonably designed to address their cybersecurity risks.¹¹⁹ All Market Entities also, at least annually, would be required to review and assess the design and effectiveness of their cybersecurity policies and procedures, including whether the policies and procedures reflect changes in cybersecurity risk over the time period covered by the review.¹²⁰ They also would be required to prepare a report (in the case of Covered Entities) and a record (in the case of Non-Covered Entities) with respect to the annual review. CISA states that organizations should “approach cyber as business risk.”¹²¹ Like other business risks (e.g., market, credit, or liquidity risk), cybersecurity risk can be addressed through policies and procedures that are reasonably designed to manage the risk. Finally, all Market Entities would need to give the Commission immediate written electronic notice of a significant cybersecurity incident upon having a reasonable basis to conclude that the

exceeding \$50 million; (4) broker-dealers with total assets equal to or exceeding \$1 billion; (5) broker-dealers that operate as market makers; and (6) broker-dealers that operate an ATS (sometimes collectively referred to as “Covered Broker-Dealers”). Broker-dealers that do not fall into one of these six categories (sometimes collectively referred to as “Non-Covered Entities” or “Non-Covered Broker-Dealers”) would not be Covered Entities for the purposes of proposed Rule 10. *See also* section II.A.1.b. of this release (discussing the categories of broker-dealers that would be “Covered Entities” in greater detail).

¹¹⁹ *See* paragraphs (b) through (d) of proposed Rule 10 (setting forth the requirements for Market Entities that meet the definition of “covered entity”); paragraph (e)(1) of proposed Rule 10 (setting forth the requirements for Market Entities that are not Covered Entities (i.e., Non-Covered Broker-Dealers)). *See also* sections II.B.1. and II.C. of this release (discussing these proposed requirements in more detail). As discussed in sections II.F. and IV.C.1.b. of this release, certain categories of Market Entities are subject to existing requirements to address aspects of cybersecurity risk or that may relate to cybersecurity. These other requirements, however, do not address cybersecurity risk as directly, broadly, or comprehensively as the requirements of proposed Rule 10.

¹²⁰ *See* paragraph (b)(2) of proposed Rule 10; paragraph (e)(1) of proposed Rule 10. *See also* sections II.B.1.f. and II.C. of this release (discussing these proposed requirements in more detail).

¹²¹ *See* CISA Cyber Essentials Starter Kit (“Ask yourself what type of impact would be catastrophic to your operations? What information if compromised or breached would cause damage to employees, customers, or business partners? What is your level of risk appetite and risk tolerance? Raising the level of awareness helps reinforce the culture of making informed decisions and understanding the level of risk to the organization.”).

significant cybersecurity incident has occurred or is occurring.¹²²

Market Entities that meet the definition of “covered entity” would be subject to certain additional requirements under proposed Rule 10.¹²³ First, as discussed in more detail below, the written policies and procedures that Covered Entities would need to establish, maintain, and enforce would need to include the following elements:

- Periodic assessments of cybersecurity risks associated with the Covered Entity’s information systems and written documentation of the risk assessments;
- Controls designed to minimize user-related risks and prevent unauthorized access to the Covered Entity’s information systems;
- Measures designed to monitor the Covered Entity’s information systems and protect the Covered Entity’s information from unauthorized access or use, and oversee service providers that receive, maintain, or process information, or are otherwise permitted to access the Covered Entity’s information systems;
- Measures to detect, mitigate, and remediate any cybersecurity threats and vulnerabilities with respect to the Covered Entity’s information systems; and

- Measures to detect, respond to, and recover from a cybersecurity incident and written documentation of any cybersecurity incident and the response to and recovery from the incident.¹²⁴

Second, Covered Entities—in addition to providing the Commission with immediate written electronic notice of a significant cybersecurity incident—would need to report and update information about the significant cybersecurity incident by filing Part I of proposed Form SCIR with the Commission.¹²⁵ The form would elicit information about the significant

¹²² *See* paragraph (c)(1) of proposed Rule 10; paragraph (e)(2) of proposed Rule 10. *See also* sections II.B.2.a. and II.C. of this release (discussing these proposed requirements in more detail).

¹²³ *Compare* paragraphs (b) through (d) of proposed Rule 10 (setting forth the requirements for Covered Entities), *with* paragraph (e) of proposed Rule 10 (setting forth the requirements for Non-Covered Entities).

¹²⁴ *See* sections II.B.1.a. through II.B.1.e. of this release (discussing these proposed requirements in more detail). In the case of Non-Covered Entities, as discussed in more detail below in section II.C. of this release, the design of the cybersecurity risk management policies and procedures would need to take into account the size, business, and operations of the broker-dealer. *See* paragraph (e) of proposed Rule 10.

¹²⁵ *See* sections II.B.2. and II.B.4. of this release (discussing these proposed requirements in more detail).

cybersecurity incident and the Covered Entity’s efforts to respond to, and recover from, the incident.

Third, Covered Entities would need to disclose publicly summary descriptions of their cybersecurity risks and the significant cybersecurity incidents they experienced during the current or previous calendar year on Part II of proposed Form SCIR.¹²⁶ The form would need to be filed with the Commission and posted on the Covered Entity’s business internet website. Covered Entities that are carrying or introducing broker-dealers also would need to provide the form to customers at account opening, when information on the form is updated, and annually.

Covered Entities and Non-Covered Entities would need to preserve certain records relating to the requirements of proposed Rule 10 in accordance with amended or existing recordkeeping requirements applicable to them or, in the case of exempt clearing agencies, pursuant to conditions in relevant exemption orders.¹²⁷

Finally, the Commission is proposing amendments to address the potential availability of substituted compliance to non-U.S. SBS Entities with respect to the proposed cybersecurity requirements.¹²⁸

In developing the proposed requirements summarized above with regard to SBSDRs and SBS Entities, the Commission consulted and coordinated with the CFTC and the prudential regulators in accordance with section 712(a)(2) of Title VII of the Dodd-Frank Act. In accordance with section 752 of Title VII of the Dodd-Frank Act, the Commission has consulted and coordinated with foreign regulatory authorities through Commission staff participation in numerous bilateral and multilateral discussions with foreign regulatory authorities addressing the regulation of OTC derivatives markets.

II. Discussion of Proposed Cybersecurity Rule

A. Definitions

Proposed Rule 10 would define a number of terms for the purposes of its requirements.¹²⁹ These definitions also would be used for the purposes of Parts

¹²⁶ *See* sections II.B.3. and II.B.4. of this release (discussing these proposed requirements in more detail).

¹²⁷ *See* sections II.B.5. and II.C. of this release (discussing these proposed requirements in more detail).

¹²⁸ *See* sections II.D. of this release (discussing these proposed amendments in more detail).

¹²⁹ *See* paragraph (a) of proposed Rule 10.

I and II of proposed Form SCIR.¹³⁰ The defined terms are intended to tailor the risk management, notification, reporting, and disclosure requirements of proposed Rule 10 to the distinctive aspects of cybersecurity risk as compared with other risks Market Entities face (e.g., market, credit, or liquidity risk).¹³¹

1. “Covered Entity”

a. Market Entities That Meet the Definition of “Covered Entity” Would Be Subject to Additional Requirements

Proposed Rule 10 would define the term “covered entity” to identify the types of Market Entities that would be subject to certain additional requirements under the rule.¹³² As discussed above, proposed Rule 10 would require all Market Entities to establish, maintain, and enforce written policies and procedures that are reasonably designed to address their cybersecurity risks.¹³³ All Market Entities also, at least annually, would be required to review and assess the design and effectiveness of their cybersecurity risk management policies and procedures, including whether the policies and procedures reflect changes in cybersecurity risk over the time period covered by the review.¹³⁴ They also would be required to prepare a report (in the case of Covered Entities) or a record (in the case of Non-Covered Entities) with respect to the annual review. Further, all Market Entities would need to give the Commission immediate written electronic notice of a

¹³⁰ See sections II.B.2. and II.B.3. of this release (discussing Parts I and II of proposed Form SCIR in more detail).

¹³¹ See paragraphs (a)(2) through (9) of proposed Rule 10 (defining, respectively, the terms “cybersecurity incident,” “cybersecurity risk,” “cybersecurity threat,” “cybersecurity vulnerability,” “information,” “information systems,” “personal information,” and “significant cybersecurity incident”).

¹³² See paragraphs (a)(1)(i) through (ix) of proposed Rule 10 (defining these Market Entities as “covered entities”). A Market Entity that falls within the definition of “covered entity” for purposes of proposed Rule 10 may not necessarily meet the definition of a “covered entity” for purposes of certain federal statutes, such as, but not limited to, CIRCIA and any regulations promulgated thereunder. CIRCIA, among other things, requires the Director of CISA to issue and implement regulations defining the term “covered entity” and requiring covered entities to report covered cyber incidents and ransom payments as the result of ransomware attacks to CISA in certain instances.

¹³³ See paragraph (b)(1) of proposed Rule 10 (setting forth the requirement for Market Entities that meet the definition of “covered entity”); paragraph (e)(1) of proposed Rule 10 (setting forth the requirement for Market Entities that do not meet the definition of “covered entity,” which, as discussed above, would be certain smaller broker-dealers).

¹³⁴ See paragraph (b)(2) of proposed Rule 10; paragraph (e)(1) of proposed Rule 10.

significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring.¹³⁵ As discussed above, Market Entities use information systems that expose them to cybersecurity risk and that risk is increasing due to the interconnectedness of the information systems and the sophistication of the tactics used by threat actors. Therefore, regardless of their function, interconnectedness, or size, all Market Entities would be subject to these requirements designed to address cybersecurity risks.

Market Entities that are Covered Entities would be subject to certain additional requirements under proposed Rule 10.¹³⁶ In particular, they would be required to: (1) include certain elements in their cybersecurity risk management policies and procedures;¹³⁷ (2) file Part I of proposed Form SCIR with the Commission and, for some Covered Entities, other regulators to report information about a significant cybersecurity incident;¹³⁸ and (3) make public disclosures on Part II of proposed Form SCIR about their cybersecurity risks and the significant cybersecurity incidents they experienced during the current or previous calendar year.¹³⁹

In determining which Market Entities would be Covered Entities subject to the additional requirements, the Commission considered: (1) how the type of Market Entity supports the fair, orderly, and efficient operation of the U.S. securities markets and the consequences if that type of Market Entity’s critical functions were disrupted or degraded by a significant cybersecurity incident; (2) the harm that could befall investors, including retail investors, if that type of Market Entity’s functions were disrupted or degraded by a significant cybersecurity incident; (3)

¹³⁵ See paragraph (c)(1) of proposed Rule 10 (setting forth the requirement for Market Entities that meet the definition of “covered entity”); paragraph (e)(2) of proposed Rule 10 (setting forth the requirement for Market Entities that do not meet the definition of “covered entity”).

¹³⁶ See paragraphs (b) through (d) of proposed Rule 10 (setting forth the requirements for Covered Entities); paragraph (e) of proposed Rule 10 (setting forth the requirements for Non-Covered Entities). As discussed above, Covered Entities would need to prepare a report with respect to their review and assessment of the policies and procedures. See paragraph (b)(2) of proposed Rule 10. Non-Covered Entities would need to make a record with the respect to the annual review and assessment of their policies and procedures. See paragraph (e) of proposed Rule 10.

¹³⁷ See paragraphs (b)(1)(i) through (v) of proposed Rule 10.

¹³⁸ See paragraph (c)(2) of proposed Rule 10. See also paragraph (a)(10) of proposed Rule 10 (defining the term “significant cybersecurity risk”).

¹³⁹ See paragraph (d) of proposed Rule 10.

the extent to which that type of Market Entity poses cybersecurity risk to other Market Entities through information system connections, including the number of connections; (4) the extent to which the that type of Market Entity would be an attractive target for threat actors; and (5) the personal, confidential, and proprietary business information about the type of Market Entity and other persons (e.g., investors) stored on the Market Entity’s information systems and the harm that could be caused if that information was accessed or used by threat actors.

b. Broker-Dealers

The following broker-dealers registered with the Commission would be Covered Entities: (1) broker-dealers that maintain custody of securities and cash for customers or other broker-dealers (i.e., carrying broker-dealers); (2) broker-dealers that introduce their customers’ accounts to a carrying broker-dealer on a fully disclosed basis (i.e., introducing broker-dealers);¹⁴⁰ (3) broker-dealers with regulatory capital equal to or exceeding \$50 million; (4) broker-dealers with total assets equal to or exceeding \$1 billion; (5) broker-dealers that operate as market makers; and (6) broker-dealers that operate an ATS. Thus, under proposed Rule 10, these six categories of broker-dealers would be subject to the additional requirements.¹⁴¹ All other types of

¹⁴⁰ When a broker-dealer introduces a customer to a carrying broker-dealer on a fully disclosed basis, the carrying broker-dealer knows the identity of the customer and holds cash and securities in an account for the customer that identifies the customer as the accountholder. This is distinguishable from a broker-dealer that introduces its customers to another carrying broker-dealer on an omnibus basis. In this scenario, the carrying broker-dealer does not know the identities of the customers and holds their cash and securities in an account that identifies the broker-dealer introducing the customers on an omnibus basis as the accountholder. A broker-dealer that introduces customers to another broker-dealer on an omnibus basis is, itself, a carrying broker-dealer for purposes of the Commission’s financial responsibility rules, including, the broker-dealer net capital and customer protection rules. See, e.g., 17 CFR 240.15c3-1 and 17 CFR 240.15c3-3. This category of broker-dealer would be a carrying broker-dealer for purposes of proposed Rule 10 and therefore subject to the rule’s requirements for Covered Entities.

¹⁴¹ See paragraphs (a)(1)(i)(A) through (F) of proposed Rule 10. Certain of the definitions in proposed Rule 10 would be used for the purposes of the requirements in the rule for broker-dealers that are not Covered Entities. Specifically, paragraph (e)(1) of proposed Rule 10 would require broker-dealers that are not Covered Entities to establish, maintain, and enforce written policies and procedures that are reasonably designed to address the *cybersecurity risks* of the broker-dealer taking into account the size, business, and operations of the broker-dealer. The term “cybersecurity risk” is defined in paragraph (a)(3) of proposed Rule 10 and that definition

broker-dealers would not meet the definition of Covered Entity.¹⁴²

The first category of broker-dealers included as Covered Entities would be carrying broker-dealers. Specifically, proposed Rule 10 would define “covered entity” to include any broker-dealer that maintains custody of cash and securities for customers or other broker-dealers and is not exempt from the requirements of Exchange Act Rule 15c3–3 (*i.e.*, a carrying broker-dealer).¹⁴³ Some carrying broker-dealers are large in terms of their assets and dealing activities or the number of their account holders. For example, they may engage in a variety of order handling, trading, and/or clearing activities, and thereby play a significant role in U.S. securities markets, often through multiple business lines and/or in multiple asset classes. Consequently, if their critical functions were disrupted or degraded by a significant cybersecurity incident it could have a potential negative impact on the U.S. securities markets by, for example, reducing liquidity in the markets or sectors of the markets due to the firm’s inability to continue dealing and trading activities. A broker-dealer in this situation could lose its ability to provide liquidity to other market participants for an indeterminate length of time, which could lead to unfavorable market conditions for investors, such as higher buy prices and lower sell prices or even the inability to execute a trade within a reasonable amount of time. Further, some carrying broker-dealers hold millions of accounts for investors. If a

incorporates the terms “cybersecurity incident,” “cybersecurity threat,” and “cybersecurity vulnerability,” which are defined, respectively, in paragraphs (a)(2), (a)(4), and (a)(5) of proposed Rule 10. In addition, paragraph (e)(2) of proposed Rule 10 would require broker-dealers that are not Covered Entities to provide immediate written electronic notice to the Commission and their examining authority if they experience a “significant cybersecurity incident” as that term is defined in the rule. Therefore, paragraph (a)(8) of proposed Rule 10 would define the term “market entity” to mean a Covered Entity and a broker-dealer registered with the Commission that is not a Covered Entity. Further, the definitions in proposed Rule 10 would refer to “market entities” (rather than “covered entities”) in order to not limit the application of these definitions to paragraphs (b) through (d) of proposed Rule 10, which set forth the requirements for Covered Entities (but not for Non-Covered Entities).

¹⁴² As discussed below in section IV.C.2. of this release, of the 3,510 broker-dealers registered with the Commission as of the third quarter of 2022, 1,541 would meet the definition of “covered entity” under proposed Rule 10, leaving 1,969 broker-dealers as Non-Covered Entities.

¹⁴³ See paragraph (a)(1)(i)(A) of proposed Rule 10. See also 17 CFR 240.15c3–3 (“Rule 15c3–3”). Rule 15c3–3 sets forth requirements for broker-dealers that maintain custody of customer securities and cash that are designed to protect those assets and ensure their prompt return to the customers.

significant cybersecurity incident prevented this investor-base from accessing the securities markets, it could impact liquidity as well.

Also, the dealing activities of carrying broker-dealers may make them attractive targets for threat actors seeking to access proprietary and confidential information about the broker-dealer’s trading positions and strategies to use for financial advantage. In addition, the size and financial resources of carrying broker-dealers may make them attractive targets for threat actors employing ransomware schemes.

Because carrying broker-dealers hold cash and securities for customers and other broker-dealers, a significant cybersecurity incident could put these assets in peril or make them unavailable. For example, a significant cybersecurity incident could cause harm to the investors that own these assets—including retail investors—if it causes the investors to lose access to their securities accounts (and, therefore, the ability to purchase or sell securities), causes the failure of the carrying broker-dealer (which could tie up the assets in a liquidation proceeding under the Securities Investor Protection Act), or, in the worst case, results in the assets being stolen. The fact that carrying broker-dealers hold cash and securities for investors also may make them attractive targets for threat actors seeking to steal those assets through hacking the accounts or using stolen credentials and log-in information. In addition, carrying broker-dealers with large numbers of customers might be attractive targets for threat actors because of the volume of personal information they maintain. Threat actors may seek to access and download this information in order to sell it to other threat actors. If this information is accessed or stolen by threat actors, it could result in harm (*e.g.*, identity theft or conversion of financial assets) to many individuals, including retail investors. Carrying broker-dealers typically are connected to a number of different Market Entities through information systems, including national securities exchanges, clearing agencies, and other broker-dealers (including introducing broker-dealers).

The second category of broker-dealers included as Covered Entities would be introducing broker-dealers.¹⁴⁴ These broker-dealers introduce customer accounts on a fully disclosed basis to a carrying broker-dealer. In this arrangement, the carrying broker-dealer knows the identities of the fully disclosed customers and maintains

custody of their securities and cash. The introducing broker-dealer typically interacts directly with the customers by, for example, making securities recommendations and accepting their orders to purchase or sell securities. An introducing broker-dealer must enter into an agreement with a carrying broker-dealer to which it introduces customer accounts on a fully disclosed basis.¹⁴⁵

These broker-dealers would be included as Covered Entities because they are a conduit to their customers’ accounts at the carrying broker-dealer and have access to information and trading systems of the carrying broker-dealer. Consequently, a significant cybersecurity incident could harm their customers to the extent it causes the customers to lose access to their securities accounts at the carrying broker-dealer. Further, a significant cybersecurity incident at an introducing broker-dealer could spread to the carrying broker-dealer given the information systems that connect the two firms. These connections also may make introducing broker-dealers attractive targets for threat actors seeking to access the information systems of the carrying broker-dealer to which the introducing broker-dealer is connected.

In addition, introducing broker-dealers may store personal information about their customers on their information systems or be able to access this information on the carrying broker-dealer’s information systems. The fact that they store this information also may make them attractive targets for threat actors seeking to use the information to steal identities or assets, or to sell the personal information to other bad actors who will seek to use it for these purposes.

The third category of broker-dealers included as Covered Entities would be broker-dealers that have regulatory capital equal to or exceeding \$50 million.¹⁴⁶ Regulatory capital is the total capital of the broker-dealer plus allowable subordinated liabilities of the broker-dealer and is reported on the FOCUS reports broker-dealers file

¹⁴⁵ See FINRA Rule 4311. Pursuant to FINRA requirements, the carrying agreement must specify the responsibilities of the carrying broker-dealer and the introducing broker-dealer, including, at a minimum, the responsibilities for: (1) opening and approving accounts; (2) accepting of orders; (3) transmitting of orders for execution; (4) executing of orders; (5) extending credit; (6) receiving and delivering of funds and securities; (7) preparing and transmitting confirmations; (8) maintaining books and records; and (9) monitoring of accounts. See FINRA Rule 4311(c)(1).

¹⁴⁶ See paragraph (a)(1)(i)(C) of proposed Rule 10.

¹⁴⁴ See paragraph (a)(1)(i)(B) of proposed Rule 10.

pursuant to Rule 17a-5.¹⁴⁷ The fourth category would be a broker-dealer with total assets equal to or exceeding \$1 billion.¹⁴⁸ The \$50 million and \$1 billion thresholds are modeled on the thresholds that trigger enhanced recordkeeping and reporting requirements for certain broker-dealers pursuant to Exchange Act Rules 17h-1T and 17h-2T.¹⁴⁹

These thresholds are designed to include as Covered Entities broker-dealers that are large in terms of their assets and dealing activities (and that would not otherwise be Covered Broker-Dealers under the definitions in proposed Rule 10).¹⁵⁰ For example, larger broker-dealers that exceed these thresholds often engage in proprietary trading (including high frequency trading) and are sources of liquidity in certain securities. Consequently, if their critical functions were disrupted or degraded by a significant cybersecurity incident it could have a potential negative impact on those securities markets if it reduces liquidity in the markets through the inability to continue dealing and trading activities. For example, a broker-dealer in this situation could lose its ability to provide liquidity to other market participants for an indeterminate length of time, which could lead to unfavorable market conditions for investors, such as higher buy prices and lower sell prices or even the ability to execute a trade within a reasonable amount of time.

In addition, the size and dealing activities of these broker-dealers could make them attractive targets for threat actors seeking to access proprietary and confidential information about the broker-dealer's trading positions and

strategies to use for financial advantage. This also may make them attractive targets for threat actors employing ransomware schemes. Further, given their size and trading activities, these broker-dealers may be connected to a number of different Market Entities through information systems, including national securities exchanges, clearing agencies, other broker-dealers, and ATSS.

The fifth category of broker-dealers included as Covered Entities would be broker-dealers that operate as market makers. Specifically, proposed Rule 10 would define "covered entity" to include a broker-dealer that operates as a market maker under the Exchange Act or the rules thereunder (which includes a broker-dealer that operates pursuant to Exchange Act Rule 15c3-1(a)(6)) or is a market maker under the rules of an SRO of which the broker-dealer is a member.¹⁵¹ The proposed rule's definition of "market maker" is tied to securities laws that confer benefits or impose requirements on market makers and, consequently, covers broker-dealers that take advantage of those benefits or are subject to those requirements. The objective is to rely on these other securities laws to define a market maker rather than set forth a new definition of "market maker" in proposed Rule 10, which could conflict with these other laws.

Market makers would be included as Covered Entities because disruptions to their operations caused by a significant cybersecurity incident could have a material impact on the fair, orderly, and efficient functioning of the U.S. securities markets. For example, a significant cybersecurity incident could imperil a market maker's operations and ability to facilitate transactions in particular securities between buyers and sellers. In addition, market makers typically are connected to a number of different Market Entities through information systems, including national securities exchanges and other broker-dealers.

The sixth category of broker-dealers included as Covered Entities would be broker-dealers that operate an ATS.¹⁵² Since Regulation ATS was adopted in 1998, ATSS have become increasingly important venues for trading securities

in a fast and automated manner. ATSS perform exchange-like functions such as offering limit order books and other order types. These developments have made ATSS significant sources of orders and trading interest for securities. ATSS use data feeds, algorithms, and connectivity to perform these functions. ATSS rely heavily on information systems to perform these functions, including to connect to other Market Entities such as broker-dealers and principal trading firms.

A significant cybersecurity incident that disrupts an ATS could negatively impact the ability of investors to liquidate or purchase certain securities at favorable or predictable prices or in a timely manner to the extent it provides liquidity to the market for those securities. Further, a significant cybersecurity incident at an ATS could provide a gateway for threat actors to attack other Market Entities that connect to it through information systems and networks of interconnected information systems. In addition, ATSS are connected to a number of different Market Entities through information systems, including national securities exchanges and other broker-dealers. Finally, the records stored by ATSS on their information systems include proprietary information about the Market Entities that use their services, including confidential business information (e.g., information about their trading activities).

For the foregoing reasons, the categories of broker-dealers discussed above would be Covered Entities under proposed Rule 10. All other categories of broker-dealers would be Non-Covered Entities.

Generally, the types of broker-dealers that would be Non-Covered Entities under proposed Rule 10 are smaller firms whose functions do not play as significant a role in promoting the fair, orderly, and efficient operation of the U.S. securities markets, as compared to broker-dealers that would be Covered Entities.¹⁵³ For example, they tend to offer a more focused and limited set of services such as facilitating private placements of securities, selling mutual funds and variable contracts, underwriting securities, and participating in direct investment

¹⁴⁷ See 17 CFR 240.17a-5; Form X-17A-5, Line Item 3550.

¹⁴⁸ See paragraph (a)(1)(i)(D) of proposed Rule 10.

¹⁴⁹ See 17 CFR 240.17h-1T and 17h-2T. See also *Order Under Section 17(h)(4) of the Securities Exchange Act of 1934 Granting Exemption from Rule 17h-1T and Rule 17h-2T for Certain Broker-Dealers Maintaining Capital, Including Subordinated Debt of Greater Than \$20 Million But Less Than \$50 Million*, Exchange Act Release No. 89184 (June 29, 2020) [85 FR 40356 (July 6, 2020)] ("17h Release") (setting forth the \$50 million and \$1 billion thresholds).

¹⁵⁰ Size has been recognized as a proxy for substantial market activity relative to other registrants of the same type and therefore a firm's relative risk to the financial markets. See 17h Release (noting that broker-dealers that have less than \$50 million in regulatory capital and less than \$1 billion in total assets are "relatively small in size," and "because of their relative size" and to the extent they are not carrying firms, these entities "present less risk to the financial markets," while stating that with respect to broker-dealers with at least \$50 million in regulatory capital or at least \$1 billion in total assets "the Commission believes . . . those broker-dealers . . . pose greater risk to the financial markets, investors, and other market participants").

¹⁵¹ See paragraph (a)(1)(i)(E) of proposed Rule 10. See also 17 CFR 240.15c3-1 ("Rule 15c3-1"). Paragraph (a)(6) of Rule 15c3-1 permits a market maker to avoid taking capital charges for its proprietary positions provided, among other things, its carrying firm takes the capital charges instead. See also, e.g., Rule 103 of the New York Stock Exchange (setting forth requirements for Designated Market Makers and Designated Market Maker Units).

¹⁵² See paragraph (a)(1)(i)(F) of proposed Rule 10.

¹⁵³ For example, as discussed below in section IV.C.2. of this release, the 1,541 broker-dealers that would be Covered Entities had average total assets of \$3.5 billion and average regulatory equity of \$325 million; whereas the 1,969 that would be Non-Covered Entities had average total assets of \$4.7 million and average regulatory equity of \$3 million. This means that Non-Covered Broker-Dealers under proposed Rule 10 accounted for about 0.2% of the total assets of all broker-dealers and 0.1% of total capital for all broker-dealers.

offerings.¹⁵⁴ Further, they do not act as custodians for customer securities and cash or serve as a conduit (*i.e.*, an introducing broker-dealer) for customers to access their accounts at a carrying broker-dealer that does maintain custody of securities and cash. Therefore, they do not pose the risk that a significant cybersecurity incident could lead to investors losing access to their securities or cash or having those assets stolen. In addition, Non-Covered Broker-Dealers likely are less connected to other Market Participants through information systems than Covered Broker-Dealers. For these reasons, the additional policies and procedures, reporting, and disclosure requirements would not apply to Non-Covered Broker-Dealers.

At the same time, Non-Covered Broker-Dealers are part of the financial sector and exposed to cybersecurity risk. Further, certain Non-Covered Broker-Dealers maintain personal information about their customers that if accessed by threat actors or mistakenly exposed to unauthorized users could result in harm to the customers. For these reasons, Non-Covered Broker-Dealers—among other things—would be required under proposed Rule 10 to: (1) establish, maintain, and enforce written policies and procedures that are reasonably designed to address their cybersecurity risks taking into account their size, business, and operations; (2) review and assess the design and effectiveness of their cybersecurity policies and procedures annually, including whether the policies and procedures reflect changes in cybersecurity risk over the time period covered by the review; (3) make a written record that documents the steps taken in performing the annual review and the conclusions of the annual review; and (4) give the Commission and their examining authority immediate written electronic notice of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring.¹⁵⁵ The Commission's objective in proposing Rule 10 is to address the cybersecurity risks faced by all Market Entities but apply a more limited set of requirements to Non-Covered Broker-Dealers commensurate with the level of risk they pose to investors, the U.S. securities markets,

¹⁵⁴ See section IV.C.2. of this release (discussing the activities of broker-dealers that would not meet the definition of "covered entity" in proposed Rule 10).

¹⁵⁵ See section II.C. of this release (discussing the requirements for these broker-dealers in more detail).

and the U.S. financial sector more generally.

c. Market Entities Other Than Broker-Dealers

The MSRB and all clearing agencies, national securities associations, national securities exchanges, SBSDRs, SBS Entities,¹⁵⁶ and transfer agents would be Covered Entities and, therefore, subject to the additional requirements regarding the minimum elements that must be included in their cybersecurity risk management policies and procedures, reporting, and public disclosure.¹⁵⁷ In particular, proposed Rule 10 would define Covered Entity to include: (1) a clearing agency (registered or exempt) under section 3(a)(23)(A) of the Exchange Act;¹⁵⁸ (2) an MSBSP that is registered pursuant to section 15F(b) of the Exchange Act;¹⁵⁹ (3) the Municipal Securities Rulemaking Board;¹⁶⁰ (4) a national securities association under section 15A of the Exchange Act;¹⁶¹ (5) a national securities exchange under section 6 of the Exchange Act;¹⁶² (6) a security-based swap data repository under section 3(a)(75) of the Exchange Act;¹⁶³ (7) a security-based swap dealer that is registered pursuant to section 15F(b) of the Exchange Act;¹⁶⁴ and (8) a transfer agent as defined in section 3(a)(25) of the Exchange Act that is registered or required to be registered with an appropriate regulatory agency

¹⁵⁶ In addition to the requirements proposed in Rule 10 itself, the scope of certain existing regulations applicable to SBS Entities would include proposed Rule 10 if adopted; *see, e.g.*, 17 CFR 240.15Fk-1(b)(2)(i) (which establishes the scope of specified chief compliance officer duties by reference to Section 15F of the Exchange Act (15 U.S.C. 78o-10) and the rules and regulations thereunder); 17 CFR 240.15Fh-3(h)(2)(iii)(I) (which establishes the scope of specified supervisory requirements by reference to Section 15F(j) of the Exchange Act (15 U.S.C. 78o-10(j))).

¹⁵⁷ See paragraphs (a)(1)(ii) through (ix) of proposed Rule 10 (defining these Market Entities as "covered entities").

¹⁵⁸ See paragraph (a)(1)(ii) of proposed Rule 10. See also 15 U.S.C. 78c(a)(23)(A) (defining the term "clearing agency").

¹⁵⁹ See paragraph (a)(1)(iii) of proposed Rule 10. See also 15 U.S.C. 78o-10(b). Registered MSBSPs include both MSBSPs that are conditionally registered pursuant to paragraph (d) of Exchange Act Rule 15Fb2-1 ("Rule 15Fb2-1") (17 CFR 240.15Fb2-1) and MSBSPs that have been granted ongoing registration pursuant to paragraph (e) of Rule 15Fb2-1.

¹⁶⁰ See paragraph (a)(1)(iv) of proposed Rule 10. See also 15 U.S.C. 78o-3.

¹⁶¹ See paragraph (a)(1)(v) of proposed Rule 10. See also 15 U.S.C. 78f.

¹⁶² See paragraph (a)(1)(vi) of proposed Rule 10. See also 15 U.S.C. 78f.

¹⁶³ See paragraph (a)(1)(vii) of proposed Rule 10.

¹⁶⁴ See paragraph (a)(1)(viii) of proposed Rule 10. See also 15 U.S.C. 78o-10(b). Registered SBSDRs include both SBSDRs that are conditionally registered pursuant to paragraph (d) of Rule 15Fb2-1 and SBSDRs that have been granted ongoing registration pursuant to paragraph (e) of Rule 15Fb2-1.

("ARA") as defined in section 3(a)(34)(B) of the Exchange Act.¹⁶⁵

SROs play a critical role in setting and enforcing rules for their members or registrants that govern trading, fair access, transparency, operations, and business conduct, among other things. SROs and SBSDRs also play a critical role in ensuring fairness in the securities markets through the transparency they provide about securities transactions and pricing, and the information about securities transactions they can provide to regulators. National securities exchanges play a critical role in ensuring the orderly and efficient operation of the U.S. securities markets through the marketplaces they operate. Clearing agencies are critical to the orderly and efficient operation of the U.S. securities markets through the centralized clearing and settlement services they provide as well as their role as securities depositories, with exempt clearing agencies serving an important role as part of this process. Market liquidity is critical to the orderly and efficient operation of the U.S. securities markets. In this regard, SBS Entities play a critical role in providing liquidity to the security-based swap market.

The disruption or degradation of the functions of an SRO (including functions that support securities marketplaces and the oversight of market participants) could cause harm to investors to the extent it negatively impacted the fair, orderly, and efficient operations of the U.S. securities markets. For example, it could prevent investors from purchasing or selling securities or doing so at fair or reasonable prices. Investors also would face harm if a transfer agent's functions were disrupted or degraded by a significant cybersecurity incident. Transfer agents provide services such as stockholder recordkeeping, processing of securities transactions and corporate actions, and paying agent activities. Their core recordkeeping systems provide a direct conduit to their issuer clients' master records that document and, in many instances provide the legal underpinning for, registered securityholders' ownership of the issuer's securities. If these functions were disrupted, investors might not be able to transfer ownership of their securities or receive dividends and

¹⁶⁵ See paragraph (a)(1)(ix) of proposed Rule 10. See also 15 U.S.C. 78q-1(c)(1) (registration requirements for transfer agents); 15 U.S.C. 78c(a)(25) (definition of transfer agent) and (a)(34)(B) (definition of appropriate regulatory agency).

interest due on their securities positions.

SROs, exempt clearing agencies, and SBSDRs connect to multiple members, registrants, users, or others through networks of information systems. The interconnectedness of these Market Entities with other Market Entities through information systems creates the potential that a significant cybersecurity incident at one Market Entity (*e.g.*, one caused by malware) could spread to other Market Entities in a cascading process that could cause widespread disruptions threatening the fair, orderly, and efficient operation of the U.S. securities markets.¹⁶⁶ Additionally, the disruption of a Market Entity that provides critical services to other Market Entities through information system connections could disrupt the activities of these other Market Entities if they cannot obtain the services from another source.

SROs, exempt clearing agencies, SBSDRs, SBS Entities, and transfer agents could be prime targets of threat actors because of the central roles they play in the securities markets. For example, threat actors could seek to disrupt their functions for geopolitical purposes. Threat actors also could seek to gain unauthorized access to their information systems to conduct espionage operations on their internal non-public activities. Moreover, because they hold financial assets (*e.g.*, clearing deposits in the case of clearing agencies) and/or store substantial confidential and proprietary information about other Market Entities or financial transactions, they may be choice targets for threat actors seeking to steal the assets or use the financial information to their advantage.

SROs, exempt clearing agencies, and SBSDRs store confidential and proprietary information about their members, registrants, and users, including confidential business information, and personal information. A significant cybersecurity incident at any of these types of Market Entities could lead to the improper use of this information to harm the members, registrants, and users or provide the unauthorized user with an unfair advantage over other market participants and, in the case of personal information, to steal identities. Moreover, given the volume of information stored by these Market Entities about different persons, the harm caused by a cybersecurity incident

could be widespread, negatively impacting many victims.

SBS Entities also store proprietary and confidential information about their counterparties on their information systems, including financial information they use to perform credit analysis. A significant cybersecurity incident at an SBS Entity could lead to the improper use of this information to harm the counterparties or provide the unauthorized user with an unfair advantage over other market participants. Transfer agents store proprietary information about securities ownership and corporate actions. A significant cybersecurity incident at a transfer agent could lead to the improper use of this information to harm securities holders. Transfer agents also may store personal information including names, addresses, phone numbers, email addresses, employers, employment history, bank and specific account information, credit card information, transaction histories, securities holdings, and other detailed and individualized information related to the transfer agents' recordkeeping and transaction processing on behalf of issuers. Threat actors breaching the transfer agent's information systems could use this information to steal identities or financial assets of the persons to whom this information pertains. They also could sell it to other threat actors.

In light of these considerations, the MSRB and all clearing agencies, national securities associations, national securities exchanges, SBSDRs, SBS Entities, and transfer agents would be Covered Entities under proposed Rule 10 and, therefore, subject to the additional requirements regarding the minimum elements that must be included in their cybersecurity risk management policies and procedures, reporting, and public disclosure.¹⁶⁷

2. "Cybersecurity Incident"

Proposed Rule 10 would define the term "cybersecurity incident" to mean an unauthorized occurrence on or conducted through a Market Entity's information systems that jeopardizes the confidentiality, integrity, or availability of the information systems or any information residing on those systems.¹⁶⁸ The objective is to use a

¹⁶⁷ See paragraphs (a)(1)(ii) through (ix) of proposed Rule 10 (defining these Market Entities as "covered entities").

¹⁶⁸ See paragraph (a)(2) of proposed Rule 10. See generally, NIST Glossary (defining "cybersecurity risk" as "an effect of uncertainty on or within information and technology" and defining "incident" as "an occurrence that actually or potentially jeopardizes the confidentiality, integrity,

term that is broad enough to encompass within the definition of "cybersecurity incident" the various categories of unauthorized occurrences that can impact an information system (*e.g.*, unauthorized access, use, disclosure, downloading, disruption, modification, or destruction). As discussed earlier, the sources of cybersecurity risk are myriad as are the tactics, techniques, and procedures employed by threat actors.¹⁶⁹

The definition of "cybersecurity incident" in proposed Rule 10 is designed to include any unauthorized incident impacting an information system or the information residing on the system. An information system can experience an unauthorized occurrence without a threat actor itself directly obtaining unauthorized access to the system. For example, a social engineering tactic could cause an employee to upload ransomware unintentionally that encrypts the information residing on the system or a DoS attack could cause the information system to shut down. In either case, the threat actor did not need to access the information system to cause harm.

While the definition is intended to be broad, the occurrence must be one that *jeopardizes* (*i.e.*, places at risk) the confidentiality, integrity, or availability of the information systems or any information residing on those systems. Confidentiality would be jeopardized if the unauthorized occurrence resulted in or could result in persons accessing an information system or the information residing on the system who are not permitted or entitled to do so or resulted in or could result in the disclosure of the information residing on the information system to the public or to any person not permitted or entitled to view it.¹⁷⁰ Integrity would be jeopardized if the unauthorized occurrence resulted in or could result in: (1) an unpermitted or unintended modification or destruction of the

or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies"); FISMA (defining "incident" as an "occurrence" that: (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. 44 U.S.C. 3552(b)(2).

¹⁶⁹ See section I.A.1. of this release (discussing the sources of the cybersecurity risk).

¹⁷⁰ See generally NIST Glossary (defining "confidentiality" as "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information").

¹⁶⁶ See, *e.g.*, Implications of Cyber Risk for Financial Stability ("[T]he interconnectedness of the financial system means that an event at one or more firms may spread to others (the domino effect).").

information system or the information residing on the system; or (2) otherwise resulted in or could result in a compromise of the authenticity of the information system (including its operations and output) and the information residing on the system.¹⁷¹ Availability would be jeopardized if the unauthorized occurrence resulted in or could result in the Market Entity or other authorized users being unable to access or use the information system or information residing on the system or being unable access or use the information system or information residing on the system in a timely or reliable manner.¹⁷²

3. “Significant Cybersecurity Incident”

Proposed Rule 10 would have a two-pronged definition of “significant cybersecurity incident.”¹⁷³ The first prong of the definition would be a cybersecurity incident, or a group of related cybersecurity incidents, that significantly disrupts or degrades the ability of the Market Entity to maintain critical operations.¹⁷⁴ As discussed earlier, significant cybersecurity incidents can negatively impact information systems and the information residing on information systems in two fundamental ways. First, they can disrupt or degrade the information system or the information residing on the information system in a manner that prevents the Market Entity from performing functions that rely on the system operating as designed (*e.g.*, an order routing system of an national securities exchange or a margin calculation and collection system of a clearing agency) or that rely on the Market Entity being able to process or access information on the system (*e.g.*, a general ledger of a broker-dealer or SBS Entity that tracks and records securities transactions).¹⁷⁵ This type of harm can be caused by, for example, a ransomware attack that encrypts the

¹⁷¹ See generally NIST Glossary (defining “integrity” as “guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity”).

¹⁷² See generally NIST Glossary (defining “availability” as “ensuring timely and reliable access to and use of information”).

¹⁷³ See paragraphs (a)(10)(i) and (ii) of proposed Rule 10.

¹⁷⁴ See paragraph (a)(10)(i) of proposed Rule 10.

¹⁷⁵ See sections I.A.1. and I.A.2. of this release (discussing the consequences of these types of information system degradations and disruptions). This type of impact would compromise the integrity or availability of the information system. See generally NIST Glossary (defining “integrity” as “guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity” and “availability” as “ensuring timely and reliable access to and use of information”).

information stored on the system, a DoS attack that overwhelms the information system, or hackers taking control of a the system or shutting it down. Generally, critical operations would be activities, processes, and services that if disrupted could prevent the Market Entity from continuing to operate or prevent it from performing a service that supports the fair, orderly, and efficient functioning of the U.S. securities markets.¹⁷⁶

The second fundamental way that a significant cybersecurity incident can negatively impact an information system or the information residing on the information system is when unauthorized persons are able to access and use the information stored on the information system (*e.g.*, proprietary business information or personal information).¹⁷⁷ Therefore, the second prong of the definition would be a cybersecurity incident, or a group of related cybersecurity incidents, that leads to the unauthorized access or use of the information or information systems of the Market Entity, where the unauthorized access or use of such information or information systems results in or is reasonably likely to result in: (1) substantial harm to the Market Entity; or (2) substantial harm to a customer, counterparty, member, registrant, or user of the Market Entity, or to any other person that interacts with the Market Entity.¹⁷⁸ As discussed earlier, this kind of significant cybersecurity incident could lead to the improper use of this information to harm persons to whom it pertains (*e.g.*, public exposure of their confidential financial information or the use of that information to steal their identities) or

¹⁷⁶ See, *e.g.*, Basel Committee on Banking Supervision, Principles for Operational Resilience (Mar. 2021) (“The term critical operations is based on the Joint Forum’s 2006 high-level principles for business continuity. It encompasses critical functions as defined by the FSB and is expanded to include activities, processes, services and their relevant supporting assets the disruption of which would be material to the continued operation of the bank or its role in the financial system.”) (footnotes omitted).

¹⁷⁷ See sections I.A.1. and I.A.2. of this release (discussing the consequences of this type of compromise of an information system). This type of impact would compromise the confidentiality of the information system. See generally NIST Glossary (defining “confidentiality” as “preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information”).

¹⁷⁸ See paragraph (a)(10)(ii) of proposed Rule 10. There could be instances where a significant cybersecurity incident meets both prongs. For example, an unauthorized user that is able to access the Market Entity’s internal computer systems could shut down critical operations of the Market Entity and use information on the systems to steal assets of the Market Entity or assets or identities of the Market Entity’s customers.

provide the unauthorized user with an unfair advantage over other market participants (*e.g.*, trading based on confidential business information).¹⁷⁹

4. “Cybersecurity Threat”

Proposed Rule 10 would define the term “cybersecurity threat” to mean any potential occurrence that may result in an unauthorized effort to affect adversely the confidentiality, integrity, or availability of a Market Entity’s information systems or any information residing on those systems.¹⁸⁰ As discussed earlier, threat actors use a number of different tactics, techniques, and procedures (*e.g.*, malware, social engineering, hacking, DoS attacks) to commit cyber-related crime.¹⁸¹ These threat actors may be nation states, individuals (acting alone or as part of organized syndicates) seeking financial gain, or individuals seeking to cause harm for a variety of reasons. Further, the threat actors may be external or internal actors. Also, as discussed earlier, errors can pose a cybersecurity threat (*e.g.*, accidentally providing access to confidential information to individuals that are not authorized to view or use it). The definition of “cybersecurity threat” in proposed Rule 10 is designed to include the potential actions of threat actors (*e.g.*, seeking to install malware on or hack into an information system or engaging in social engineering tactics) and potential errors (*e.g.*, an employee failing to secure confidential, proprietary, and personal information) that may result in an unauthorized effort to affect adversely the confidentiality, integrity, or availability of a Market Entity’s information systems or any information residing on those systems.

5. “Cybersecurity Vulnerability”

Proposed Rule 10 would define the term “cybersecurity vulnerability” to mean a vulnerability in a Market Entity’s information systems, information system security procedures, or internal controls, including, for example, vulnerabilities in their design,

¹⁷⁹ See sections I.A.1. and I.A.2. of this release (discussing the consequences of this type of compromise of an information system).

¹⁸⁰ See paragraph (a)(4) of proposed Rule 10. See generally NIST Glossary (defining “threat” as any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service and also the potential for a threat-source to successfully exploit a particular information system vulnerability).

¹⁸¹ See section I.A.1. of this release (discussing the various tactics, techniques, and procedures used by threat actors).

configuration, maintenance, or implementation that, if exploited, could result in a cybersecurity incident.¹⁸² Cybersecurity vulnerabilities are weaknesses in the Covered Entity's information systems that threat actors could exploit, for example, to hack into the system or install malware.¹⁸³ One example would be an information system that uses outdated software that is no longer updated to address known flaws that could be exploited by threat actors to access the system. Cybersecurity vulnerabilities also are weaknesses in the procedures and controls the Market Entity uses to protect its information systems and the information residing on them such as procedures and controls that do not require outdated software to be replaced or that do not adequately restrict access to the system. Cybersecurity vulnerabilities can also include lack of training opportunities for employees to increase their cybersecurity awareness, such as how to properly secure sensitive data and recognize harmful files. The definition of "cybersecurity vulnerability" in proposed Rule 10 is designed to include weaknesses in the information systems themselves and weaknesses in the measures the Covered Entity takes to protect the systems and the information residing on the systems.

6. "Cybersecurity Risk"

Proposed Rule 10 would define the term "cybersecurity risk" to mean financial, operational, legal, reputational, and other adverse consequences that could stem from cybersecurity incidents, cybersecurity threats, and cybersecurity vulnerabilities.¹⁸⁴ As discussed earlier, cybersecurity incidents have the

¹⁸² See paragraph (a)(5) of proposed Rule 10. See generally NIST Glossary (defining "vulnerability" as a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source").

¹⁸³ See section I.A.1. of this release (discussing information system vulnerabilities). See generally CISA 2021 Vulnerability Report ("Globally, in 2021, malicious cyber actors targeted internet-facing systems, such as email servers and virtual private network (VPN) servers, with exploits of newly disclosed vulnerabilities.").

¹⁸⁴ See paragraph (a)(3) of proposed Rule 10. See also paragraphs (a)(4) and (5) of proposed Rule 10 (defining, respectively, "cybersecurity threat" to mean "any potential occurrence that may result in an unauthorized effort to affect adversely the confidentiality, integrity, or availability of a Market Entity's information systems or any information residing on those systems" and "cybersecurity vulnerability" to mean "a vulnerability in a Market Entity's information systems, information system security procedures, or internal controls, including, for example, vulnerabilities in their design, configuration, maintenance, or implementation that, if exploited, could result in a cybersecurity incident").

potential to cause harm to Market Entities and others who use their services or are connected to them through information systems and, if severe enough, negatively impact the fair, orderly, and efficient operations of the U.S. securities markets.¹⁸⁵ The definition of "cybersecurity risk" in proposed Rule 10 is designed to encompass the types of harm and damage that can befall a Market Entity that experiences a cybersecurity incident.

7. "Information"

As discussed in more detail below, a Market Entity would be required under proposed Rule 10 to establish, maintain, and enforce written policies and procedures that are reasonably designed to address the Market Entity's cybersecurity risks.¹⁸⁶ Cybersecurity risks—as discussed above—would be financial, operational, legal, reputational, and other adverse consequences that could result from cybersecurity incidents, cybersecurity threats, and cybersecurity vulnerabilities.¹⁸⁷ Cybersecurity incidents would be unauthorized occurrences on or conducted through a market entity's *information systems* that jeopardize the confidentiality, integrity, or availability of the *information systems* or any *information* residing on those systems.¹⁸⁸ Cybersecurity threats would be any potential occurrences that may result in an unauthorized effort to affect adversely the confidentiality, integrity, or availability of a market entity's *information systems* or any *information* residing on those systems.¹⁸⁹ Finally, cybersecurity vulnerabilities would be a vulnerability in a Market Entity's *information systems*, *information system* security procedures, or internal controls, including, for example, vulnerabilities in their design, configuration, maintenance, or implementation that, if exploited, could result in a

¹⁸⁵ See sections I.A.1. and I.A.2. of this release (discussing, respectively, the harms that can be caused by significant cybersecurity incidents generally and with respect to each category of Market Entity).

¹⁸⁶ See paragraphs (b)(1) and (e) of proposed Rule 10 (requiring Covered Entities and Non-Covered Entities, respectively, to have policies and procedures to address their cybersecurity risks); sections II.B.1. and II.C. of this release (discussing the requirements of paragraphs (b)(1) and (e) of proposed Rule 10, respectively, in more detail).

¹⁸⁷ See paragraph (a)(3) of proposed Rule 10 (defining "cybersecurity risk").

¹⁸⁸ See paragraph (a)(2) of proposed Rule 10 (defining "cybersecurity incident").

¹⁸⁹ See paragraph (a)(4) of proposed Rule 10 (defining "cybersecurity threat").

cybersecurity incident.¹⁹⁰ Consequently, the policies and procedures required under proposed Rule 10 would need to cover all of the Market Entity's *information systems* and *information* residing on those systems in order to address the Market Entity's cybersecurity risks.

Proposed Rule 10 would define the term "information" to mean any records or data related to the Market Entity's business residing on the Market Entity's information systems, including, for example, personal information received, maintained, created, or processed by the Market Entity.¹⁹¹ The definition is designed to cover the full range of information stored by Market Entities on their information systems regardless of the digital format in which the information is stored.¹⁹² As discussed earlier, Market Entities create and maintain a wide range of information on their information systems.¹⁹³ This includes information used to manage and conduct their operations, manage and mitigate their risks, monitor the progress of their business, track their financial condition, prepare financial statements, prepare regulatory filings, and prepare tax returns. They also store personal, confidential, and proprietary business information about their customers, counterparties, members, registrants or users. This includes information maintained by clearing agencies, the MSRB, the national securities exchanges, and SBSDRs about market activity and about their members, registrants, and users.

The information maintained by Market Entities on their information systems is an attractive target for threat actors, particularly confidential, proprietary, and personal information.¹⁹⁴ Also, it also can be

¹⁹⁰ See paragraph (a)(5) of proposed Rule 10 (defining "cybersecurity vulnerability").

¹⁹¹ See paragraph (a)(6) of proposed Rule 10.

¹⁹² See generally NIST Glossary (defining "information" as any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual. *Id.* (defining "data" (among other things) as: (1) pieces of information from which "understandable information" is derived; (2) distinct pieces of digital information that have been formatted in a specific way; and (3) a subset of information in an electronic format that allows it to be retrieved or transmitted. *Id.* (defining "records" (among other things) as units of related data fields (*i.e.*, groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).

¹⁹³ See section I.A.2. of this release.

¹⁹⁴ See sections I.A.1. and I.A.2. of this release (discussing how threat actors seek unauthorized access to and use of confidential, proprietary, and personal information to, among other reasons, conduct espionage operations, steal identities, use it for business advantage, hold it hostage (in effect)

critical to performing their various functions, and the inability to access and use their information could disrupt or degrade their ability to operate in support of the fair, orderly, and efficient operation of the U.S. securities markets.¹⁹⁵ Consequently, protecting the confidentiality, integrity, and availability of information residing on a Market Entity's information systems is critical to avoiding the harms that can be caused by cybersecurity risk. The definition of "information" in proposed Rule 10 is designed to encompass this information and, therefore, to extend the proposed protections of the rule to it.

8. "Information Systems"

The policies and procedures required under proposed Rule 10 also would need to cover the Market Entity's *information systems* in order to address the Market Entity's cybersecurity risks. Proposed Rule 10 would define the term "information systems" to mean the information resources owned or used by the Market Entity, including, for example, physical or virtual infrastructure controlled by the information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the Market Entity's information to maintain or support the Market Entity's operations.¹⁹⁶

As discussed earlier, Market Entities use information systems to perform a wide range of functions.¹⁹⁷ For example, they use information systems to maintain books and records to manage and conduct their operations, manage and mitigate their risks, monitor the progress of their business, track their financial condition, prepare financial statements, prepare regulatory filings, and prepare tax returns. Market Entities also use information systems so that their employees can communicate with each other and with external persons. These include email, text messaging, and virtual meeting applications. They also use internet websites to communicate information to their customers, counterparties, members, registrants, or users. They use information systems to perform the functions associated with their status and obligations as a broker-dealer, registered or exempt clearing agency, national securities association, national

securities exchange, SBSDR, SBS Entity, SRO, or transfer agent.

Information systems are targets that threat actors attack to access and use information maintained by Market Entities related to their business (particularly confidential, proprietary, and personal information).¹⁹⁸ In addition, the interconnectedness of Market Entities through information systems creates channels through which malware, viruses, and other destructive cybersecurity threats can spread throughout the financial system. Moreover, the disruption or degradation of a Market Entity's information systems could negatively impact the entity's ability to operate in support of the U.S. securities markets.¹⁹⁹ Consequently, protecting the confidentiality, integrity, and availability of a Market Entity's information systems is critical to avoiding the harms that can be caused by cybersecurity risk. The definition of the term "information systems" in proposed Rule 10 is designed to be broad enough to encompass all the electronic information resources owned or used by a Market Entity to carry out its various operations. Accordingly, the definition of "information systems" would require a Market Entity's policies and procedures to address cybersecurity risks to cover all of its information systems.

9. "Personal Information"

Proposed Rule 10 would define the term "personal information" to mean any information that can be used, alone or in conjunction with any other information, to identify a person, including, but not limited to, name, date of birth, place of birth, telephone number, street address, mother's maiden name, Social Security number, government passport number, driver's license number, electronic mail address, account number, account password, biometric records, or other non-public authentication information.²⁰⁰ The

¹⁹⁸ See sections I.A.1. and I.A.2. of this release.

¹⁹⁹ *Id.*

²⁰⁰ See paragraph (a)(9) of proposed Rule 10. See generally NIST Glossary (defining "personal information" as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual and defining "personally identifying information" (among other things) as information that can be used to distinguish or trace an individual's identity—such as name, social security number, biometric data records—either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.)); 17 CFR 248.201(b)(8) ((defining "identifying information" as any name or number that may be used, alone or in conjunction with any other information, to identify a specific

definition of "personal information" was guided by a number of established sources and aims to capture a broad array of information that can reside on a Market Entity's information systems that may be used alone, or with other information, to identify an individual. The definition is designed to encompass information that if compromised could cause harm to the individuals to whom the information pertains (e.g., identity theft or theft of assets).

Personal information is an attractive target for threat actors because they can use it to steal a person's identity and then use the stolen identity to appropriate the person's assets through unauthorized transactions or to make unlawful purchases on credit or to effect other unlawful transactions in the name of the person.²⁰¹ They also can sell personal information they obtain through unauthorized access to an information system to criminals who will seek to use the information for these purposes. Moreover, the victims of identity theft can be the more vulnerable members of society (e.g., individuals on fixed-incomes, including retirees). Consequently, proposed Rule 10 would have a provision that specifically addresses protecting personal information.²⁰²

10. Request for Comment

The Commission requests comment on all aspects of the proposed definitions. In addition, the Commission is requesting comment on the following specific aspects of the proposals:

1. In designing the definitions of proposed Rule 10, the Commission considered a number of sources cited in the sections above, including, in particular, the NIST Glossary and certain Federal statutes and regulations. Are these appropriate sources to consider? If so, explain why. If not, explain why not. Are there other sources the Commission should use? If so, identify them and explain why they should be considered and how they

person, including any: (1) name, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number; (2) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation; (3) unique electronic identification number, address, or routing code; or (4) telecommunication identifying information or access device (as defined in 18 U.S.C. 1029(e)).

²⁰¹ See sections I.A.1. and I.A.2. of this release.

²⁰² See paragraph (b)(1)(iii)(A)(2) of proposed Rule 10. See also proposed Form SCIR, which would elicit information about whether personal information was compromised in a significant cybersecurity incident.

through a ransomware attack, or sell it to other threat actors).

¹⁹⁵ *Id.*

¹⁹⁶ See paragraph (a)(7) of proposed Rule 10.

¹⁹⁷ See section I.A.2. of this release.

could inform potential modifications to the definitions.

2. In determining which categories of Market Entities would be Covered Entities subject to the additional requirements of proposed Rule 10, the Commission considered: (1) how the category of Market Entity supports the fair, orderly, and efficient operation of the U.S. securities markets and the consequences if that type of broker-dealer's critical functions were disrupted or degraded by a significant cybersecurity incident; (2) the harm that could befall investors, including retail investors, if that category of Market Entity's functions were disrupted or degraded by a significant cybersecurity incident; (3) the extent to which the category of Market Entity poses cybersecurity risk to other Market Entities through information system connections, including the number of connections; (4) the extent to which the category of Market Entity would be an attractive target for threat actors; and (5) the personal, confidential, and proprietary business information about the category of Market Entity and other persons (e.g., investors) stored on the Market Entity's information systems and the harm that could be caused if that information was accessed or used by threat actors through a cybersecurity breach. Are these appropriate factors to consider? If so, explain why. If not, explain why not. Are there other factors the Commission should take into account? If so, identify them and explain why they should be considered.

3. Should proposed Rule 10 be modified to include other categories of broker-dealers as Covered Entities? If so, identify the category of broker-dealers and explain how to define broker-dealers within that category and why it would be appropriate to apply the additional policies and procedures, reporting, and disclosure requirements of the proposed rule to that category of broker-dealers. For example, should the \$50 million regulatory capital threshold be lowered (e.g., to \$25 million or some other amount) or should the \$1 billion total assets threshold be lowered (e.g., to \$500 million or some other amount) to include more broker-dealers as Covered Entities? If so, identify the threshold and explain why it would be appropriate to apply the additional requirements to broker-dealers that fall within that threshold.

4. Should proposed Rule 10 be modified to include as a Covered Entity any broker-dealer that is an SCI entity for the purposes of Regulation SCI? Currently, under Regulation SCI, an ATS that trades certain stocks exceeding specific volume thresholds is an SCI

entity?²⁰³ As discussed above, a broker-dealer that operates an ATS would be a Covered Entity under proposed Rule 10 and, therefore, subject to the additional policies and procedures, reporting, and disclosure requirements of the proposed rule. However, the Commission is proposing to amend Regulation SCI to broaden the definition of "SCI entity" to include, among other Commission registrants, a broker-dealer that exceeds an asset-based size threshold or a volume-based trading threshold in NMS stocks, exchange-listed options, agency securities, or U.S. treasury securities.²⁰⁴ A broker-dealer that exceeds the asset-based size threshold under the proposed amendments to Regulation SCI (which would be several hundred billion dollars) would be subject to the requirements of proposed Rule 10 applicable to Covered Entities, as it would exceed the \$1 billion total assets threshold in the broker-dealer definition of "covered entity."²⁰⁵ Further, a broker-dealer that exceeds one or more of the volume-based trading thresholds under the proposed amendments to Regulation SCI likely would meet one of the broker-dealer definitions of "covered entity" in proposed Rule 10 given its size and activities. For example, it may be carrying broker-dealer, have regulatory capital equal to or exceeding \$50 million, have total assets equal to or exceeding \$1 billion, or operate as a market maker.²⁰⁶ Nonetheless, should the definition of "covered entity" in proposed Rule 10 be modified to include any broker-dealer that is an SCI entity under Regulation SCI? If so, explain why. If not, explain why not.

5. Should proposed Rule 10 be modified to narrow the categories of broker-dealers that would be Covered Entities? If so, explain how the category should be narrowed and why it would be appropriate not to apply the additional requirements to broker-dealers that would no longer be included as Covered Entities. For example, are there certain types of carrying broker-dealers, introducing broker-dealers, market makers, or ATSs that should not be included as Covered

²⁰³ See 17 CFR 242.1000 (defining the term "SCI alternative trading system" and including that defined term in the definition of "SCI Entity").

²⁰⁴ Regulation SCI 2023 Proposing Release.

²⁰⁵ See paragraph (a)(1)(i)(D) of proposed Rule 10. See also section II.F.1.c. of this release (discussing why this type of broker-dealer would be a Covered Entity).

²⁰⁶ See paragraphs (a)(1)(i)(A), (C), (D), and (E) of proposed Rule 10 (defining these categories of broker-dealers as "covered entities"). See also section II.F.1.c. of this release (discussing why this type of broker-dealer likely would be a Covered Entity).

Entities? If so, identify the type of broker-dealer and explain why it would be appropriate not to impose the additional policies and procedures, reporting, and disclosure requirements of the proposed rule on that type of broker-dealer. Similarly, should the proposed \$50 million regulatory capital threshold be increased (e.g., to \$100 million or some other amount) or should the \$1 billion total assets threshold be increased (e.g., to \$5 billion or some other amount) to exclude more broker-dealers from the definition of "covered entity"? If so, identify the threshold and explain why it would be appropriate not to apply the additional requirements on the broker-dealers that would not be Covered Entities under the narrower definition.

6. Should proposed Rule 10 be modified to divide other categories of Market Entities into Covered Entities and Non-Covered Entities? If so, identify the category of Market Entity and explain how to define Covered Entity and Non-Covered Entity within that category and explain why it would be appropriate not to impose the additional policies and procedures, reporting, and disclosure requirements on the Market Entities that would be Non-Covered Entities. For example, are there types of clearing agencies (registered or exempt), MSBSPs, national securities exchanges, SBSDRs, SBSDs, or transfer agents that pose a level of cybersecurity risk to the U.S. securities markets and the participants in those markets that is no greater than the cybersecurity risk posed by the categories of broker-dealers that would be Non-Covered Entities? If so, explain why it would be appropriate not to apply the additional requirements of proposed Rule 10 to these types of Market Entities.

7. Should proposed Rule 10 be modified so that it applies to other participants in the U.S. securities markets that are registered with the Commission? If so, identify the registrant type and explain why it should be subject to the requirements of proposed Rule 10. For example, should competing consolidators or plan processors be subject to the requirements of proposed Rule 10?²⁰⁷ If so, explain why. If not, explain why not. If competing consolidators or plan processors should be subject to proposed Rule 10, should they be treated as Covered Entities or Non-Covered Entities? If Covered Entities,

²⁰⁷ See 17 CFR 242.600(16) and (67) (defining the terms "competing consolidator" and "plan processor," respectively). See also 17 CFR 242.1000 (defining "SCI competing consolidator" and defining "SCI entity" to include SCI competing consolidator).

explain why. If Non-Covered Entities, explain why. Should certain competing consolidators or plan processors be treated as Covered Entities and others be treated as Non-Covered Entities? If so, explain how to define Covered Entity and Non-Covered Entity within that category and explain why it would be appropriate not to apply the additional policies and procedures, reporting, and disclosure requirements of the proposed rule to the competing consolidators or plan processors in that category that would not be Covered Entities.

8. Should proposed Rule 10 be modified to revise the broker-dealer definitions of “covered entity”? For example, in order to include carrying broker-dealers as Covered Entities, paragraph (a)(1)(i)(A) of proposed Rule 10 would define the term “covered entity” to include a broker-dealer that maintains custody of cash and securities for customers or other brokers-dealers and is not exempt from the requirements of Rule 15c3–3. In addition, in order to include introducing broker-dealers as Covered Entities, paragraph (a)(1)(i)(B) of proposed Rule 10 would define the term “covered entity” to include a broker-dealer that introduces customer accounts on a fully disclosed basis to another broker-dealer that is a carrying broker-dealer under paragraph (a)(1)(i)(A) of the proposed rule. Would these broker-dealer definitions of “covered entity” work as designed? If not, explain why and suggest modifications to improve their design.

9. In order to include market makers as Covered Entities, paragraph (a)(1)(i)(E) of proposed Rule 10 would define the term “covered entity” to include a broker-dealer that is a market maker under the Exchange Act or the rules thereunder (which includes a broker-dealer that operates pursuant to paragraph (a)(6) of Rule 15c3–1) or is a market maker under the rules of an SRO of which the broker-dealer is a member. Would the definition work as designed? If not, explain why and suggest modifications to improve its design. For example, should the definition be based on a list of the functions and activities of a market maker as distinct from the functions and activities of other categories of broker-dealers? If so, identify the relevant functions and activities and explain how they could be incorporated into a definition.

10. Should paragraph (a)(2) of proposed Rule 10 be modified to revise the definition of “cybersecurity incident”? For example, as discussed above, the definition is designed to include any unauthorized occurrence that impacts an information system or

the information residing on the system. Would the definition work as designed? If not, explain why and suggest modifications to improve its design. Is this design objective appropriate? If not, explain why and suggest an alternative design objective for the definition. Is the definition of “cybersecurity incident” overly broad in that it refers to an incident that jeopardizes the confidentiality, integrity, or availability of the information systems or any information residing on those systems? If so, explain why and suggest modifications to appropriately narrow its scope without undermining the objective of the rule to address cybersecurity risks facing Market Entities. Is the definition of “cybersecurity incident” too narrow? If so, how should it be broadened?

11. Should paragraph (a)(3) of proposed Rule 10 be modified to revise definition of “cybersecurity risk”? For example, the NIST definition of “cybersecurity risk” focuses on how this risk can cause harm: it can adversely impact organizational operations (*i.e.*, mission, functions, image, or reputation) and assets, individuals, other organizations, and the Nation. The definition of “cybersecurity risk” in proposed Rule 10 was guided by this aspect of cybersecurity risk. Does the definition appropriately incorporate this aspect of cybersecurity risk? If not, explain why and suggest modifications to improve its design. Is this design objective appropriate? If not, explain why and suggest an alternative design objective for the definition.

12. Should paragraph (a)(4) of proposed Rule 10 be modified to revise the definition of “cybersecurity threat”? For example, as discussed above, the definition is designed to include the potential actions of threat actors and errors that may result in an unauthorized effort to affect adversely the confidentiality, integrity, or availability of a Market Entity’s information systems or any information residing on those systems. Would the definition work as designed? If not, explain why and suggest modifications to improve its design. Is the definition of “cybersecurity threat” overly broad in that it includes any “potential occurrence”? If so, explain why and suggest modifications to appropriately narrow its scope without undermining the objective of the rule to address cybersecurity risks facing Market Entities. Is the definition of “cybersecurity threat” too narrow? If so, how should it be broadened?

13. Should paragraph (a)(5) of proposed Rule 10 be modified to revise the definition of “cybersecurity

vulnerability”? For example, as discussed above, the definition is designed to include weaknesses in the information systems themselves and weaknesses in the measures the Covered Entity takes to protect the systems and the information residing on the systems. Would the definition work as designed? If not, explain why and suggest modifications to improve its design. Is this design objective appropriate? If not, explain why and suggest an alternative design objective for the definition. Is the definition of “cybersecurity vulnerability” overly broad? If so, explain why and suggest modifications to appropriately narrow its scope without undermining the objective of the rule to address cybersecurity risks facing Market Entities. Is the definition of “cybersecurity vulnerability” too narrow? If so, how should it be broadened?

14. Should paragraph (a)(6) of proposed Rule 10 be modified to revise the definition of “information”? For example, as discussed above, the definition is designed to be broad enough to encompass the wide range of information that resides on the information systems of Market Entities. Would the definition work as designed? If not, explain why and suggest modifications to improve its design. Is this design objective appropriate? If not, explain why and suggest an alternative design objective for the definition. For example, should the definition focus on information that, if compromised, could cause harm to the Market Entity or others and exclude information that, if compromised, would not cause harm? If so, explain why and suggest rule text to implement this modification.

15. Should paragraph (a)(7) of proposed Rule 10 be modified to revise the definition of “information systems”? For example, as discussed above, the definition is designed to be broad enough to encompass all the electronic information resources owned or used by a Market Entity to carry out its various operations. Would the definition work as designed? If not, explain why and suggest modifications to improve its design. Is this design objective appropriate? If not, explain why and suggest an alternative design objective for the definition. Is the definition of “information systems” overly broad in that it includes any information resource “used by” the Market Entity, which may include information resources developed and maintained by a third party (other than a service provider that that receives, maintains, or processes information, or is otherwise permitted to access the Market Entity’s information systems and any of the

Market Entity's information residing on those systems)? If so, explain why and suggest modifications to improve its design. Is this design objective appropriate? If not, explain why and suggest an alternative design objective for the definition. Is the definition of "information system" overly narrow? If so, how should it be broadened?

16. Should paragraph (a)(9) of proposed Rule 10 be modified to revise the definition of "personal information"? For example, as discussed above, the definition is designed to encompass information that if compromised could cause harm to the individuals to whom the information pertains (e.g., identity theft or theft of assets). Would the definition work as designed? If not, explain why and suggest modifications to improve its design. Is this design objective appropriate? If not, explain why and suggest an alternative design objective for the definition.

17. Should paragraph (a)(10) of proposed Rule 10 be modified to revise the definition of "significant cybersecurity incident"? For example, as discussed above, the definition would have two prongs: the first relating to incidents that significantly disrupt or degrade the ability of the Market Entity to maintain critical operations and the second relating to the unauthorized access or use of the information or information systems of the Market Entity. Are these the fundamental ways that significant cybersecurity incidents can negatively impact information systems and the information residing on information systems? If not, explain why and identify other fundamental ways that information and information systems can be negatively impacted by significant cybersecurity incidents that should be incorporated into the definition of "significant cybersecurity incident." Should the term "significant" be defined separately? If so, explain why and suggest potential definitions for this term. Instead, of "significant" should the definition use the word "material." If so, explain why and how that would change the meaning of the definition.

18. Should paragraph (a)(10)(i) of proposed Rule 10 be modified to revise the first prong of the definition of "significant cybersecurity incident"? For example, as explained above, the first prong is designed to address how a "significant cybersecurity incident" can disrupt or degrade the information system or the information residing on the system in a manner that prevents the Market Entity from performing functions that rely on the system operating as designed or that rely on the

Market Entity being able to process or access information on the system. Would the first prong of the definition work as designed? If not, explain why and suggest modifications to improve its design. Is this design objective appropriate? If not, explain why and suggest an alternative design objective for the first prong of the definition. For example, should the first prong of the definition be limited to cybersecurity incidents that "disrupt" the ability of the Market Entity to maintain critical operations (i.e., not include incidents that "degrade" that ability)? If so, explain why and also explain how to distinguish between an incident that degrades the ability of the Market Entity to maintain critical operations and an incident that disrupts that ability. Also, explain why reporting to the Commission and other regulators (as applicable) and publicly disclosing incidents that degrade the ability of the Market Entity to maintain critical operations would not be necessary because they would no longer be significant cybersecurity incidents.²⁰⁸

19. Should paragraph (a)(10)(ii) of proposed Rule 10 be modified to revise the second prong of the definition of "significant cybersecurity incident"? For example, as explained above, the second prong is designed to address how a "significant cybersecurity incident" can cause harm if unauthorized persons are able to access and use the information system or the information residing on the system. Would the definition work as designed? If not, explain why and suggest modifications to improve its design. Is this design objective appropriate? If not, explain why and suggest an alternative design objective for the second prong of the definition. For example, should the second prong of the definition be limited to cybersecurity incidents that "result" in substantial harm to the Market Entity or substantial harm to a customer, counterparty, member, registrant, or user of the Market entity, or to any other person that interacts with the Market Entity (i.e., not include incidents that are "reasonably likely" to result in these consequences)? If so, explain why and also explain why reporting to the Commission and other regulators (as applicable) and publicly disclosing incidents that are reasonably likely to result in these consequences would not be necessary because they would no longer be significant

²⁰⁸ See paragraphs (c) and (d) of proposed Rule 10 (requiring, respectively, immediate notification and subsequent reporting of significant cybersecurity incidents and public disclosure of significant cybersecurity incidents).

cybersecurity incidents.²⁰⁹ Alternatively, should the second prong of the definition be limited to an incident of unauthorized access or use that leads to "substantial harm" to a customer, counterparty, member, registrant or user of the Covered Entity, or should "inconvenience" to a customer, counterparty, member, registrant or user be enough? If yes, explain why. Should the second prong of the definition be modified so that it is limited to cybersecurity incidents that result in or are reasonably likely to result in substantial harm to more than one customer, counterparty, member, registrant, or user of the Market Entity, or to any other market participant that interacts with the Market Entity? If so, explain why.

20. Should proposed Rule 10 be modified to define additional terms for the purposes of the rule and Parts I and II of proposed Form SCIR? If so, identify the term, suggest a definition, and explain why including the definition would be appropriate. For example, would including additional defined terms improve the clarity of the requirements of proposed Rule 10 and Parts I and II of proposed Form SCIR? If so, explain why. Should proposed Rule 10 be modified to define the terms "confidentiality," "integrity", and "availability"? If so, explain why and suggest definitions.

B. Proposed Requirements for Covered Entities

1. Cybersecurity Risk Management Policies and Procedures

Risk management is the ongoing process of identifying, assessing, and responding to risk.²¹⁰ To manage risk generally, Market Entities should understand the likelihood that an event will occur and the potential resulting impacts.²¹¹ Cybersecurity risk—like other business risks (e.g., market, credit, or liquidity risk)—can be addressed through policies and procedures that are reasonably designed to manage the risk.²¹²

Accordingly, proposed Rule 10 would require Covered Entities to establish, maintain, and enforce written policies and procedures that are reasonably designed to address the Covered Entity's

²⁰⁹ See paragraphs (c) and (d) of proposed Rule 10 (requiring, respectively, immediate notification and subsequent reporting of significant cybersecurity incidents and public disclosure of significant cybersecurity incidents).

²¹⁰ See generally NIST Framework.

²¹¹ *Id.*

²¹² See generally CISA Cyber Essentials Starter Kit (stating that organizations should "approach cyber as business risk").

cybersecurity risks.²¹³ Further, proposed Rule 10 would set forth minimum elements that would need to be included in the policies and procedures.²¹⁴ In particular, the policies and procedures would need to address: (1) risk assessment; (2) user security and access; (3) information protection; (4) cybersecurity threat and vulnerability management; and (5) cybersecurity incident response and recovery. As discussed in more detail below, the inclusion of these elements is designed to enumerate the core areas that Covered Entities would need to address when designing, implementing, and assessing their policies and procedures. Proposed Rule 10 also would require Covered Entities to review annually and assess their policies and procedures and prepare a written report describing the review and other related matters. Taken together, these requirements are designed to position Covered Entities to be better prepared to protect themselves against cybersecurity risks, to mitigate cybersecurity threats and vulnerabilities, and to recover from cybersecurity incidents. They are also designed to help ensure that Covered Entities focus their efforts and resources on the cybersecurity risks associated with their operations and business practices.

The policies and procedures that would be required by proposed Rule 10—because they would need to address the *Covered Entity's cybersecurity risks*—generally should be tailored to the nature and scope of the Covered Entity's business and address the Covered Entity's specific cybersecurity risks. Thus, proposed Rule 10 is not intended to impose a one-size-fits-all approach to addressing cybersecurity risks. In addition, cybersecurity threats are constantly evolving and measures to address those threats continue to evolve. Therefore, proposed Rule 10 is designed to provide Covered Entities with the flexibility to update and modify their policies and procedures as needed so that they continue to be reasonably designed to address the Covered Entity's cybersecurity risks over time.

a. Risk Assessment

Proposed Rule 10 would specify that the Covered Entity's cybersecurity risk management policies and procedures must include policies and procedures that require periodic assessments of cybersecurity risks associated with the

Covered Entity's information systems and information residing on those systems.²¹⁵ Further, with respect to the periodic assessments, the policies and procedures would need to include two components.

First, the policies and procedures would need to provide that the Covered Entity will categorize and prioritize cybersecurity risks based on an inventory of the components of the Covered Entity's information systems and information residing on those systems and the potential effect of a cybersecurity incident on the Covered Entity.²¹⁶ As discussed earlier, proposed Rule 10 would define the term "cybersecurity risk" to mean financial, operational, legal, reputational, and other adverse consequences that could result from cybersecurity incidents, cybersecurity threats, and cybersecurity vulnerabilities.²¹⁷ For example, Covered Entities may be subject to different cybersecurity risks as a result of, among other things: (1) the functions they perform and the extent to which they use information systems to perform those functions; (2) the criticality of the functions they perform that rely on information systems; (3) the interconnectedness of their information systems with third-party information

systems; (4) the software that operates on their information systems, including whether it is proprietary or vendor-supplied software; (5) the nature and volume of the information they store on information systems (e.g., personal, confidential, and/or proprietary information); (6) the complexity and scale of their information systems (i.e., the size of their IT footprint); (7) the location of their information systems; (8) the number of users authorized to access their information systems; (9) the types of devices permitted to access their information systems (e.g., company-owned or personal desktop computers, laptop computers, or smart phones); (10) the extent to which they conduct international operations and allow access to their information systems from international locations; and (11) the extent to which employees access their information systems from remote locations, including international locations. In categorizing and prioritizing cybersecurity risks, the Covered Entity generally should consider consulting with, among others, personnel familiar with the Covered Entity's operations, its business partners, and third-party cybersecurity experts.²¹⁸ In addition, a Covered Entity could consider an escalation protocol in its risk assessment plan to ensure that its senior officers, including appropriate legal and compliance personnel, receive necessary information regarding cybersecurity risks on a timely basis.²¹⁹ Only after assessing, categorizing, and prioritizing its cybersecurity risks can a Covered Entity establish, maintain, and enforce reasonably designed cybersecurity policies and procedures under proposed Rule 10 to address those risks.

A Covered Entity also would need to reassess and re-prioritize its cybersecurity risks periodically. The Covered Entity would need to determine the frequency of these assessments and the types of developments in

²¹³ See paragraph (b)(1)(i)(A) of proposed Rule 10. See generally NIST Framework (providing that the first core element of the framework is "identify"—meaning develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities); IOSCO Cybersecurity Report ("A key component of the risk management program is the identification of critical assets, information and systems, including order routing systems, risk management systems, execution systems, data dissemination systems, and surveillance systems. Practices supporting the identification function include the establishment and maintenance of an inventory of all hardware and software. This risk management program should also typically include third-party and technology providers' security assessments. Finally, accessing information about the evolving threat landscape is important in identifying the changing nature of cyber risk.").

²¹⁴ See paragraph (b)(1)(i)(A)(1) of proposed Rule 10. See generally CISA Cyber Essentials Starter Kit ("Consider how much your organization relies on information technology to conduct business and make it a part of your culture to plan for contingencies in the event of a cyber incident. Identify and prioritize your organization's critical assets and the associated impacts to operations if an incident were to occur. Ask the questions that are necessary to understanding your security planning, operations, and security-related goals. Develop an understanding of how long it would take to restore normal operations. Resist the "it can't happen here" pattern of thinking. Instead, focus cyber risk discussions on "what-if" scenarios and develop an incident response plan to prepare for various cyber events and scenarios.").

²¹⁵ See paragraph (a)(3) of proposed Rule 10; see also paragraphs (a)(2), (a)(4), and (a)(5) of proposed Rule 10 (defining, respectively, the terms "cybersecurity incident," "cybersecurity threat," and "cybersecurity vulnerability," which are used in the definition of "cybersecurity risk").

²¹⁶ See generally CISA Cyber Essentials Starter Kit ("[H]ave conversations with your staff, business partners, vendors, managed service providers, and others within your supply chain. . . . Maintain situational awareness of cybersecurity threats and explore available communities of interest. These may include sector-specific Information Sharing and Analysis Centers, government agencies, law enforcement, associations, vendors, etc.").

²¹⁷ See generally *id.* (stating that organizational leaders drive cybersecurity strategy, investment, and culture, and that leaders should, among other things: (1) use risk assessments to identify and prioritize allocation of resources and cyber investments; (2) perform a review of all current cybersecurity and risk policies and identify gaps or weaknesses; and (3) develop a policy roadmap, prioritize policy creation and updates based on the risk to the organization as determined by business leaders and technical staff).

²¹³ See paragraph (b)(1) of proposed Rule 10.

²¹⁴ See paragraphs (b)(1)(i) through (v) of proposed Rule 10. Covered Entities may wish to consult a number of resources in connection with these elements. See generally NIST Framework; CISA Cyber Essentials Starter Kit.

cybersecurity risk that would trigger an assessment based on its particular circumstances. Consequently, the Covered Entity generally should consider whether to reassess its cybersecurity risks to reflect internal changes as they arise, such as changes to its business, online presence, or customer website access, or external changes, such as changes in the evolving technology and cybersecurity threat landscape.²²⁰ The Covered Entity generally should also consider raising any material changes in its risk assessment plan to senior officers, as appropriate. In assessing ongoing and emerging cybersecurity threats, a Covered Entity could monitor and consider updates and guidance from private sector and governmental resources, such as the FS-ISAC and CISA.²²¹

Second, the policies and procedures would need to require the Covered Entity to identify its service providers that receive, maintain, or process information, or are otherwise permitted to access its information systems and the information residing on those systems, and assess the cybersecurity risks associated with its use of these service providers.²²² Covered Entities are exposed to cybersecurity risks through the technology of their service providers.²²³ Having identified the

²²⁰ See generally *id.* (“Maintain awareness of current events related to cybersecurity. Be proactive; alert staff to hazards that the organization may encounter. Maintain vigilance by asking yourself: what types of cyber attack[s] are hitting my peers or others in my industry? What tactics were successful in helping my peers limit damage? What does my staff need to know to help protect the organization and each other? On a national-level, are there any urgent cyber threats my staff need to know about?”).

²²¹ The FS-ISAC is a global private industry cyber intelligence sharing community solely focused on financial services. Additional information about FS-ISAC is available at <https://www.fsisac.com>. Often, private industry groups maintain relationships and information sharing agreements with government cybersecurity organizations, such as CISA. Private sector companies, such as information technology and cybersecurity consulting companies, may have insights on cybersecurity (given the access their contractual status gives them to customer networks) that the government initially does not. See, e.g., Verizon DBIR; Microsoft Report. For example, private-sector cybersecurity firms may often be in the position to spot new malicious cybersecurity trends before they become more widespread and common.

²²² See paragraph (b)(1)(i)(A)(2) of proposed Rule 10; paragraphs (a)(6) and (7) of proposed Rule 10 (defining, respectively, the terms “information” and “information systems”). Oversight of third-party service provider or vendor risk is a component of many cybersecurity frameworks. See, e.g., NIST Framework (discussing supply chain risks associated with products and services an organization uses).

²²³ See GAO Cyber Security Report (“Increased connectivity with third-party providers and the potential for increased cyber risk is a concern in the

relevant service providers, the Covered Entity would need to assess how they expose it to cybersecurity risks. In identifying these cybersecurity risks, the service provider’s cybersecurity practices would be relevant, including: (1) how the service provider protects itself against cybersecurity risk; and (2) its ability to respond to and recover from cybersecurity incidents.

A Covered Entity generally should take into account whether a cybersecurity incident at a service provider could lead to process failures or the unauthorized access to or use of information or information systems. For example, a Covered Entity may use a cloud service provider to maintain required books and records. If all of the Covered Entity’s books and records were concentrated at this cloud service provider and a cybersecurity incident disrupts or degrades the cloud service provider’s information systems, there could potentially be detrimental data loss affecting the ability of the Covered Entity to provide services and comply with regulatory obligations. Accordingly, as part of identifying the cybersecurity risks associated with using a cloud service provider, a Covered Entity should consider how the service provider will secure and maintain data and whether the service provider has response and recovery procedures in place such that any compromised or lost data in the event of a cybersecurity incident can be recovered and restored.

Finally, the Covered Entity’s risk assessment policies and procedures would need to require written documentation of these risk assessments.²²⁴ This documentation would be relevant to the reviews performed by the Covered Entity to analyze whether the policies and procedures need to be updated, to inform the Covered Entity of risks specific to it, and to support responses to cybersecurity risks by identifying cybersecurity threats to information systems that, if compromised, could

financial industry as core systems and critical data are moved offsite to third parties.”). For purposes of proposed Rule 10, the Covered Entity’s assessment of service providers should not be limited to only certain service providers, such as those that provide core functions or services for the Covered Entity. Rather, the cybersecurity risk of any service provider that receives, maintains, or processes information, or is otherwise permitted to access the information systems of the Covered Entity and the information residing on those systems should be evaluated. Furthermore, it is possible that a service provider for a Covered Entity may itself be a Covered Entity under proposed Rule 10. For example, a carrying broker-dealer may be a service provider for a number of introducing broker-dealers.

²²⁴ See paragraph (b)(1)(i)(B) of proposed Rule 10.

result in significant cybersecurity incidents.²²⁵ It also could be used by Commission and SRO staff and possibly internal auditors of the Covered Entity to examine for adherence to the risk assessment policies and procedures.

b. User Security and Access

Proposed Rule 10 would specify that the Covered Entity’s cybersecurity risk management policies and procedures must include controls designed to minimize user-related risks and prevent unauthorized access to the Covered Entity’s information systems and the information residing on those systems.²²⁶ Further, the rule would require that these policies and procedures include controls addressing five specific aspects relating to user security and access.

First, there would need to be controls requiring standards of behavior for individuals authorized to access the Covered Entity’s information systems and the information residing on those systems, such as an acceptable use policy.²²⁷ Second, there would need to be controls for identifying and authenticating individual users, including but not limited to implementing authentication measures that require users to present a combination of two or more credentials for access verification.²²⁸ Third, there would need to be controls for establishing procedures for the timely distribution, replacement, and revocation of passwords or methods of

²²⁵ See paragraph (b)(2) of proposed Rule 10 (which would require a Covered Entity to review and assess the design and effectiveness of the cybersecurity policies and procedures, including whether the policies and procedures reflect changes in cybersecurity risk over the time period covered by the review). See also section II.B.1.f. of this release (discussing the review proposal in more detail).

²²⁶ See paragraph (b)(1)(ii) of proposed Rule 10; paragraphs (a)(6) and (7) of proposed Rule 10 (defining, respectively, the terms “information” and “information systems”). See generally NIST Framework (providing that the second core element of the framework is “protect”—meaning develop and implement appropriate safeguards to ensure delivery of critical services); CISA Cyber Essentials Starter Kit (stating with respect to user security and access that (among other things): (1) the authority and access granted employees, managers, and customers into an organization’s digital environment needs limits; (2) setting approved access privileges requires knowing who operates on an organization’s systems and with what level of authorization and accountability; and (3) organizations should ensure only those who belong on their “digital workplace have access”); IOSCO Cybersecurity Report (stating that network access controls are one of the types of controls trading venues use as the protection function).

²²⁷ See paragraph (b)(1)(ii)(A) of proposed Rule 10.

²²⁸ See paragraph (b)(1)(ii)(B) of proposed Rule 10.

authentication.²²⁹ Fourth, there would need to be controls for restricting access to specific information systems of the Covered Entity or components thereof and the information residing on those systems solely to individuals requiring access to the systems and information as is necessary for them to perform their responsibilities and functions on behalf of the Covered Entity.²³⁰ Fifth, there would need to be controls for securing remote access technologies.²³¹

The objective of these policies, procedures, and controls would be to protect the Covered Entity's information systems from unauthorized access and improper use. There are a variety of controls that a Covered Entity, based on its particular circumstances, could include in these policies and procedures to make them reasonably designed to achieve this objective. For example, access to information systems could be controlled through the issuance of user credentials, digital rights management with respect to proprietary hardware and copyrighted software, authentication and authorization methods (e.g., multi-factor authentication and geolocation), and tiered access to personal, confidential, and proprietary information and data and network resources.²³² Covered Entities may wish to consider multi-factor authentication methods that are not based solely on SMS-delivery (e.g., text message delivery) of authentication codes, because SMS-delivery methods may provide less security than other non-SMS based multi-factor authentication methods. Furthermore, Covered Entities could require employees to attend cybersecurity training on how to secure sensitive data and recognize harmful files prior to obtaining access to certain information systems. The training generally could address best practices in creating new

passwords, filtering through suspicious emails, or browsing the internet.²³³

Further, a Covered Entity could use controls to monitor user access regularly in order to remove users that are no longer authorized. These controls generally should address the Covered Entity's employees (e.g., removing access for employees that leave the firm) and external users of the Covered Entity's information systems (e.g., customers that no longer use the firm's services or external service providers that no longer are under contract with the firm to provide it with any services). In addition, controls to monitor for unauthorized login attempts and account lockouts, and the handling of customer requests, including for user name and password changes, could be a part of reasonably designed policies and procedures. Similarly, controls to assess the need to authenticate or investigate any unusual customer, member, or user requests (e.g., wire transfer or withdrawal requests) could be a part of reasonably designed policies and procedures.

A Covered Entity also generally should take into account the types of technology through which its users access the Covered Entity's information systems. For example, mobile devices (whether firm-issued or personal devices) that allow employees to access information systems and personal, confidential, or proprietary information residing on these systems may create additional and unique vulnerabilities, including when such devices are used internationally. Consequently, controls limiting mobile or other devices approved for remote access to those issued by the firm or enrolled through a mobile device manager could be part of reasonably designed policies and procedures.

In addition, a Covered Entity could consider controls with respect to its network perimeter such as securing remote network access used by teleworking and traveling employees. This could include controls to identify threats on a network's endpoints. For example, Covered Entities could consider using software that monitors and inspects all files on an endpoint, such as a mobile phone or remote laptop, and identifies and blocks incoming unauthorized communications. Covered Entities generally would need to consider potential user-related and access risks

relating to the remote access technologies used at their remote work and telework locations to include controls designed to secure such technologies. For example, a Covered Entity's personnel working remotely from home or a co-working space may create unique cybersecurity risks—such as unsecured or less secure Wi-Fi—that threat actors could exploit to access the Covered Entity's information systems and the information residing on those systems. Accordingly, a Covered Entity could consider whether its user security and access policies, procedures, and controls should have controls requiring approval of mobile or other devices for remote access, and whether training on device policies would be appropriate. The training for remote workers in particular could focus on phishing, social engineering, compromised passwords, and the consequences of weak network security.

c. Information Protection

Information protection is a key aspect of managing cybersecurity risk.²³⁴ Therefore, proposed Rule 10 would specify that the Covered Entity's cybersecurity risk management policies and procedures would need to address information protection in two ways.²³⁵ First, the policies and procedures would need to include measures designed to protect the Covered Entity's information systems and protect the information residing on those systems from unauthorized access or use, based on a periodic assessment of the Covered

²²⁹ See paragraph (b)(1)(ii)(C) of proposed Rule 10.

²³⁰ See paragraph (b)(1)(ii)(D) of proposed Rule 10.

²³¹ See paragraph (b)(1)(ii)(E) of proposed Rule 10; paragraphs (a)(6) and (7) of proposed Rule 10 (defining, respectively, the terms "information" and "information systems").

²³² See generally CISA Cyber Essentials Starter Kit (stating that organizations should (among other things): (1) learn who is on their networks and maintain inventories of network connections (e.g., user accounts, vendors, and business partners); (2) leverage multi-factor authentication for all users, starting with privileged, administrative and remote access users; (3) grant access and administrative permissions based on need-to-know basis; (4) leverage unique passwords for all user accounts; and (5) develop IT policies and procedures addressing changes in user status (e.g., transfers and terminations).

²³³ See generally CISA Cyber Essentials Starter Kit (stating that organizations should (among other things) leverage basic cybersecurity training to improve exposure to cybersecurity concepts, terminology, and activates associated with implementing cybersecurity best practices).

²³⁴ See generally NIST Framework ("The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology."); IOSCO Cybersecurity Report ("There are numerous controls and protection measures that regulated entities may wish to consider in enhancing their cyber security. Such measures can be organizational (like the establishment of security operations centers) or technical (like anti-virus and intrusion prevention systems). Risk assessments help determine the minimum level of controls to be implemented within a project, an application or a database. In addition, employee training and awareness initiatives are critical parts of any cyber security program, including induction programs for newcomers, general training, as well as more specific training (for instance, social engineering awareness). Proficiency tests could be conducted to demonstrate staff understanding and third party training could also be organized. Other initiatives which contribute to raising employees' awareness of cyber security threats include monthly security bulletins emailed to all employees, regular communications regarding new issues and discovered vulnerabilities, use of posters and screen savers, and regular reminders sent to employees. Mock tests can also be conducted to assess employees' preparedness. Employees are also often encouraged to report possible attacks.").

²³⁵ See paragraph (b)(1)(iii) of proposed Rule 10.

Entity's information systems and the information that resides on the systems.²³⁶ The periodic assessment would need to take into account: (1) the sensitivity level and importance of the information to the Covered Entity's business operations; (2) whether any of the information is personal information;²³⁷ (3) where and how the information is accessed, stored and transmitted, including the monitoring of information in transmission; (4) the information systems' access controls and malware protection;²³⁸ and (5) the potential effect a cybersecurity incident involving the information could have on the Covered Entity and its customers, counterparties, members, registrants, or users, including the potential to cause a significant cybersecurity incident.²³⁹

By performing these assessments, a Covered Entity should be able to determine the measures it would need to implement to prevent the unauthorized access or use of information residing on its information systems. Measures that could be used for this purpose include encryption, network segmentation, and access controls to ensure that only authorized users have access to personal, confidential, and proprietary information and data or critical systems. Measures to identify suspicious behavior also could be used for this purpose. These measures could include consistent monitoring of systems and personnel, such as the generation and review of activity logs, identification of

potential anomalous activity, and escalation of issues to senior officers, as appropriate. Further data loss prevention measures could include processes to identify personal, confidential, or proprietary information and data (e.g., account numbers, Social Security numbers, trade information, and source code) and block its transmission to external parties. Additional measures could include testing of systems, including penetration tests. A Covered Entity also could consider measures to track the actions taken in response to findings from testing and monitoring, material changes to business operations or technology, or any other significant events. Appropriate measures for preventing the unauthorized use of information may differ depending on the circumstances of a Covered Entity, such as the systems used by the Covered Entity, the Covered Entity's relationship with service providers, or the level of access granted by the Covered Entity to employees or contractors. Appropriate measures generally should evolve with changes in technology and the increased sophistication of cybersecurity attacks.

Second, the policies and procedures for protecting information would need to require oversight of service providers that receive, maintain, or process the Covered Entity's information, or are otherwise permitted to access the Covered Entity's information systems and the information residing on those systems, pursuant to a written contract between the covered entity and the service provider.²⁴⁰ Further, pursuant to that written contract, the service provider would be required to implement and maintain appropriate measures, including the practices described in paragraphs (b)(1)(i) through (v) of proposed Rule 10, that are designed to protect the Covered Entity's information systems and information residing on those systems. These policies and procedures could include measures to perform due diligence on a service provider's cybersecurity risk management prior to using the service provider and periodically thereafter during the relationship with the service provider. Covered Entities also could consider including periodic contract review processes that allow them to assess whether, and help to ensure that, their agreements with service providers contain provisions that require service providers to implement and maintain appropriate measures designed to

protect the Covered Entity's information systems and information residing on those systems.

d. Cybersecurity Threat and Vulnerability Management

Rule 10 would specify that the Covered Entity's cybersecurity risk management policies and procedures must include measures designed to detect, mitigate, and remediate any cybersecurity threats and vulnerabilities with respect to the Covered Entity's information systems and information residing on those systems.²⁴¹ Because Covered Entities depend on information systems to process, store, and transmit personal, confidential, and proprietary information and data and to conduct critical business functions, it is essential that they manage cybersecurity threats and vulnerabilities effectively.²⁴² Moreover, detecting, mitigating, and remediating threats and vulnerabilities is essential to preventing significant cybersecurity incidents.

Measures to detect cybersecurity threats and vulnerabilities could include ongoing monitoring (e.g., comprehensive examinations and risk management processes), including, for example, conducting network, system, and application vulnerability assessments. This could include scans or reviews of internal systems, externally facing systems, new systems, and systems used by service providers. Further, measures could include monitoring industry and government

²³⁶ See paragraph (b)(1)(iii)(A) of proposed Rule 10; paragraphs (a)(6) and (7) of proposed Rule 10 (defining, respectively, the terms "information" and "information systems"). See generally CISA Cyber Essentials Starter Kit ("Learn what information resides on your network. Inventory critical or sensitive information. An inventory of information assets provides an understanding of what you are protecting, where that information resides, and who has access. The inventory can be tracked in a spreadsheet, updated quickly and frequently").

²³⁷ See paragraph (a)(9) of proposed Rule 10 (defining the term "personal information").

²³⁸ See generally CISA Cyber Essentials Starter Kit ("Leverage malware protection capabilities. Malware is designed to spread quickly. A lack of defense against it can completely corrupt, destroy or render your data inaccessible.").

²³⁹ See paragraphs (b)(1)(iii)(A)(1) through (5) of proposed Rule 10. See generally CISA Cyber Essentials Starter Kit ("Learn how your data is protected. Data should be handled based on its importance to maintaining critical operations in order to understand what your business needs to operate at a basic level. For example, proprietary research, financial information, or development data need protection from exposure in order to maintain operations. Understand the means by which your data is currently protected; focus on where the protection might be insufficient. Guidance from the Cyber Essentials Toolkits, including authentication, encryption, and data protection help identify methods and resources for how to best secure your business information and devices.").

²⁴⁰ See paragraph (b)(1)(iii)(B) of proposed Rule 10; paragraphs (a)(6) and (7) of proposed Rule 10 (defining, respectively, the terms "information" and "information systems").

²⁴¹ See paragraph (b)(1)(iv) of proposed Rule 10; paragraphs (a)(4) through (7) of proposed Rule 10 (defining, respectively, the terms "cybersecurity threat," "cybersecurity vulnerability," "information," and "information systems"). See generally NIST Framework (providing that the third core element of the framework is "detect"—meaning develop and implement appropriate activities to identify the occurrence of a cybersecurity event); CISA Cyber Essentials Starter Kit (stating regarding detection that organizations should (among other things): (1) learn what is happening on their networks; (2) manage network and perimeter components, host and device components, data at rest and in transit, and user behavior and activities; and (3) actively maintain information as it will provide a baseline for security testing, continuous monitoring, and making security-based decisions); IOSCO Cybersecurity Report ("External and internal monitoring of traffic and logs generally should be used to detect abnormal patterns of access (e.g., abnormal user activity, odd connection durations, and unexpected connection sources) and other anomalies. Such detection is crucial as attackers can use the period of presence in the target's systems to expand their footprint and their access gaining elevated privileges and control over critical systems. Many regulated entities have dedicated cyber threat teams and engage in file servers integrity and database activity monitoring to prevent unauthorized modification of critical servers within their organization's enterprise network. Different alarm categories and severity may be defined.").

²⁴² See section I.A.2. of this release (discussing how Covered Entities use information systems).

sources for new threat and vulnerability information that may assist in detecting cybersecurity threats and vulnerabilities.²⁴³

Measures to mitigate and remediate an identified threat or vulnerability are more effective if they minimize the window of opportunity for attackers to exploit vulnerable hardware and software. These measures could include, for example, implementing a patch management program to ensure timely patching of hardware and software vulnerabilities and maintaining a process to track and address reports of vulnerabilities.²⁴⁴ Covered Entities also generally should consider the vulnerabilities associated with “end of life systems” (*i.e.*, systems in which software is no longer supported by the particular vendor and for which security patches are no longer issued). These measures also could establish accountability for handling vulnerability reports by, for example, establishing processes for their intake, assignment, escalation, remediation, and remediation testing. For example, a Covered Entity could use a vulnerability tracking system that includes severity ratings, and metrics for measuring the time it takes to identify, analyze, and remediate vulnerabilities.

Covered Entities also could consider role-specific cybersecurity threat and vulnerability response training.²⁴⁵ For example, training could include secure system administration courses for IT professionals, vulnerability awareness and prevention training for web application developers, and social engineering awareness training for employees and executives. Covered Entities that do not proactively address threats and discovered vulnerabilities face an increased likelihood of having their information systems—including the Covered Entity’s information

residing on those systems—accessed or disrupted by threat actors or otherwise compromised. The requirement for Covered Entities to include cybersecurity threats and vulnerabilities measures in their cybersecurity policies and procedures is designed to address this risk and help ensure threats and vulnerabilities are adequately and proactively addressed by Covered Entities.

e. Cybersecurity Incident Response and Recovery

Proposed Rule 10 would specify that the Covered Entity’s cybersecurity risk management policies and procedures must include measures designed to detect, respond to, and recover from a cybersecurity incident.²⁴⁶ Further, the rule would require that these measures include policies and procedures that are reasonably designed to ensure: (1) the continued operations of the Covered Entity; (2) the protection of the Covered Entity’s information systems and the information residing on those systems;²⁴⁷ (3) external and internal cybersecurity incident information sharing and communications; and (4) the reporting of significant cybersecurity incidents pursuant to the requirements of paragraph (c) of proposed Rule 10 discussed below.²⁴⁸

²⁴⁶ See paragraph (b)(1)(v) of proposed Rule 10; paragraph (c)(2) of proposed Rule 10 (defining the term “cybersecurity incident”). See generally NIST Framework (providing that the fourth core element of the framework is “respond”—meaning develop and implement appropriate activities to take action regarding a detected cybersecurity incident; and providing that the fifth core element of the framework is “recover”—meaning develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident).

²⁴⁷ See paragraphs (a)(6) and (7) of proposed Rule 10 (defining, respectively, the terms “information” and “information systems”).

²⁴⁸ See section II.B.2. of this release (discussing the requirements to report significant cybersecurity incidents); paragraph (a)(10) of proposed Rule 10 (defining the term “significant cybersecurity incident”). See generally CISA Cyber Essentials Starter Kit (stating regarding response and recovery that the objective is to limit damage and accelerate restoration of normal operations and, to this end, organizations (among other things) can: (1) leverage business impact assessments to prioritize resources and identify which systems must be recovered first; (2) “learn who to call for help (*e.g.*, outside partners, vendors, government/industry responders, technical advisors and law enforcement);” (3) develop an internal reporting structure to detect, communicate and contain attacks; and (4) develop in-house containment measures to limit the impact of cyber incidents when they occur); IOSCO Cybersecurity Report (“Regulated entities generally should consider developing response plans for those types of incidents to which the organization is most likely to be subject. Elements associated with response plans may include: preparing communication/notification plans to inform relevant stakeholders; conducting forensic analysis to understand the anatomy of a breach or an attack;

Cybersecurity incidents can lead to significant business disruptions, including losing the ability to send internal or external communications, transmit information, or connect to internal or external systems necessary to carry out the Covered Entity’s critical functions and provide services to customers, counterparties, members, registrants, or users.²⁴⁹ They also can lead to the inability to access accounts holding cash or other financial assets of the Covered Entity or its customers, counterparties, members, registrants, or users.²⁵⁰ Therefore, the proposed incident response and recovery policies and procedures are designed to place the Covered Entity in a position to respond to a cybersecurity incident, which should help to reduce business disruptions and other harms the incident may cause the Covered Entity or its customers, counterparties, members, registrants, or users. A cybersecurity program with a clear incident response plan designed to ensure continued operational capability, and the protection of, and access to, personal, confidential, or proprietary information and data, even if a Covered Entity loses access to its systems, would assist in mitigating the effects of a cybersecurity incident.²⁵¹ A Covered Entity, therefore, may wish to consider maintaining physical copies of its incident response plan—and other cybersecurity policies and procedures—to help ensure they can be accessed and implemented during a cybersecurity incident.

Covered Entities generally should focus on operational capability in creating reasonably designed policies and procedures to ensure their continued operations in the event of a cybersecurity incident (*e.g.*, the ability to withstand a DoS attack). The objective is to place Covered Entities in a position to be able to continue providing services to other Market Entities and other participants in the U.S. securities markets (including investors) and, thereby, continue to support the fair, orderly, and efficient

maintaining a database recording cyber attacks; and conducting cyber drills, firm specific simulation exercises as well as industry-wide scenario exercises.”).

²⁴⁹ See sections I.A.1. and I.A.2. of this release (discussing these consequences).

²⁵⁰ *Id.*

²⁵¹ See generally CISA Cyber Essentials Starter Kit (“Plan, prepare, and conduct drills for cyber-attacks and incidents as you would a fire or robbery. Make your reaction to cyber incidents or system outages an extension of your other business contingency plans. This involves having incident response plans and procedures, trained staff, assigned roles and responsibilities, and incident communications plans.”).

²⁴³ See generally CISA, *National Cyber Awareness System—Alerts*, available at <https://us-cert.cisa.gov/ncas/alerts> (providing information about current security issues, vulnerabilities, and exploits).

²⁴⁴ See generally CISA Cyber Essentials Starter Kit (stating that organizations should: (1) enable automatic updates whenever possible; (2) replace unsupported operating systems, applications and hardware; and (3) test and deploy patches quickly).

²⁴⁵ See generally CISA Cyber Essentials Starter Kit (“Leverage basic cybersecurity training. Your staff needs a basic understanding of the threats they encounter online in order to effectively protect your organization. Regular training helps employees understand their role in cybersecurity, regardless of technical expertise, and the actions they take help keep your organization and customers secure. Training should focus on threats employees encounter, like phishing emails, suspicious events to watch for, and simple best practices individual employees can adopt to reduce risk. Each aware employee strengthens your network against attack, and is another ‘sensor’ to identify an attack.”).

operation of the U.S. securities markets. For example, this requirement is designed to place Covered Entities in a position to be able to continue to perform market and member surveillance and oversight in the case of SROs, clearance and settlement in the case of clearing agencies, and brokerage or dealing activities in the case of broker-dealers and SBSBs.

The ability of Covered Entities to recover from a cybersecurity incident in a timeframe that minimizes disruptions to their business or regulatory activities is critically important to the fair, orderly, and efficient operations of the U.S. securities markets and, therefore, to the U.S. economy, investors, and capital formation. A Covered Entity generally should consider implementing safeguards, such as backing up data, which can help facilitate a prompt recovery that allows the Covered Entity to resume operations following a cybersecurity incident.²⁵² A Covered Entity also generally should consider whether to designate personnel to perform specific roles in the case of a cybersecurity incident. This could entail identifying and/or hiring personnel or third parties who have the requisite cybersecurity and recovery expertise (or are able to coordinate effectively with outside experts) as well as identifying personnel who should be kept informed throughout the response and recovery process. In addition, a Covered Entity could consider an escalation protocol in its incident response plan to ensure that its senior officers, including appropriate legal and compliance personnel, receive necessary information regarding cybersecurity incidents on a timely basis.²⁵³

²⁵² See generally CISA Cyber Essentials Starter Kit (“Leverage protections for backups, including physical security, encryption and offline copies. Ensure the backed-up data is stored securely offsite or in the cloud and allows for at least seven days of incremental rollback. Backups should be stored in a secure location, especially if you are prone to natural disasters. Periodically test your ability to recover data from backups. Online and cloud storage backup services can help protect against data loss and provide encryption as an added level of security. Identify key files you need access to if online backups are unavailable to access your files when you do not have an internet connection.”).

²⁵³ See generally CISA Cyber Essentials Starter Kit (stating that: (1) organizations should develop an internal reporting structure to detect, communicate, and contain attacks and that effective communication plans focus on issues unique to security breaches; (2) a standard reporting procedure will reduce confusion and conflicting information between leadership, the workforce, and stakeholders; and (3) communication should be continuous, since most data breaches occur over a long period of time and not instantly and that it should come from top leadership to show commitment to action and knowledge of the situation).

Moreover, as discussed in further detail below, under proposed Rule 10, a Covered Entity would need to give the Commission immediate written electronic notice of a significant cybersecurity incident after having a reasonable basis to conclude that the incident has occurred or is occurring.²⁵⁴ Further, the Covered Entity would need to report information about the significant cybersecurity incident promptly, but no later than 48 hours, after having a reasonable basis to conclude that the incident has occurred or is occurring by filing Part I of proposed Form SCIR with the Commission.²⁵⁵ Thereafter, the Covered Entity would need to file an amended Part I of proposed Form SCIR with the Commission under certain circumstances.²⁵⁶ Accordingly, proposed Rule 10 would require the Covered Entity to include in its incident response and recovery policies and procedures measures designed to ensure compliance with these notification and reporting requirements.²⁵⁷ The Covered Entity also may wish to implement a process to determine promptly whether and how to contact local and Federal law enforcement authorities, such as the FBI, about an incident.²⁵⁸

A Covered Entity also could consider including periodic testing requirements in its incident response and recovery policies and procedures.²⁵⁹ These tests

²⁵⁴ See paragraph (c)(1) of proposed Rule 10. See also section II.B.2. of this release (discussing this proposed notification requirement in more detail).

²⁵⁵ See paragraph (c)(2) of proposed Rule 10. See also section II.B.2. of this release (discussing this proposed reporting requirement in more detail).

²⁵⁶ The circumstances under which an amended Part I of proposed Form SCIR would need to be filed are discussed below in section II.B.2. of this release.

²⁵⁷ See paragraph (b)(1)(v)(A)(4) of proposed Rule 10.

²⁵⁸ For example, the FBI has instructed individuals and organizations to contact their nearest FBI field office to report cybersecurity incidents or to report them online at <https://www.ic3.gov/Home/FileComplaint>. See FBI, *What We Investigate, Cyber Crime*, available at <https://www.fbi.gov/investigate/cyber>. See also CISA Cyber Essentials Starter Kit (“As part of your incident response, disaster recovery, and business continuity planning efforts, identify and document partners you will call on to help. Consider building these relationships in advance and understand what is required to obtain support. CISA and the Federal Bureau of Investigation (FBI) provide dedicated hubs for helping respond to cyber and critical infrastructure attacks. Both have resources and guidelines on when, how, and to whom an incident is to be reported in order to receive assistance. You should also file a report with local law enforcement, so they have an official record of the incident.”).

²⁵⁹ See generally CISA Cyber Essentials Starter Kit (“Lead development of an incident response and disaster recovery plan outlining roles and responsibilities. Test it often. Incident response plans and disaster recovery plans are crucial to information security, but they are separate plans. Incident response mainly focuses on information

could assess the efficacy of the policies and procedures to determine whether any changes are necessary, for example, through tabletop or full-scale exercises. Relatedly, proposed Rule 10 would require that the incident response and recovery policies and procedures include written documentation of a cybersecurity incident, including the Covered Entity’s response to and recovery from the incident.²⁶⁰ This record could be used by the Covered Entity to assess the efficacy of, and adherence to, its incident response and recovery policies and procedures. It further could be used as a “lessons-learned” document to help the Covered Entity respond more effectively the next time it experiences a cybersecurity incident. The Commission staff and SRO staff also would use the records to review compliance with this aspect of proposed Rule 10.

f. Annual Review and Required Written Reports

In addition to requiring a Covered Entity to establish, maintain, and enforce written policies and procedures to address cybersecurity risk, proposed Rule 10 would require the Covered Entity, at least annually, to: (1) review and assess the design and effectiveness of the cybersecurity policies and procedures, including whether the policies and procedures reflect changes in cybersecurity risk over the time period covered by the review; and (2) prepare a written report that describes the review, the assessment, and any control tests performed, explains their results, documents any cybersecurity incident that occurred since the date of the last report, and discusses any material changes to the policies and procedures since the date of the last report.²⁶¹ The annual review requirement is designed to require the Covered Entity to evaluate whether its cybersecurity policies and procedures continue to work as designed. In making this assessment, Covered Entities generally should consider whether changes are needed to ensure their continued effectiveness, including oversight of any delegated responsibilities. As discussed earlier, the sophistication of the tactics,

asset protection, while disaster recovery plans focus on business continuity. Once you develop a plan, test the plan using realistic simulations (known as “war-gaming”), where roles and responsibilities are assigned to the people who manage cyber incident responses. This ensures that your plan is effective and that you have the appropriate people involved in the plan. Disaster recovery plans minimize recovery time by efficiently recovering critical systems.”).

²⁶⁰ See paragraph (b)(1)(v)(B) of proposed Rule 10.

²⁶¹ See paragraph (b)(2) of proposed Rule 10.

techniques, and procedures employed by threat actors is increasing.²⁶² The review requirement is designed to impose a discipline on Covered Entities to be vigilant in assessing whether their cybersecurity risk management policies and procedures continue to be reasonably designed to address this risk.

The review would need to be conducted no less frequently than annually. As discussed above, one of the required elements that would need to be included in the policies and procedures is the requirement to perform periodic assessments of cybersecurity risks associated with the covered entity's information systems and information residing on those systems.²⁶³ Based on the findings of those risk assessments, a Covered Entity could consider whether to perform a review prior to the one-year anniversary of the last review. In addition, the occurrence of a cybersecurity incident or significant cybersecurity incident impacting the Covered Entity or other entities could cause the Covered Entity to consider performing a review before the next annual review is required.

The Covered Entity would need to document the review in a written report.²⁶⁴ The required written report generally should be prepared or overseen by the persons who administer the Covered Entity's cybersecurity program. This report requirement is designed to assist the Covered Entity in evaluating the efficacy of organization's cybersecurity risk management policies and procedures. Additionally, the requirement to review and assess the design and effectiveness of the cybersecurity policies and procedures includes whether they reflect changes in cybersecurity risk over the time period covered by the review. Therefore, the Covered Entity generally would need to take into account the periodic assessments of cybersecurity risks performed pursuant to the requirements of paragraphs (b)(1)(i)(A) and (b)(1)(iii)(A) of proposed Rule. This could provide Covered Entities with valuable insights into potential enhancements to the policies and procedures to keep them up-to-date (*i.e.*, reasonably designed to address emerging cybersecurity threats). For

example, incorporating the cybersecurity risk assessments into the required written report could provide senior officers who review the report with information on the specific risks identified in the assessments. This could lead them to ask questions and seek relevant information regarding the effectiveness of the Covered Entity's cybersecurity risk management policies and procedures and its implementation in light of those risks. This could include questions as to whether the Covered Entity has adequate resources with respect to cybersecurity matters, including access to cybersecurity expertise.

g. Request for Comment

The Commission requests comment on all aspects of the requirements that Covered Entities establish, maintain, and enforce written policies and procedures to address their cybersecurity risks, the elements that would need to be included in the cybersecurity risk management policies and procedures, and the required (at least) annual review of the cybersecurity risk management policies and procedure under paragraph (b) of proposed Rule 10. In addition, the Commission is requesting comment on the following specific aspects of the proposals:

21. In designing the cybersecurity risk management policies and procedures requirements of proposed Rule 10, the Commission considered a number of sources cited in the sections above, including, in particular, the NIST Framework and the CISA Cyber Essentials Starter Kit. Are there other sources the Commission should use? If so, identify them and explain why they should be considered and how they could inform potential modifications to the cybersecurity risk management policies and procedures requirements.

22. Should the policies and procedures requirements of paragraph (b)(1) of proposed Rule 10 be modified? For example, are there other elements that should be included in cybersecurity risk management policies and procedures? If so, identify them and explain why they should be included. Should any of the minimum required elements be eliminated? If so, identify them and explain why it would be appropriate to eliminate them from the rule.

23. Should the policies and procedures requirements of paragraph (b)(1) of proposed Rule 10 be modified to provide more flexibility in how a Covered Entity implements them? If so, identify the requirements that are too prescriptive and explain why and suggest ways to make them more

flexible without undermining the objective of having Covered Entities adequately address cybersecurity risks.

24. Should the policies and procedures requirements of paragraph (b)(1) of proposed Rule 10 be modified to provide less flexibility in how a Covered Entity had to implement them? If so, identify the requirements that should be more prescriptive and explain why and suggest ways to make them more prescriptive without undermining the objective of having Covered Entities implement cybersecurity risk management policies and procedures that address their particular circumstances.

25. Should the policies and procedures requirements of paragraph (b)(1) of proposed Rule 10 be deemed to be reasonably designed if they are consistent with industry standards comprised of cybersecurity risk management practices that are widely available to cybersecurity professionals in the financial sector and issued by an authoritative body that is a U.S. governmental entity or agency, association of U.S. governmental entities or agencies, or widely recognized organization? If so, identify the standard or standards and explain why it would be appropriate to deem the policies and procedures requirements of paragraph (b)(1) of proposed Rule 10 reasonably designed if they are consistent with the standard or standards.

26. The policies and procedures requirements of paragraph (b)(1) of proposed Rule 10 would require Covered Entities to cover "information" and "information systems" as defined, respectively, in paragraphs (a)(6) and (7) of proposed Rule 10 without limitation. Should the proposed policies and procedures requirements of paragraph (b)(1) of proposed Rule 10 be modified to address a narrower set of information and information systems? If so, describe how the narrower set of information and information systems should be defined and why it would be appropriate to limit the policies and procedures requirements to this set of information and information systems. For example, should the policies and procedures requirements of paragraph (b)(1) of proposed Rule 10 be limited to information and information systems that, if compromised, would result in, or would be reasonably likely to result in, harm to the Covered Entity or others? If so, explain why. If not, explain why not. Is there another way to limit the application of the policies and procedures requirements to certain information and information systems that would not undermine the objective

²⁶² See section I.A.1. of this release (discussing, for example, how cybersecurity threats are evolving); see also Bank of England CBEST Report (stating that "[t]he threat actor community, once dominated by amateur hackers, has expanded to include a broad range of professional threat actors, all of whom are strongly motivated, organised and funded").

²⁶³ See paragraph (b)(1)(i) of proposed Rule 10. See also section II.B.1.a. of this release (discussing the assessment proposal in more detail).

²⁶⁴ See paragraph (b)(2)(ii) of proposed Rule 10.

that Covered Entities implement policies and procedures that adequately address their cybersecurity risks? If so, explain how.

27. Should the requirements of paragraph (b)(1)(i) of proposed Rule 10 relating to periodic assessments of the cybersecurity risks associated with the Covered Entity's information systems and information residing on those systems be modified? If so, explain why. If not, explain why not.

28. Should the requirements of paragraph (b)(1)(i)(A)(1) of proposed Rule 10 relating to categorizing and prioritizing cybersecurity risks based on an inventory of the components of the Covered Entity's information systems and information residing on those systems and the potential effect of a cybersecurity incident on the Covered Entity be modified? If so, explain why. If not, explain why not.

29. Should the requirements of paragraph (b)(1)(i)(A)(2) of proposed Rule 10 relating to identifying the Covered Entity's service providers that receive, maintain, or process information, or are otherwise permitted to access the Covered Entity's information systems and any of the Covered Entity's information residing on those systems, and assess the cybersecurity risks associated with the Covered Entity's use of these service providers be modified? If so, explain why. If not, explain why not. Certain Covered Entities may use data feeds from third-party providers that do not receive, maintain, or process information for the Covered Entity but that could nonetheless cause significant disruption for the Covered Entity if they were the subject of a cybersecurity incident. For example, broker-dealers may subscribe to third-party data feeds to satisfy their obligations for best execution under the federal securities laws. If a third-party provider of data feeds experienced a cybersecurity breach, it could lead to faulty market information being shared with the broker-dealer, which could in turn impact the broker-dealer's ability to operate and execute trades for its customers. Likewise, SBS Entities might rely on data from counterparties. Should the Commission require the risk assessment to include service providers that provide data feeds to Covered Entities but do not otherwise have access to the Covered Entities' information systems? If so, should the risk assessment be limited to only those third parties who provide data critical to the Covered Entity's business operations? Are there other cybersecurity risks associated with utilizing a third party who provides data

feeds that should be addressed? If so, identify the risks and explain how they could be addressed.

30. Should the requirements of paragraph (b)(1)(i)(B) of proposed Rule 10 relating to requiring written documentation of the risk assessments required by paragraph (b)(1)(i)(A) of proposed Rule 10 be modified? If so, explain why. If not, explain why not.

31. Should the requirements of paragraph (b)(1)(ii) of proposed Rule 10 relating to controls designed to minimize user-related risks and prevent unauthorized access to the Covered Entity's information systems and the information residing on those systems? If so, explain why. If not, explain why not. Should requirements of paragraph (b)(1)(ii) of proposed Rule 10 be modified to revise the requirement to include the following identified controls: (1) controls requiring standards of behavior for individuals authorized to access the Covered Entity's information systems and the information residing on those systems, such as an acceptable use policy; (2) controls identifying and authenticating individual users, including but not limited to implementing authentication measures that require users to present a combination of two or more credentials for access verification; (3) controls establishing procedures for the timely distribution, replacement, and revocation of passwords or methods of authentication; (4) controls restricting access to specific information systems of the Covered Entity or components thereof and the information residing on those systems solely to individuals requiring access to the systems and information as is necessary for them to perform their responsibilities and functions on behalf of the Covered Entity; and (5) securing remote access technologies? If so, explain why. If not, explain why not. For example, should this paragraph of the proposed rule be modified to include any additional type of controls? If so, identify the controls and explain why they should be included. Should the text of the proposed controls be modified? For example, should the control pertaining to the timely distribution, replacement, and revocation of passwords or methods of authentication use a word other than "distribution"? If so, explain why and suggest an alternative word that would be more appropriate. Would "establishment" or "setting up" be more appropriate in this context? Should this paragraph of the proposed rule be modified to eliminate any of the identified controls? If so, identify the control and explain why it should be eliminated. For example, could the

control pertaining to implementing authentication measures requiring users to present a combination of two or more credentials for access verification potentially become obsolete? If so, explain why and suggest an alternative control that could incorporate this requirement as well as other authentication controls that may develop in the future.

32. CISA has developed a catalog of cyber "bad practices" that are exceptionally risky and can increase risk to an organization's critical infrastructure.²⁶⁵ These bad practices include the use of unsupported (or end-of-life) software, use of known or default passwords and credentials, and the use of single-factor authentication. In addition, the Federal Financial Institutions Examination Council ("FFIEC") has issued guidance on authentication and access to financial institution services and systems, and suggests that the use of single-factor authentication as a control mechanism has shown to be inadequate against certain cyber threats and adverse impacts from ransomware, customer account fraud, and identity theft.²⁶⁶ Instead, the FFIEC guidance suggests the use of multi-factor authentication and other measures, such as specific authentication solutions, password controls, and access and transaction controls. Should paragraph (b)(1)(ii) of proposed Rule 10 be modified to specifically require controls that users provide multi-factor authentication before they can access an information system of the Covered Entity? If so, explain why. If not, explain why not. Would it be appropriate to require multi-factor authentication for all of the Covered Entity's information systems or for a more limited set of information systems? For example, should multi-factor authentication be required for public-facing information systems such as applications that provide users access to their accounts at the Covered Entity and not required for internal information systems used by the Covered Entity's employees? If so, explain why. If not, explain why not.

²⁶⁵ See CISA, *Bad Practices*, available at <https://www.cisa.gov/BadPractices>.

²⁶⁶ See FFIEC, *Authentication and Access to Financial Institution Services and Systems* (Aug. 2021), available at <https://www.ffiec.gov/guidance/Authentication-and-Access-to-Financial-Institution-Services-and-Systems.pdf>. See also FDIC and the Office of the Comptroller of the Currency ("OCC"), *Joint Statement on Heightened Cybersecurity Risk* (Jan. 16, 2020), available at <https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-5a.pdf> (noting that identity and access management controls include multifactor authentication to segment and safeguard access to critical systems and data on an organization's network).

Should multi-factor authentication be required regardless of whether the information system is public facing if personal, confidential, or proprietary information resides on the information system? If so, explain why. If not, explain why not. Should the rule require phishing-resistant multi-factor authentication? If so, explain why. If not, explain why not.

33. Should the requirements of paragraph (b)(1)(iii)(A) of proposed Rule 10 relating to measures designed to monitor the Covered Entity's information systems and protect the information residing on those systems from unauthorized access or use be modified? For example, should the requirements of paragraph (b)(1)(iii)(A) of proposed Rule 10 specifically require encryption of certain information residing on the Covered Entity's information systems? If so, explain why. If not, explain why not.

34. The measures discussed in paragraph (b)(1)(iii)(A) of proposed Rule 10 designed to monitor the Covered Entity's information systems and protect the information residing on those systems from unauthorized access or use would need to be based on a periodic assessment of the Covered Entity's information systems and the information that resides on the systems that takes into account: (1) the sensitivity level and importance of the information to Covered Entity's business operations; (2) whether any of the information is personal information; (3) where and how the information is accessed, stored and transmitted, including the monitoring of information in transmission; (4) the information systems' access controls and malware protection; and (5) the potential effect a cybersecurity incident involving the information could have on the Covered Entity and its customers, counterparties, members, or users, including the potential to cause a significant cybersecurity incident. Should this paragraph of the proposed rule be modified to include any additional factors that would need to be taken into account? If so, identify the factors and explain why they should be taken into account. Should this paragraph of the proposed rule be modified to eliminate any of the identified factors that should be taken into account? If so, identify the factors and explain why they should be eliminated.

35. Should the requirements of paragraph (b)(1)(iii)(A) of proposed Rule 10 relating periodic assessments of the Covered Entity's information systems and information residing of the systems be modified to specifically require periodic (e.g., semi-annual or annual

penetration tests? If so, explain why. If not, explain why not. If proposed Rule 10 should be modified to require periodic penetration tests, should the rule specify the information systems and information to be tested? If so, explain why. If not, explain why not. For example, should the penetration tests be performed on all information systems and information of the Covered Entity? Alternatively, should the penetration tests be performed: (1) on a random selection of information systems and information; (2) on a prioritized selection of the information systems and information residing on them that are most critical to the Covered Entity's functions or that maintain information that if accessed by or disclosed to persons not authorized to view it could cause the most harm to the Covered Entity or others; and/or (3) on information systems for which the Covered Entity has identified vulnerabilities pursuant to the requirements of paragraph (b)(1)(iv) of proposed Rule 10? Please explain the advantages and disadvantages of each potential approach to requiring penetration tests.

36. Should the requirements of paragraph (b)(1)(iii)(B) of proposed Rule 10 relating to the oversight of service providers that receive, maintain, or process the Covered Entity's information, or are otherwise permitted to access the Covered Entity's information systems and the information residing on those systems, pursuant to a written contract between the covered entity and the service provider, through which the service providers are required to implement and maintain appropriate measures, including the practices described in paragraphs (b)(1)(i) through (v) of proposed Rule 10, that are designed to protect the Covered Entity's information systems and information residing on those systems be modified? If so, explain why. If not, explain why not. For example, would there be practical difficulties with implementing the requirement to oversee the service providers through a written contract? If so, explain why. If not, explain why not. Are there alternative approaches to addressing the cybersecurity risk that arises when Covered Entities use service providers? If so, describe them and explain why they would be appropriate in terms of addressing this risk. For example, rather than addressing this risk through written contract, could it be addressed through policies and procedures to obtain written assurances or certifications from service providers that the service provider manages

cybersecurity risk in a manner that would be consistent with how the Covered Entity would need to manage this risk under paragraph (b) of proposed Rule 10? If so, explain why and describe the type of assurances or certifications Covered Entities could reasonably obtain to ensure that their service providers are taking appropriate measures to manage cybersecurity risk? In responding, please explain how assurances or certifications would be an appropriate alternative to written contracts in terms of addressing the cybersecurity risk caused by the use of service providers.

37. Should the requirements of paragraph (b)(1)(iv) of proposed Rule 10 relating to measures designed to detect, mitigate, and remediate any cybersecurity threats and vulnerabilities with respect to the Covered Entity's information systems and the information residing on those systems be modified? If so, explain why. If not, explain why not.

38. Should the requirements of paragraph (b)(1)(v)(A) of proposed Rule 10 relating to measures designed to detect, respond to, and recover from a cybersecurity incident be modified? If so, explain why. If not, explain why not. For example, these measures would need to include policies and procedures that are reasonably designed to ensure: (1) the continued operations of the covered entity; (2) the protection of the Covered Entity's information systems and the information residing on those systems; (3) external and internal cybersecurity incident information sharing and communications; and (4) the reporting of significant cybersecurity incidents pursuant to paragraph (c) of proposed Rule 10. Would these four specific design objectives required of the policies and procedures place the Covered Entity in a position to effectively detect, respond to, and recover from a cybersecurity incident? If so, explain why. If not, explain why not. Should this paragraph of the proposed rule be modified to include any additional design objectives for these policies and procedures? If so, identify the design objectives and explain why they should be included. For example, should the rule require policies and procedures that are designed to recover from a cybersecurity incident within a specific timeframe such as 24, 48, or 72 hours or some other period? If so, identify the recovery period and explain why it would be appropriate. Should this paragraph of the proposed rule be modified to eliminate any of the specified design objectives? If so, identify the design objectives and explain why they should be eliminated.

39. Should the requirements of paragraph (b)(1)(v)(B) of proposed Rule 10 relating to written documentation of any cybersecurity incidents be modified? If so, explain why. If not, explain why not. For example, should the written documentation requirements apply to a narrower set of incidents than those that would meet the definition of “cybersecurity incident” under proposed Rule 10? If so, describe the narrower set of incidents and explain why it would be appropriate to limit the written documentation requirements to them.

40. Should the requirements of paragraph (b)(2) of proposed Rule 10 relating to the review and assessment of the policies and procedures and a written report of the review be modified? If so, explain why. If not, explain why not. For example, this paragraph would require: (1) a review and assessment of the design and effectiveness of the cybersecurity risk management policies and procedures, including whether the policies and procedures reflect changes in cybersecurity risk over the time period covered by the review; and (2) the preparation of a written report that describes the review, the assessment, and any control tests performed, explains their results, documents any cybersecurity incident that occurred since the date of the last report, and discusses any material changes to the policies and procedures since the date of the last report. Should the review requirement be modified to provide greater flexibility based on the Covered Entity’s assessment of what it believes would be most effective in light of its cybersecurity risks? If so, explain why. If not, explain why not. Should the review, assessment, and report be required on a more frequent basis such as quarterly? If so, explain why. If not, explain why not. Should the review, assessment, and report requirement be triggered after certain events regardless of when the previous review was conducted? If so, explain why. If not, explain why not. For example, should the requirement be triggered if the Covered Entity experiences a significant cybersecurity incident or undergoes a significant business event such as a merger, acquisition, or the commencement of a new business line that relies on information systems? If so, explain why and suggest how a “significant business event” should be defined for the purposes of the review and assessment requirement. If not, explain why not. Should the rule require that persons with a minimum level of cybersecurity expertise or

experience must perform the review and assessment or that the review and assessment must be performed by a senior officer of the Covered Entity? If so, explain why. If not, explain why not. Should the rule require that the review and assessment be performed by personnel who are not involved in designing and implementing the cybersecurity policies and procedures? If so, explain why. If not, explain why not. Should the rule require that the annual report be subject to periodic third-party audits or reviews? If so, explain why. If not, explain why not. Should the Commission provide guidance to clarify how the review and report requirements of paragraph (b)(2) proposed Rule 10 interact with the requirements that SBS Entities perform assessments under 17 CFR 240.15Fk–1 or reviews under 17 CFR 250.15c3–4(c)(3)? If so, explain why. If not, explain why not.

2. Notification and Reporting of Significant Cybersecurity Incidents

a. Timing and Manner of Notification and Reporting

FSOC observed that “[s]haring timely and actionable cybersecurity information can reduce the risk that cybersecurity incidents occur and can mitigate the impacts of those that do occur.”²⁶⁷ The Commission is proposing to require that Covered Entities provide immediate notice and subsequent reports about significant cybersecurity incidents to the Commission and, in the case of certain Covered Entities, other regulators. The objective is to improve the Commission’s ability to monitor and evaluate the effects of a significant cybersecurity incident on Covered Entities and their customers, counterparties, members, registrants, or users, as well as assess the potential risks affecting financial markets more broadly.

For these reasons, proposed Rule 10 would require a Covered Entity to provide immediate written electronic notice to the Commission of a significant cybersecurity incident upon having a reasonable basis to conclude that the incident has occurred or is occurring.²⁶⁸ The Commission would

²⁶⁷ FSOC 2021 Annual Report.

²⁶⁸ See paragraph (c)(1) of proposed Rule 10. See also paragraph (a)(10) of proposed Rule 10 (defining the term “significant cybersecurity incident”). As discussed below in section II.C. of this release, Non-Covered Broker-Dealers would be subject to an identical immediate written electronic notice requirement. See paragraph (e)(2) of proposed Rule 10. If proposed Rule 10 is adopted, it is anticipated that a dedicated email address would be set up to receive the notices from Covered Entities and Non-

keep the notices nonpublic to the extent permitted by law. The notice would need to identify the Covered Entity, state that the notice is being given to alert the Commission of a significant cybersecurity incident impacting the Covered Entity, and provide the name and contact information of an employee of the Covered Entity who can provide further details about the nature and scope of the significant cybersecurity incident.

The immediate notice would need to be submitted by the Covered Entity electronically in written form (as opposed to permitting the notice to be made telephonically).²⁶⁹ The Commission is proposing a written notification requirement because of the number of Market Entities that would be subject to the requirement and because of the different types of Market Entities.²⁷⁰ A written notification would also facilitate the Commission in identifying patterns and trends across Market Entities experiencing significant cybersecurity incidents.

The notice requirement would be triggered when the Covered Entity *has a reasonable basis to conclude* that a significant cybersecurity incident has occurred or is occurring.²⁷¹ This does not mean that the Covered Entity can wait until it definitively concludes that

Covered Broker-Dealers. See, e.g., *Staff Guidance for Filing Broker-Dealer Notices, Statements and Reports*, available at <https://www.sec.gov/divisions/marketreg/bdnotices>; *Staff Statement on Submitting Notices, Statements, Applications, and Reports for Security-Based Swap Dealers and Major Security-Based Swap Participants Pursuant to the Financial Responsibility Rules (Exchange Act Rules 18a–1 through 18a–10)*, available at <https://www.sec.gov/tm/staff-statement-on-submissions>.

²⁶⁹ See paragraph (c)(1) of proposed Rule 10. But see 17 CFR 242.1002(b)(1) (requiring an SCI entity to provide the Commission with immediate notice after having a reasonable basis to conclude that an SCI event has occurred without specifying that the notice be written); OCC, Federal Reserve Board, FDIC, *Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers*, 86 FR 66424 (Nov. 23, 2021) (requiring a banking organization to provide notice to a designated point of contact of a computer-security incident through telephone, email, or similar methods).

²⁷⁰ Non-Covered Broker-Dealers also would be subject to an immediate written electronic notice requirement under paragraph (e)(2) of proposed Rule 10 and, therefore, the Commission potentially could receive notices from all types of Market Entities. As discussed in section V.C. of this release, it is estimated that 1,989 Market Entities would be Covered Entities and 1,969 broker-dealers would be Non-Covered Entities resulting in a 3,958 total Market Entities. This is a far larger number of entities than the 47 entities that currently are SCI entities.

²⁷¹ The notice requirement for Non-Covered Broker-Dealers also would be triggered when the broker-dealer has a reasonable basis to conclude that a significant cybersecurity incident has occurred or is occurring. See paragraph (e)(2) of proposed Rule 10.

a significant cybersecurity incident has occurred or is occurring. In the early stages of discovering the existence of a cybersecurity incident, it may not be possible for the Covered Entity to conclude definitively that it is a *significant* cybersecurity incident. For example, the Covered Entity may need to assess which information systems have been subject to the cybersecurity incident and the impact that the incident has had on those systems before definitively concluding that it is a significant cybersecurity incident.²⁷² The objective of the notification requirement is to alert the Commission staff as soon as the Covered Entity detects the existence of a cybersecurity incident that it has a reasonable basis to conclude is a significant cybersecurity incident and not to wait until the Covered Entity definitively concludes it is a significant cybersecurity incident. This would provide the Commission staff with the ability to begin to assess the situation at an earlier stage of the cybersecurity incident.

This proposed immediate written notification requirement is modelled on other notification requirements that apply to broker-dealers and SBSDs pursuant to other Exchange Act rules. Under these existing requirements, broker-dealers and certain SBSDs must provide the Commission with same-day written notification if they undergo certain adverse events, including falling below their minimum net capital requirements or failing to make and keep current required books and records.²⁷³ The objective of these requirements is to provide the Commission staff with the opportunity to respond when a broker-dealer or SBSD is in financial or operational difficulty.²⁷⁴ Similarly, the written notification requirements of proposed Rule 10 are designed to provide the Commission staff with the opportunity to begin assessing the situation promptly when a Covered Entity is experiencing a significant cybersecurity incident by, for example, assessing the

Covered Entity's operating status and engaging in discussions with the Covered Entity to understand better what steps it is taking to protect its customers, counterparties, members, registrants, or users. In addition, a Covered Entity that is a broker-dealer would need to provide the written notice to its examining authority, and a transfer agent would need to provide the written notice to its ARA.²⁷⁵ The objective is to notify other supervisory authorities to allow them the opportunity to respond to the significant cybersecurity incident impacting the Covered Entity.

As discussed above, the immediate written electronic notice is designed to alert the Commission on a confidential basis to the existence of a significant cybersecurity incident impacting a Covered Entity so the Commission staff can begin to assess the event. It is not intended as a means to report written information about the significant cybersecurity incident. Therefore, in addition to the immediate written electronic notice, a Covered Entity would be required to report detailed information about the significant cybersecurity incident by filing, on a confidential basis, Part I of proposed Form SCIR with the Commission through the Electronic Data Gathering, Analysis, and Retrieval System ("EDGAR" or "EDGAR system").²⁷⁶ Because of the sensitive nature of the information and the fact that threat actors could potentially use it to cause more harm, the Commission would not make the filings available to the public to the extent permitted by law.

As with the notice, the requirement to file Part I of proposed Form SCIR would be triggered when the Covered Entity *has a reasonable basis to conclude* that a significant cybersecurity incident has occurred or is occurring. Therefore, the notification and reporting requirements would be triggered at the same time. However, in order to provide the Covered Entity time to gather the information that would be elicited by Part I of proposed Form SCIR, the Covered Entity would need to file the

form promptly, but no later than 48 hours, upon having a reasonable basis to conclude that a significant cybersecurity incident has occurred or is occurring.

Proposed Rule 10 also would require the Covered Entity to file an amended Part I of proposed Form SCIR with updated information about the significant cybersecurity incident in four circumstances.²⁷⁷ In each case, the amended Part I of proposed Form SCIR would need to be filed promptly, but no later than 48 hours, after the update requirement is triggered. First, the Covered Entity would need to file an amended Part I of proposed Form SCIR if any information previously reported to the Commission on the form pertaining to the significant cybersecurity incident becomes materially inaccurate.²⁷⁸ Second, the Covered Entity would need to file an amended Part I of proposed Form SCIR if any new material information pertaining to the significant cybersecurity incident previously reported to the Commission on the form is discovered.²⁷⁹ The Commission staff generally would use the information reported on Part I of proposed Form SCIR to assess the operating status of the Covered Entity and assess the impact that the significant cybersecurity incident could have on other participants in the U.S. securities markets. The requirement to file an amended Part I of proposed Form SCIR under the first and second circumstances is designed to ensure the Commission and Commission staff have reasonably accurate and complete information when undertaking these activities.

Third, the Covered Entity would need to file an amended Part I of proposed Form SCIR after the significant cybersecurity incident is resolved.²⁸⁰ A significant cybersecurity incident impacting a Covered Entity would be resolved when the situation no longer meets the definition of "significant cybersecurity incident."²⁸¹ The resolution of a significant cybersecurity incident would be a material development in the situation and, therefore, would be a reporting trigger under proposed Rule 10.

²⁷² See paragraph (a)(2) of proposed Rule 10 (defining "cybersecurity incident" to mean an unauthorized occurrence on or conducted through a Market Entity's information systems that jeopardizes the confidentiality, integrity, or availability of the information systems or any information residing on those systems).

²⁷³ See 17 CFR 240.17a-11 (notification rule for broker-dealers); 17 CFR 240.18a-8 (notification rule for SBS Entities).

²⁷⁴ See *Recordkeeping and Reporting Requirements for Security-Based Swap Dealers, Major Security-Based Swap Participants, and Broker-Dealers; Capital Rule for Certain Security-Based Swap Dealers*, Exchange Act Release No. 71958 (Apr. 17, 2014) [79 FR 25194, 25247 (May 2, 2014)] ("SBS Entity Recordkeeping and Reporting Proposing Release").

²⁷⁵ See paragraphs (c)(1)(i) and (ii) of proposed Rule 10. Non-Covered Broker-Dealers also would be required to provide the written notice to their examining authority. See paragraph (e)(2) of proposed Rule 10.

²⁷⁶ See paragraph (c)(2) of proposed Rule 10. As discussed below, Part II of proposed Form SCIR would be used by Covered Entities to make public disclosures about the cybersecurity risks they face and the significant cybersecurity incidents they experienced during the current or previous calendar year. See sections II.B.2. and II.B.4. of this release (discussing these proposed requirements). Non-Covered Broker-Dealers would not be subject to the requirements to file Part I and Part II of proposed Form SCIR.

²⁷⁷ See paragraphs (c)(2)(ii)(A) through (D) of proposed Rule 10.

²⁷⁸ See paragraph (c)(2)(ii)(A) of proposed Rule 10.

²⁷⁹ See paragraph (c)(2)(ii)(B) of proposed Rule 10.

²⁸⁰ See paragraph (c)(2)(ii)(C) of proposed Rule 10.

²⁸¹ See paragraph (a)(10) of proposed Rule 10 (defining the term "significant cybersecurity incident").

Finally, if the Covered Entity conducted an internal investigation pertaining to the significant cybersecurity incident, it would need to file an amended Part I of proposed Form SCIR after the investigation is closed.²⁸² This would be an investigation of the significant cybersecurity incident that seeks to determine the cause of the incident or to examine whether there was a failure to adhere to the Covered Entity's policies and procedures to address cybersecurity risk or whether those policies and procedures are effective. An internal investigation could be conducted by the Covered Entity's own personnel (e.g., internal auditors) or by external consultants hired by the Covered Entity. The closure of an internal investigation would be a reporting trigger under proposed Rule 10 because it could yield material new information about the incident that had not been reported in a previously filed Part I of proposed Form SCIR.

As with the immediate written electronic notice, a Covered Broker-Dealer would need to promptly transmit a copy of each Part I of proposed Form SCIR it files with the Commission to its examining authority, and a transfer agent would need to promptly transmit a copy of each Part I of proposed Form SCIR it files with the Commission to its ARA.²⁸³ The objective is to provide these other supervisory authorities with the same information about the significant cybersecurity incident that the Commission receives.

In this regard, the reporting requirements under proposed Rule 10 would provide the Commission and its staff with information to understand better the nature and extent of a particular significant cybersecurity incident and the efficacy of the Covered Entity's response to mitigate the disruption and harm caused by the incident. The Commission staff could use the reports to focus on the Covered Entity's operating status and to facilitate their outreach to, and discussions with, personnel at the Covered Entity who are addressing the significant cybersecurity incident. For example, certain information provided in a report may be sufficient to address any questions the staff has about the incident; and in other instances staff may want to ask follow-up questions to get a better understanding of the matter. In addition, the reporting would provide the staff with a view into the Covered Entity's understanding of the scope and

impact of the significant cybersecurity incident. All of this information would be used by the Commission and its staff in assessing the impact of the significant cybersecurity incident on the Covered Entity.

The information provided to the Commission under the proposed reporting requirements also would be used to assess the potential cybersecurity risks affecting U.S. securities markets more broadly. This information could be useful in assessing other and future significant cybersecurity incidents. For example, these reports could assist the Commission in identifying patterns and trends across Covered Entities, including widespread cybersecurity incidents affecting multiple Covered Entities at the same time. Further, the reports could be used to evaluate the effectiveness of various approaches to respond to and recover from a significant cybersecurity incident.

b. Part I of Proposed Form SCIR

Proposed Rule 10 would require a Covered Entity to report information about a significant cybersecurity incident confidentially on Part I of proposed Form SCIR.²⁸⁴ The form would elicit certain information about the significant cybersecurity incident through check boxes, date fields, and narrative fields. Covered Entities would file Part I of proposed Form SCIR electronically with the Commission using the EDGAR system in accordance with the EDGAR Filer Manual, as defined in Rule 11 of Regulation S–T,²⁸⁵ and in accordance with the requirements of Regulation S–T.²⁸⁶

A Covered Entity would need to indicate on Part I of proposed Form SCIR whether the form is being filed with respect to a significant cybersecurity incident as an initial report, amended report, or final amended report by checking the appropriate box. As discussed above, proposed Rule 10 would require a Covered Entity to file Part I of proposed Form SCIR upon having a reasonable basis to conclude that a significant cybersecurity incident has occurred or is occurring.²⁸⁷ This would be the initial Part I of proposed Form SCIR with respect to the significant cybersecurity

incident.²⁸⁸ Thereafter, a Covered Entity would be required to file an amended Part I of proposed Form SCIR with respect to the significant cybersecurity incident after: (1) any information previously reported to the Commission on Part I of proposed Form SCIR pertaining to the significant cybersecurity incident becomes materially inaccurate; (2) any new material information pertaining to the significant cybersecurity incident previously reported to the Commission on Part I of proposed Form SCIR is discovered; (3) the significant cybersecurity incident is resolved; or (4) an internal investigation pertaining to a significant cybersecurity incident is closed.²⁸⁹ If a Covered Entity checks the box indicating that the filing is a final Part I of proposed Form SCIR, the firm also would need to check the appropriate box to indicate why a final form was being filed: either the significant cybersecurity incident was resolved or an internal investigation pertaining to the incident was closed.

Part I of proposed Form SCIR would elicit information about the Covered Entity that would be used to identify the filer.²⁹⁰ In particular, the Covered Entity would need to provide its full legal name and business name (if different from its legal name), tax identification number, unique identification code ("UIC") (if the filer has a UIC), central index key ("CIK number"),²⁹¹ and main address.²⁹² The instructions to proposed Form SCIR (which would be applicable to Parts I and II) would provide that a UIC is an identification number that has been issued by an internationally recognized standards-setting system ("IRSS") that has been recognized by the Commission pursuant to Rule 903(a) of Regulation SBSR.²⁹³ Currently, the Commission has recognized only the Global Legal Entity Identifier Foundation ("GLEIF")—which is responsible for overseeing the Global Legal Entity Identifier System ("GLEIS")—as an IRSS.²⁹⁴ Part I of

²⁸⁸ See Instruction B.1. of proposed Form SCIR.

²⁸⁹ See paragraphs (c)(2)(ii)(A) through (D) of proposed Rule 10.

²⁹⁰ See Line Items 1.A. through 1.E. of Part I of proposed Form SCIR.

²⁹¹ A CIK number is used on the Commission's computer systems to identify persons who have filed disclosures with the Commission.

²⁹² See Line Items 1.A. through 1.C. of Part I of proposed Form SCIR.

²⁹³ See Instruction A.5.g. of proposed Form SCIR. See also, e.g., Form SBSE available at <https://www.sec.gov/files/form-sbse.pdf> (providing a similar definition of UIC).

²⁹⁴ See Regulation SBSR—Reporting and Dissemination of Security-Based Swap Information, Exchange Act Release No. 74244 (Feb. 11, 2015), 80 FR 14563, 14632 (Mar. 19, 2015) ("Regulation SBSR Release"). LEIs are unique alphanumeric codes that

²⁸² See paragraph (c)(2)(ii)(D) of proposed Rule 10.

²⁸³ See paragraphs (c)(2)(iii)(A) and (B) of proposed Rule 10.

²⁸⁴ See paragraph (c)(2) of proposed Rule 10.

²⁸⁵ See 17 CFR 232.11.

²⁸⁶ See paragraphs (c)(2)(i) and (ii) of proposed Rule 10. As discussed below in section II.B.4. of this release, the Covered Entity would need to file Part I of proposed Form SCIR using a structured data language.

²⁸⁷ See paragraph (c)(2)(i) of proposed Rule 10. See also section II.B.2.a. of this release (discussing the proposed filing requirements in more detail).

proposed Form SCIR also would elicit the name, phone number, and email address of the contact employee of the Covered Entity.²⁹⁵ The contact employee would need to be an individual authorized by the Covered Entity to provide the Commission with information about the significant cybersecurity incident (*i.e.*, information the individual can provide directly) and make information about the incident available to the Commission (*e.g.*, information the individual can provide by, for example, making other employees of the Covered Entity available to answer questions of the Commission staff).²⁹⁶ The Covered Entity also would need to indicate the type of Market Entity it is by checking the appropriate box or boxes.²⁹⁷ For example, if the Covered Entity is dually registered as a broker-dealer and SBSB, it would need to check the box for each of those entity types.

Page 1 of Part I of proposed Form SCIR also would contain fields for the individual executing the form to sign and date the form. By signing the form, the individual would: (1) certify that the form was executed on behalf of, and with the authority of, the Covered Entity; (2) represent individually, and on behalf of the Covered Entity, that the information and statements contained in the form are current, true and complete; and (3) represent individually, and on behalf of the Covered Entity, that to the extent any information previously submitted is not amended such information is current, true, and complete. The form of the certification is designed to ensure that the Covered Entity, through the individual executing the form, provides information that the Commission and Commission staff can rely on to evaluate the operating status of the Covered Entity, assess the impact the significant cybersecurity incident may have on other participants in the

identify legal entities in financial transactions in international markets. See Financial Stability Board (“FSB”), *Options to Improve Adoption of the LEI, in Particular for Use in Cross-Border Payments* (July 7, 2022). Information associated with the LEI, which is a globally-recognized digital identifier that is not specific to the Commission, includes the “official name of the legal entity as recorded in the official registers[,]” the entity’s address, country of incorporation, and the “legal form of the entity.” *Id.* Accordingly, in proposing to require each Covered Entity to provide its UIC if it has a UIC, the Commission is proposing to require each Covered Entity identify itself with an LEI if it has an LEI.

²⁹⁵ See Line Item 1.D. of Part I of proposed Form SCIR.

²⁹⁶ See Instruction B.4. of proposed Form SCIR.

²⁹⁷ See Line Item 1.E. of Part I of proposed Form SCIR (setting forth check boxes to indicate whether the Covered Entity is a broker-dealer, clearing agency, MSBSP, the MRSB, a national securities association, a national securities exchange, SBSB, SBSDR, or transfer agent).

U.S. securities markets, and formulate an appropriate response to the incident.

Line Items 2 through 14 of Part I of proposed Form SCIR would elicit information about the significant cybersecurity incident and the Covered Entity’s response to the incident. After discovering the existence of a significant cybersecurity incident, a Covered Entity may need time to determine the scope and impact of the incident in order to provide meaningful responses to these questions. For example, the Covered Entity may be working diligently to investigate and resolve the significant cybersecurity incident at the same time it would be required to complete and file Part I of proposed Form SCIR. The Covered Entity’s priorities in the early stages after detecting the significant cybersecurity incident may be to devote its staff resources to mitigating the harms caused by the incident or that could be caused by the incident if necessary corrective actions are not promptly implemented. Moreover, during this period, the Covered Entity may not have a complete understanding of the cause of the significant cybersecurity incident, all the information systems impacted by the incident, the harm caused by the incident, or how to best resolve and recover from the incident (among other relevant information).

Therefore, the first form filed with respect to a given significant cybersecurity incident should include information that is known to the Covered Entity at the time of filing and not include speculative information. If information is unknown at the time of filing, the Covered Entity should indicate that on the form. Understanding the aspects of the significant cybersecurity incident that are not yet known would inform the Commission’s assessment. The process of filing an amended Part I of proposed Form SCIR is designed to update earlier filings as information becomes known to the Covered Entity. In particular, proposed Rule 10 would require the Covered Entity to file an amended Part I of proposed Form SCIR if information reported on a previously filed form pertaining to the significant cybersecurity incident becomes materially incomplete because new information is discovered.²⁹⁸ Therefore, as the Covered Entity reasonably concludes that additional information about the significant cybersecurity incident is necessary to make its filing not materially inaccurate, it would need to file amended forms. In this way, the

²⁹⁸ See paragraph (c)(2)(ii)(B) of proposed Rule 10.

reporting requirements of proposed Rule 10 are designed to provide the Commission and Commission staff with current known information and provide a means for the Covered Entity to report information as it becomes known.

This does not mean that the Covered Entity can refrain from providing known information in Part I of proposed Form SCIR. As discussed above, the Covered Entity must certify through the individual executing the form that the information and statements in the form are current, true, and complete, among other things. A failure to provide current, true, and complete information that is known to the Covered Entity would be inconsistent with this required certification. In addition, failing to investigate the significant cybersecurity incident would be inconsistent with the policies and procedures required by proposed Rule 10. As discussed above, the cybersecurity incident response and recovery policies and procedures that would be required by proposed Rule 10 would need to include policies and procedures that are reasonably designed to ensure the reporting of significant cybersecurity incidents as required by the rule.²⁹⁹ The failure to diligently investigate the significant cybersecurity incident could indicate that the Covered Entity’s incident response and recovery policies and procedures are not reasonably designed or are not being enforced by the Covered Entity as required by proposed Rule 10.³⁰⁰ Moreover, reasonably designed policies and procedures to detect, respond to, and recover from a cybersecurity incident, as required by proposed Rule 10 generally should require diligent investigation of the significant cybersecurity incident.³⁰¹ Further, diligently investigating the significant cybersecurity incident would be in the interest of the Covered Entity as it could lead to a quicker resolution of the incident by revealing—for example—its cause and impact.

In terms of the information about the significant cybersecurity incident elicited in Part I of proposed Form SCIR, the Covered Entity first would be required to provide the approximate

²⁹⁹ See paragraph (b)(1)(v)(A)(4) of proposed Rule 10. See also section II.B.1.e. of this release (discussing these proposed required policies and procedures in more detail).

³⁰⁰ See paragraph (b)(1) of proposed Rule 10 (requiring that the Covered Entity establish, maintain, and enforce written policies and procedures that are reasonably designed to address the covered entity’s cybersecurity risks).

³⁰¹ See paragraph (b)(1)(v)(A) of proposed Rule 10. See also section II.B.1.e. of this release (discussing these proposed required policies and procedures in more detail).

date that it discovered the significant cybersecurity incident.³⁰² As discussed above, a Covered Entity would be required to provide the Commission with immediate written electronic notice of a significant cybersecurity incident upon having a reasonable basis to conclude that the incident has occurred or is occurring.³⁰³ This can be based on, for example, the Covered Entity reviewing or receiving a record, alert, log, or notice about the incident. In addition, reaching this conclusion would trigger the requirement to file promptly (but within 48 hours) an initial Part I of proposed Form SCIR with the Commission to first report the significant cybersecurity incident using the form.³⁰⁴ The date that would need to be reported on proposed Part I of Form SCIR is the date the Covered Entity has a reasonable basis to conclude that the incident has occurred or is occurring.³⁰⁵

Line Item 3 of Part I of proposed Form SCIR would elicit information about the approximate duration of the significant cybersecurity incident.³⁰⁶ First, the Covered Entity would need to indicate whether the significant cybersecurity incident is ongoing.³⁰⁷ The form would provide the option of answering yes, no, or unknown. Second, the Covered Entity would need to provide the approximate start date of the cybersecurity incident or indicate that it does not know the start date.³⁰⁸ The start date may be well before the date the Covered Entity discovered the significant cybersecurity incident. Therefore, the start date of the incident reported on Line Item 3 may be different than the discovery date reported on Line Item 2. Third, the Covered Entity would need to provide the approximate date the significant cybersecurity incident is resolved.³⁰⁹ This would be the date the Covered Entity was no longer undergoing a significant cybersecurity incident.³¹⁰ As discussed above, the resolution of the

significant cybersecurity incident triggers the requirement to file an amended Part I of proposed Form SCIR under proposed Rule 10.³¹¹

Line Item 4 of Part I of proposed Form SCIR would require the Covered Entity to indicate whether an internal investigation pertaining to the significant cybersecurity incident was being conducted. An “internal investigation” would be defined as a formal investigation of the significant cybersecurity incident by internal personnel of the Covered Entity or external personnel hired by the Covered Entity that seeks to determine any of the following: the cause of the significant cybersecurity incident; whether there was a failure to adhere to the Covered Entity’s policies and procedures to address cybersecurity risk; or whether the Covered Entity’s policies and procedures to address cybersecurity are effective.³¹² If an internal investigation is conducted, the Covered Entity also would need to provide the date the investigation was closed. As discussed above, the closure of an internal investigation pertaining to the significant cybersecurity incident triggers the requirement to file an amended Part I of Form SCIR under proposed Rule 10.³¹³

Line Item 5 of Part I of proposed Form SCIR would require the Covered Entity to indicate whether a law enforcement or government agency (other than the Commission) had been notified of the significant cybersecurity incident.³¹⁴ If so, the Covered Entity would need to identify each law enforcement or government agency. The Commission and Commission staff could use this information to coordinate with other law enforcement and government agencies if needed both to assess the incident and to share information as appropriate to understand the impact of the incident better.

Line Item 6 of Part I of proposed Form SCIR would require the Covered Entity to describe the nature and scope of the significant cybersecurity incident, including the information systems affected by the incident and any effect on the Covered Entity’s critical operations.³¹⁵ This item would enable the Commission to obtain information

about the incident to understand better how it is impacting the Covered Entity’s operating status and whether the Covered Entity can continue to provide services to its customers, counterparties, members, registrants, or users. This would include understanding which services and systems have been impacted and whether the incident was the result of a cybersecurity incident that occurred at a service provider.

Line Item 7 of Part I of proposed Form SCIR would require the Covered Entity to indicate whether the threat actor(s) causing the significant cybersecurity incident has been identified.³¹⁶ If so, the Covered Entity would be required to identify the threat actor(s). In addition, the Covered Entity would need to indicate in Line Item 7 whether there has been communication(s) from or with the threat actor(s) that caused or claims to have caused the significant cybersecurity incident.³¹⁷ The Covered Entity would need to answer the question even if the threat actor(s) has not been identified. If there had been communications, the Covered Entity would need to describe them. This information would help the Commission staff to assess whether the same threat actor(s) had sought to access information systems of other Commission registrants and to warn other registrants (as appropriate) about the threat posed by the actor(s). It also could help in developing measures to protect against the risk to Commission registrants posed by the threat actor. In addition, the information would help the Commission assess the impact on the Covered Entity experiencing the significant cybersecurity incident to the extent other Commission registrants has been attacked by the same threat actor(s) using similar tactics, techniques, and procedures.

Line Item 8 of Part I of proposed Form SCIR would require the Covered Entity to describe the actions taken or planned to respond to and recover from the significant cybersecurity incident.³¹⁸ The objective is to obtain information to assess the Covered Entity’s operating status, including its critical operations. This information also could assist the Commission and Commission staff in considering if the response measures are effective or ineffective in addressing the Covered Entity’s significant cybersecurity incident.

Line Item 9 of Part I of proposed Form SCIR would require the Covered Entity

³⁰² See Line Item 2 of Part I of proposed Form SCIR.

³⁰³ See paragraph (c)(1) of proposed Rule 10. See also section II.B.2.a. of this release (discussing the proposed notification requirement in more detail).

³⁰⁴ See paragraph (c)(2)(i) of proposed Rule 10. See also section II.B.2.a. of this release (discussing the proposed reporting trigger in more detail).

³⁰⁵ See Instruction B.5.a. of proposed Form SCIR.

³⁰⁶ See Line Items 3.A. through 3.C. of Part I of proposed Form SCIR.

³⁰⁷ See Line Item 3.A. of Part I of proposed Form SCIR.

³⁰⁸ See Line Item 3.B. of Part I of proposed Form SCIR.

³⁰⁹ See Line Item 3.C. of Part I of proposed Form SCIR.

³¹⁰ See Instruction B.5.b. of proposed Form SCIR. See also paragraph (a)(10) of proposed Rule 10 (defining the term “significant cybersecurity incident”).

³¹¹ See paragraph (c)(2)(ii)(C) of proposed Rule 10. See section II.B.2.a. of this release (discussing the notification requirements in more detail).

³¹² See Instruction A.5.d. of proposed Form SCIR.

³¹³ See paragraph (c)(2)(ii)(D) of proposed Rule 10. See also section II.B.2.a. of this release (discussing the notification requirement in more detail).

³¹⁴ See Line Item 5 of Part I of proposed Form SCIR.

³¹⁵ See Line Item 6 of Part I of proposed Form SCIR.

³¹⁶ See Line Item 7.A. of Part I of proposed Form SCIR.

³¹⁷ See Line Item 7.B. of Part I of proposed Form SCIR.

³¹⁸ See Line Item 8 of Part I of proposed Form SCIR.

to indicate whether any data was stolen, altered, or accessed or used for any other unauthorized purpose.³¹⁹ The Covered Entity would have the option of checking yes, no, or unknown. If yes, the Covered Entity would need to describe the nature and scope of the data. This information would help the Commission and its staff understand the potential harm to the Covered Entity and its customers, counterparties, members, registrants, or users that could result from the compromise of the data. It also would provide insight into how the significant cybersecurity incident could impact other Market Entities.

Line Item 10 of Part I of proposed Form SCIR would require the Covered Entity to indicate whether any personal information was lost, stolen, modified, deleted, destroyed, or accessed without authorization as a result of the significant cybersecurity incident.³²⁰ The Covered Entity would have the option of checking yes, no, or unknown. If yes, the Covered Entity would need to describe the nature and scope of the information. Additionally, if the Covered Entity answered yes, it would need to indicate whether notification has been provided to persons whose personal information was lost, stolen, damaged, or accessed without authorization.³²¹ If the answer is no, the Covered Entity would need to indicate whether this notification is planned.³²² For the purposes of proposed Form SCIR, the term “personal information” would have the same meaning as that term is defined in proposed Rule 10.³²³ The compromise of personal information can have severe consequences on the persons to whom the information relates. For example, it potentially can be used to steal their identities or access their accounts at financial institutions to steal assets held in those accounts. Consequently, this information would help the Commission assess the extent to which the significant cybersecurity incident

has created this risk and the potential harm that could result from the compromise of personal data.

Line Item 11 of Part I of proposed Form SCIR would require the Covered Entity to indicate whether any of its assets were lost or stolen as a result of the significant cybersecurity incident.³²⁴ The Covered Entity would have the option of checking yes, no, or unknown. If yes, the Covered Entity would need to describe the types of assets that were lost or stolen and include an approximate estimate of their value, if known. This question is not limited to particular types of assets and, therefore, the Covered Entity would need to respond affirmatively if, among other types of assets, financial assets such as cash and securities were lost or stolen or intellectual property was lost or stolen. The loss or theft of the Covered Entity’s assets could potentially cause the entity to fail financially or put a strain on its liquidity. Further, to the extent counterparties become aware of the loss or theft, it could cause them to withdraw assets from the entity or stop transacting with the entity further straining its financial condition. Consequently, the objective is to understand whether the significant cybersecurity incident has created this risk and whether there may be other spillover effects or consequences to the U.S. securities markets.

Line Item 12 of Part I of proposed Form SCIR would require the Covered Entity to indicate whether any assets of the Covered Entity’s customers, counterparties, clients, members, registrants, or users were lost or stolen as a result of the significant cybersecurity incident.³²⁵ The Covered Entity would have the option of checking yes, no, or unknown. If yes, the Covered Entity would need to describe the types of assets that were lost or stolen and include an approximate estimate of their value, if known. Additionally, if the Covered Entity answered yes, it would need to indicate whether notification has been provided to persons whose assets were lost or stolen.³²⁶ If the answer is no, the Covered Entity would need to indicate whether this notification is planned.³²⁷

Certain types of Covered Entities hold assets belonging to other persons or maintain ownership records of the

assets of other persons.³²⁸ For example, certain broker-dealers maintain custody of securities and cash for other persons and clearing agencies hold clearing deposits of their members. A significant cybersecurity incident impacting a Covered Entity that results in the loss or theft of assets can cause severe financial hardship to the owners of those assets. It also can impact the financial condition of the Covered Entity if it is liable for the loss or theft. Consequently, the objective is to understand whether the significant cybersecurity incident has created this risk.

As discussed in more detail below, proposed Rule 10 would require a Covered Entity to make a public disclosure that generally describes each significant cybersecurity incident that has occurred during the current or previous calendar year and promptly update this disclosure after the occurrence of a new significant cybersecurity incident or when information about a previously disclosed significant cybersecurity incident materially changes.³²⁹ The Covered Entity would be required to make the disclosure on the Covered Entity’s business internet website and by filing Part II of proposed Form SCIR through the EDGAR system.³³⁰ In addition, if the Covered Entity is a carrying or introducing broker-dealer, it would need to make the disclosure to its customers using the same means that a customer elects to receive account statements.³³¹

Line Item 13 of Part I of proposed Form SCIR would require the Covered Entity to indicate whether the significant cybersecurity incident has been disclosed pursuant to the requirements of proposed Rule 10.³³² The Covered Entity also would need to indicate whether it made the required disclosures of Part II of proposed Form SCIR on its website and through EDGAR and, if it had made the disclosure, it would need to indicate the date of the disclosure.³³³ A Covered Entity that is a carrying or introducing broker-dealer would need to indicate separately

³²⁸ See Section I.A.2. of this release (discussing the functions of Market Entities).

³²⁹ See paragraph (d)(1)(ii) of proposed Rule 10. See also sections II.B.3. and II.B.4. of this release (discussing these proposed disclosure requirements in more detail).

³³⁰ See paragraphs (d)(2)(i) and (ii) of proposed Rule 10.

³³¹ See paragraph (d)(3) of proposed Rule 10. See section II.B.3.b. of this release (discussing the broker-dealer disclosure requirement in more detail).

³³² See Line Items 13.A. through C. of proposed Form SCIR.

³³³ See Line Items 13.A. through B. of proposed Part I of Form SCIR.

³¹⁹ See Line Item 9 of Part I of proposed Form SCIR.

³²⁰ See Line Item 10.A. of Part I of proposed Form SCIR.

³²¹ See Line Item 10.B.i. of Part I of proposed Form SCIR.

³²² See Line Item 10.B.ii. of Part I of proposed Form SCIR.

³²³ See Instruction A.5.e. of proposed Form SCIR. See also paragraph (a)(9) of proposed Rule 10 (defining “personal information” to mean any information that can be used, alone or in conjunction with any other information, to identify a person, such as name, date of birth, place of birth, telephone number, street address, mother’s maiden name, government passport number, Social Security number, driver’s license number, electronic mail address, account number, account password, biometric records, or other non-public authentication information).

³²⁴ See Line Item 11 of Part I of proposed Form SCIR.

³²⁵ See Line Item 12.A. Part I of proposed Form SCIR.

³²⁶ See Line Item 11.B.i. of Part I of proposed Form SCIR.

³²⁷ See Line Item 12.B.ii. of Part I of proposed Form SCIR.

whether it made the required disclosure of Part II of proposed Form SCIR to its customers.³³⁴ The Covered Entity would not need to indicate a date for the customer disclosure because it could be made in a number of ways (e.g., by email or mail) and that process could span a number of days. If the Covered Entity has not disclosed the significant cybersecurity incident as required by proposed Rule 10, it would need to explain why. The requirement to report this information is designed to promote compliance with the disclosure requirements of proposed Rule 10.

Line Item 14 of Part I of proposed Form SCIR would elicit information about any insurance coverage the Covered Entity may have with respect to the significant cybersecurity incident.³³⁵ First, the Covered Entity would need to indicate whether the significant cybersecurity incident is covered by an insurance policy of the Covered Entity.³³⁶ The Covered Entity would have the option of checking yes, no, or unknown. If yes, the Covered Entity would need to indicate whether the insurance company has been contacted. The existence of insurance coverage to cover losses could be relevant to Commission staff in assessing the potential magnitude of harm to the Covered Entity's customers, counterparties, members, registrants, or users and to the Covered Entity's financial condition. For example, the existence of insurance coverage, to the extent the significant cybersecurity incident is covered by the policy, could indicate a greater possibility that the Covered Entity and/or any of its customers, counterparties, members, registrants, or users affected by the incident are made whole.

Finally, Line Item 15 of Part I of proposed Form SCIR would permit the Covered Entity to include in the form any additional information the entity would want the Commission and Commission staff to know as well as provide any comments about the information included in the report.³³⁷

c. Request for Comment

The Commission requests comment on all aspects of the proposed requirements to report significant cybersecurity incidents on Part I of proposed Form SCIR. In addition, the Commission is requesting comment on

the following specific aspects of the proposals:

41. Should paragraph (c)(1) of proposed Rule 10 be modified to revise the immediate notification requirement? For example, should the requirement permit the notice to be made by telephone or email? If so, explain why. If not, explain why not. If telephone or email notice is permitted, should the rule specify the Commission staff, Division, or Office to phone or email?

42. Should paragraph (c)(1) of proposed Rule 10 be modified to revise the requirement to provide immediate written electronic notice to specify how the notice must be transmitted to the Commission? For example, should the rule specify an email address or other type of electronic portal to be used to transmit the notice? If so, explain why. If not, explain why not. Should the rule be modified to require that the notice be transmitted to the Commission through the EDGAR system? If so, explain why. If not, explain why not. Should the rule be modified to require that the notice be transmitted to the Commission through the EDGAR system using a structured data language other than custom XML format?

43. Should paragraph (c)(1) of proposed Rule 10 be modified to revise the requirement to provide immediate written electronic notice to require the notice to be provided within a specific timeframe such as on the same day the requirement was triggered or within 24 hours? If so, explain why. If not, explain why not.

44. Should paragraph (c)(1) of proposed Rule 10 be modified to revise the trigger for the immediate notification and reporting requirements? If so, explain why. If not, explain why not. For example, should the trigger be when the Covered Entity "detects" a significant cybersecurity incident (rather than when it has a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring)? If so, explain why. If not, explain why not. For example, would a detection standard be a less subjective standard? If so, explain why. If not, explain why not. Is there another trigger standard that would be more appropriate? If so, identify it and explain why it would be more appropriate.

45. If the immediate notification requirement of paragraph (c)(1) is adopted as proposed, it is anticipated that a dedicated email address would be established to receive these notices. Are there other methods the Commission should use for receiving these notices? If so, identify them and explain why they would be more appropriate than

email. For example, should the notices be received through the EDGAR system? If so, explain why. If not, explain why not.

46. Should paragraph (c)(2) of proposed Rule 10 be modified to revise the reporting requirements to incorporate the cybersecurity reporting program that CISA will implement under recently adopted legislation ("CISA Reporting Program") to the extent it will be applicable to Covered Entities?³³⁸ If so, explain why and suggest modifications to the proposed reporting requirements for Covered Entities to incorporate the CISA Reporting Program. For example, if a Covered Entity would be required to file a report under the CISA Reporting Program, should that report satisfy the obligations to report to the Commission a significant cybersecurity incident under paragraph (c) of proposed Rule 10? If so, explain why. If not, explain why not.

47. Should paragraph (c)(2) of proposed Rule 10 be modified to revise the timeframe for filing an initial Part I of proposed Form SCIR? If so, explain why. If not, explain why not. For example, should the reporting requirements be revised to permit Covered Entities more than 48 hours to file an initial Part I of proposed Form SCIR with the Commission? If yes, explain how long they should have to file the initial Part I of proposed Form SCIR and why that timeframe would be appropriate. For example, should Covered Entities have 72 or 96 hours to file the initial Part I of proposed Form SCIR? If so, explain why. If not, explain why not. Would providing more time to file the initial Part I of proposed Form SCIR make the filing more useful inasmuch as the Covered Entity would have more time to investigate the significant cybersecurity incident? If so, explain why and how to balance that benefit against the delay in providing this information to the Commission within 48 hours. Would the immediate notification requirement of paragraph (c) of proposed Rule 10 make it appropriate to lengthen the timeframe for when the Covered Entity would need to file the initial Part I of proposed Form SCIR? If so, explain why. If not, explain why not. For example, could the immediate notification requirement and the ability of the Commission staff to follow-up with the contact person identified on the notification serve as an appropriate alternative to receiving the initial Part I of proposed Form SCIR within 48 hours. If so, explain why. If not, explain why not. Conversely,

³³⁴ See Line Item 13.C. of Part I of proposed Form SCIR.

³³⁵ See Line Items 14.A. and B. of Part I of proposed Form SCIR.

³³⁶ See Line Item 14.A. of Part I of proposed Form SCIR.

³³⁷ See Line Item 15 of proposed Part I of Form SCIR.

³³⁸ See CIRCIA.

should the timeframe for filing an initial Part I of proposed Form SCIR be shortened to 24 hours or some other period of time that is less than 48 hours? If so, explain why. If not, explain why not.

48. Should paragraph (c)(2) of proposed Rule 10 be modified to revise the timeframe for filing an initial or amended Part I of proposed Form SCIR so the timeframes are expressed in business days or calendar days instead of hours? If so, explain why. If not, explain why not. For example, should Covered Entities have two, five, or some other number business or calendar days to file an initial or amended Part I of proposed Form SCIR? Would business or calendar days be more appropriate given that Part I of proposed Form SCIR would be filed through the EDGAR system?³³⁹ If so, explain why. If not, explain why not.

49. Should paragraph (c)(2) of proposed Rule 10 be modified to revise the timeframe for filing an initial or amended Part I of proposed Form SCIR so that it must be filed promptly after the filing requirement is triggered without specifying the 48 hour limit? If so, explain why and describe how “promptly” should be interpreted for purposes of the reporting requirements of paragraph (c) of proposed Rule 10. If not, explain why not.

50. Should paragraph (c)(2) of proposed Rule 10 be modified to revise the reporting requirements to include the filing of an initial Part I of proposed Form SCIR and a final Part I of proposed Form SCIR but not require the filing of interim amended forms? If so, explain why. If not, explain why not. For example, could informal communications between the Commission staff and the Covered Entity facilitated by the contact employee identified in the immediate notice that would be required under paragraph (c)(1) of proposed Rule 10 be an appropriate alternative to requiring the filing of interim amended forms? If so, explain why. If not, explain why not.

51. Should paragraph (c)(2) of proposed Rule 10 be modified to revise the reporting requirements to include

the filing of interim amended forms on a pre-set schedule? If so, explain why. If not, explain why not. For example, should Covered Entities be required to file an initial Part I of proposed Form SCIR and a final Part I of proposed Form SCIR pursuant to the requirements of paragraph (c) of proposed Rule 10 but file interim amended forms on a pre-set schedule? If so, explain why this would be appropriate, including why a pre-set reporting requirement would not undermine the objectives of the proposed reporting requirements, and how often the interim reporting should be required (e.g., weekly, bi-weekly, monthly, quarterly). Would a pre-set reporting cadence (e.g., weekly, bi-weekly, monthly, quarterly) undermine the objectives of the proposed reporting requirements by inappropriately delaying the Commission’s receipt of important information about a significant cybersecurity incident? If so, explain why. If not, explain why not. Would the immediate notification requirement and the ability of the Commission staff to follow-up with the contact person identified on the notification mitigate this potential consequence? If so, explain why. If not, explain why not.

52. Should paragraph (c)(2)(ii)(D) of proposed Rule 10 and Part I of proposed Form SCIR be modified to revise the reporting requirements relating to internal investigations? If so, explain why. If not, explain why not. For example, would these reporting requirements create a disincentive for Covered Entities to perform internal investigations in response to significant cybersecurity incidents? If so, explain why. If not, explain why not.

53. Should Part I of proposed Form SCIR be modified? If so, explain why. If not, explain why not. For example, does the form strike an appropriate balance of providing enough detail to the Commission to be helpful while also not being unduly burdensome to Covered Entities? If so, explain why. If not, explain why not. Is certain information that would be elicited in Part I of Form SCIR unnecessary? If so, identify the information and explain why it would be unnecessary. Is there additional information that should be required to be included in Part I of proposed Form SCIR? If so, identify the information and explain why it would be appropriate to require a Covered Entity to report it in the form.

54. Should Part I of proposed Form SCIR be modified to require that Covered Entities provide a UIC—such as

an LEI³⁴⁰ (which would require each Covered Entity without a UIC (such as an LEI) to obtain one to comply with the rule)? If so, explain why. If not, explain why not. For example, would a requirement to provide a UIC allow the Commission staff to better evaluate cyber-threats to Covered Entities? If so, explain why. If not, explain why not. Should the form be modified to require Covered Entities to provide another type of standard identifier other than a CIK number and UIC (if they have a UIC)? If so, explain why. If not, explain why not.

3. Disclosure of Cybersecurity Risks and Incidents

a. Cybersecurity Risks and Incidents Disclosure

Proposed Rule 10 would require a Covered Entity to make two types of public disclosures relating to cybersecurity on Part II of proposed Form SCIR.³⁴¹ First, the Covered Entity would need to, in plain English, provide a summary description of the cybersecurity risks that could materially affect its business and operations and how the Covered Entity assesses, prioritizes, and addresses those cybersecurity risks.³⁴² A cybersecurity risk would be material to a Covered Entity if there is a substantial likelihood that a reasonable person would consider the information important based on the total mix of facts and information.³⁴³ The facts and circumstances relevant to determining materiality in this context may include, among other things, the likelihood and extent to which the cybersecurity risk or resulting incident: (1) could disrupt or degrade the Covered Entity’s ability to maintain critical operations; (2) could adversely affect the confidentiality, integrity, or availability of information residing on the Covered Entity’s information systems, including whether the information is personal, confidential, or proprietary information; and/or (3) could harm the Covered Entity or its customers, counterparties, members, registrants, users, or other persons.

The second element of the disclosure would be a summary description of each

³³⁹ The Commission accepts electronic submissions through the EDGAR system Monday through Friday, except federal holidays, from 6:00 a.m. to 10:00 p.m. Eastern Time. See Chapter 2 of the EDGAR Filer Manual (Volume I), version 41 (Dec. 2022). Further, filings submitted by direct transmission commencing on or before 5:30 p.m. Eastern Standard Time or Eastern Daylight Saving Time, whichever is currently in effect, shall be deemed filed on the same business day, and all filings submitted by direct transmission commencing after 5:30 p.m. Eastern Standard Time or Eastern Daylight Saving Time, whichever is currently in effect, shall be deemed filed as of the next business day. 17 CFR 232.13.

³⁴⁰ The Commission approved a UIC (namely, the LEI) in a previous rulemaking. See section II.B.2.b. of this release; see also *Regulation SBSR Release*, 80 FR at 14632. The Commission is aware that additional identifiers could be recognized as UICs in the future, but for the purposes of this release, the Commission is equating the UIC with the LEI.

³⁴¹ See paragraph (d)(1) of proposed Rule 10.

³⁴² See paragraph (d)(1)(i) of proposed Rule 10; Line Item 2 of Part II proposed of Form SCIR.

³⁴³ See, e.g., *SEC v. Steadman*, 967 F.2d 636, 643 (D.C. Cir. 1992); cf. *Basic Inc. v. Levinson*, 485 U.S. 224, 231–232 (1988); *TSC Industries v. Northway, Inc.*, 426 U.S. 438, 445, 449 (1976).

significant cybersecurity incident that occurred during the current or previous calendar year, if applicable.³⁴⁴ The look-back period of the current and previous calendar years is designed to make the disclosure period consistent across all Covered Entities. The look-back period also is designed to provide a short history of significant cybersecurity incidents affecting the Covered Entity while not overburdening the firm with a longer disclosure period. The summary description of each significant cybersecurity incident would need to include: (1) the person or persons affected;³⁴⁵ (2) the date the incident was discovered and whether it is ongoing; (3) whether any data was stolen, altered, or accessed or used for any other unauthorized purpose; (4) the effect of the incident on the Covered Entity's operations; and (5) whether the Covered Entity, or service provider, has remediated or is currently remediating the incident.³⁴⁶ This disclosure—because it addresses actual significant cybersecurity incidents—would serve as another way for market participants to evaluate the Covered Entity's cybersecurity risks and vulnerabilities apart from the general disclosure of its cybersecurity risk. For example, a Covered Entity's disclosure of multiple significant cybersecurity incidents during the current or previous calendar year (particularly, if they did not impact other Covered Entities) would be useful in assessing whether the Covered Entity is adequately addressing cybersecurity risk or is more vulnerable to that risk as compared with other Covered Entities.

The objective of these disclosures is to provide greater transparency to customers, counterparties, registrants, or members of the Covered Entity, or to users of its services, about the Covered Entity's exposure to material harm as a result of a cybersecurity incident, which, in turn, could cause harm to customers, counterparties, members, registrants, or users. This information could be used by these persons to manage their own cybersecurity risk and, to the extent they have choice, select a Covered Entity with which to

transact or otherwise conduct business. Information about prior attacks and their degree of success is immensely valuable in mounting effective countermeasures.³⁴⁷

However, the intent of the disclosure on Part II of proposed Form SCIR is to avoid overly detailed disclosures that could increase cybersecurity risk for the Covered Entity and other persons. Revealing too much information could assist future attackers as well as lead to loss of customers, reputational harm, litigation, or regulatory scrutiny, which would be a cost associated with public disclosure.³⁴⁸ Therefore, under proposed Rule 10, the Covered Entity would be required to provide only a summary description of its cybersecurity risk and significant cybersecurity incidents.³⁴⁹ The requirement that the disclosures contain summary descriptions only is designed to produce meaningful disclosures but not disclosures that would reveal information (e.g., proprietary or confidential methods of addressing cybersecurity risk or known cybersecurity vulnerabilities) that could be used by threat actors to cause harm to the Covered Entity or its customers, counterparties, members, users, or other persons. This requirement is also designed to produce high-level disclosures about the Covered Entity's cybersecurity risks and significant cybersecurity incidents that can be easily reviewed by interested parties in order to give them a general understanding of the Covered Entity's risk profile.

b. Disclosure Methods and Updates

Proposed Rule 10 would require a Covered Entity to make the public disclosures discussed above (*i.e.*, the information about cybersecurity risks and significant cybersecurity incidents) on Part II of proposed Form SCIR.³⁵⁰ Part II of proposed Form SCIR would elicit information about the Covered Entity that would be used to identify the filer.³⁵¹ In particular, the Covered Entity would need to provide its full legal name and business name (if different from its legal name), UIC (if the filer has

a UIC),³⁵² CIK number, and main address.³⁵³ The Covered Entity also would need to indicate the type of Market Entity it is by checking the appropriate box or boxes.³⁵⁴ For example, if the Covered Entity is dually registered as a broker-dealer and SBSB, it would need to check the box for each of those entity types.

Page 1 of Part II of proposed Form SCIR also would contain fields for the individual executing the form to sign and date the form. By signing the form, the individual would: (1) certify that the form was executed on behalf of, and with the authority of, the Covered Entity; and (2) represent individually, and on behalf of the Covered Entity, that the information and statements contained in the form are current, true and complete. The form of the certification is designed to ensure that the Covered Entity, through the individual executing the form, discloses information that can be used by the Covered Entity's customers, counterparties, members, registrants, or users, or by other interested persons to assess the Covered Entity's cybersecurity risk profile and compare it with the risk profiles of other Covered Entities.

As discussed above, proposed Rule 10 would require the Covered Entity to publicly disclose a summary description of the cybersecurity risks that could materially affect the Covered Entity's business and operations and how the Covered Entity assesses, prioritizes, and addresses those cybersecurity risks.³⁵⁵ Line Item 2 of Part II of proposed Form SCIR would contain a narrative field in which the Covered Entity would provide this summary description.³⁵⁶ In order to provide context to the meaning of the disclosure, the beginning of Line Item 2 would set forth the definition of "cybersecurity risk" in proposed Rule 10 as well as the definitions of "cybersecurity incident," "cybersecurity

³⁴⁴ See paragraph (d)(1)(ii) of proposed Rule 10; Line Item 3 of Part II proposed of Form SCIR. See also paragraph (a)(10) of proposed Rule 10 (defining the term "significant cybersecurity incident").

³⁴⁵ This element of the disclosure would not need to include the identities of the persons affected or personal information about those persons. Instead, the disclosure could use generic terms to identify the person or persons affected. For example, the disclosure could state that "customers of the broker-dealer," "counterparties of the SBSB," or "members of the SRO" are affected (as applicable).

³⁴⁶ See paragraphs (d)(1)(ii)(A) through (E) of proposed Rule 10; Line Item 3 of Part II proposed of Form SCIR.

³⁴⁷ See Peter W. Singer and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press 222 (2014).

³⁴⁸ See, e.g., *Federal Trade Commission v. Equifax, Inc.*, FTC Matter/File Number: 172 3203, Civil Action Number: 1:19-cv-03297-TWT (2019), available at <https://www.ftc.gov/enforcement/cases-proceedings/172-3203/equifax-inc> ("FTC Equifax Civil Action").

³⁴⁹ See paragraphs (d)(1)(i) and (ii) of proposed Rule 10.

³⁵⁰ See paragraph (d) of proposed Rule 10.

³⁵¹ See Line Items 1.A. through 1.D. of Part II of proposed Form SCIR.

³⁵² As mentioned previously, the Commission approved a UIC—namely, the LEI—in a prior rulemaking. See section II.B.2.b. of this release. Therefore, for the purposes of this release, the Commission is proposing to require those Covered Entities that already have LEIs to identify themselves with LEIs on Part II of Form SCIR.

³⁵³ See Line Items 1.A. through 1.C. of Part I of proposed Form SCIR. See also section II.B.2.b. of this release (discussing UIC and CIK numbers in more detail with respect to Part I of proposed Form SCIR).

³⁵⁴ See Line Item 1.D. of Part II of proposed Form SCIR (setting forth check boxes to indicate whether the Covered Entity is a broker-dealer, clearing agency, MSBSP, the MRSB, a national securities association, a national securities exchange, SBSB, SBSDR, or transfer agent).

³⁵⁵ See paragraph (d)(1)(i) of proposed Rule 10.

³⁵⁶ See Line Item 2 of Part II of proposed Form SCIR.

threat,” and “cybersecurity vulnerability” because these three terms are used in the definition of “cybersecurity risk.”³⁵⁷

Line Item 3 of Part II of proposed Form SCIR would be used to make the disclosure about each significant cybersecurity incident that occurred during the current and previous calendar year.³⁵⁸ The definition of “significant cybersecurity incident” would be set forth at beginning of Line Item 3 in order to provide context to the meaning of the disclosure. To complete the line item, the Covered Entity first would need to indicate by checking “yes” or “no” whether it had experienced one or more significant cybersecurity incidents during the current or previous calendar year. If the answer is yes, the Covered Entity would need to provide in a narrative field on Line Item 3 the summary description of each significant cybersecurity incident.³⁵⁹

As discussed next, there would be two methods of making the disclosure, which would be required of all Covered Entities under proposed Rule 10, and an additional third method that would be required of Covered Entities that are carrying or introducing broker-dealers. First, Covered Entities would be required to file Part II of Form SCIR with the Commission electronically through the EDGAR system in accordance with the EDGAR Filer Manual, as defined in Rule 11 of Regulation S–T,³⁶⁰ and in accordance with the requirements of Regulation S–T.³⁶¹ The Commission would make these filings available to the public. The objective of requiring centralized EDGAR-filing of Part II of proposed Form SCIR is to facilitate the ability to compare disclosures across different Covered Entities or categories of Covered Entities in the same manner that EDGAR filing facilitates comparison of financial statements, annual reports, and other disclosures across Commission registrants. By creating a single location for all of the disclosures, Commission staff, investors, market participants, and analysts as well as Covered Entities’ customers, counterparties, members, registrants, or users would be able to run search queries to compare the disclosures of

multiple Covered Entities. Centralized EDGAR filing could make it easier for Commission staff and others to assess the cybersecurity risk profiles of different types of Covered Entities and could facilitate trend analysis of significant cybersecurity incidents. Thus, by providing a central location for the cybersecurity disclosures, filing Part II of proposed Form SCIR through EDGAR could lead to greater transparency of the cybersecurity risks in the U.S. securities markets.

Second, proposed Rule 10 would require the Covered Entity to post a copy of the Part II of proposed Form SCIR most recently filed on EDGAR on an easily accessible portion of its business internet website that can be viewed by the public without the need of entering a password or making any type of payment or providing any other consideration.³⁶² Consequently, the disclosures could not be located behind a “paywall” or otherwise require a person to pay a registration fee or provide any other consideration to access them. The purpose of requiring the form to be posted on the Covered Entity’s business internet website is that individuals naturally may visit a company’s business internet website when seeking timely and updated information about the company, particularly if the company is experiencing an incident that disrupts or degrades the services it provides. Therefore, requiring the form to be posted on the website is designed to make it available through this commonly used method of obtaining information. Additionally, individuals may naturally visit a company’s business internet website as part of their due diligence process in determining whether to use its services. Therefore, posting the form on the Covered Entity’s business internet website could provide individuals with information about the Covered Entity’s cybersecurity risks before they elect to enter into an arrangement with the firm. It could

serve a similar purpose for individuals considering whether to maintain an ongoing business relationship with the Covered Entity.

In addition to those two disclosure methods, a Covered Entity that is either a carrying or introducing broker-dealer would be required to provide a copy of the Part II of proposed Form SCIR most recently filed on EDGAR to a customer as part of the account opening process.³⁶³ Thereafter, the Covered Entity would need to provide the customer with the most recently posted form annually and when it is updated. The broker-dealer would need to deliver the form using the same means that the customer elects to receive account statements (*e.g.*, by email or through the postal service).³⁶⁴ This additional method of disclosure is designed to make the information readily available to the broker-dealer’s customers (many of whom may be retail investors) through the same processes that other important information (*i.e.*, information about their securities accounts) is communicated to them. Requiring a broker-dealer to deliver copies of the form is designed to enhance investor protection by enabling customers to take protective or remedial measures to the extent appropriate. It would also assist customers in determining whether their engagement of that particular broker-dealer remains appropriate and consistent with their investment objectives.

Finally, a Covered Entity would be required to file on EDGAR an updated Part II of proposed Form SCIR promptly if the information required to be disclosed about cybersecurity risks or significant cybersecurity incidents materially changes, including, in the case of the disclosure about significant cybersecurity incidents, after the occurrence of a new significant cybersecurity incident or when

³⁶³ See paragraph (d)(3) of proposed Rule 10.

³⁶⁴ If the disclosure requirements of proposed Rule 10 are adopted, the Commission would establish a compliance date by which a Covered Entity would need to make its first public disclosure on Part II of proposed Form SCIR. At a minimum, the initial disclosure would need to include a summary description of the cybersecurity risks that could materially affect the Covered Entity’s business and operations and how the Covered Entity assesses, prioritizes, and addresses those cybersecurity risks. In setting an initial compliance date, the Commission could take a bifurcated approach in which each method of disclosure has a different compliance date. For example, the compliance date for making the website disclosure could come before the compliance date for making the EDGAR disclosure and the additional disclosure required of carrying and introducing broker-dealers. The Commission seeks comment below on a potential compliance date or compliance dates for the disclosure requirements.

³⁵⁷ *Id.* See also paragraphs (a)(2) through (5) of proposed Rule 10 (defining, respectively, “cybersecurity incident,” “cybersecurity risk,” “cybersecurity threat,” and “cybersecurity vulnerability”).

³⁵⁸ See Line Item 3 of Part II of proposed Form SCIR.

³⁵⁹ See paragraph (d)(1)(ii) of proposed Rule 10.

³⁶⁰ See 17 CFR 232.11.

³⁶¹ See paragraph (d)(2)(i) of proposed Rule 10.

³⁶² See paragraph (d)(2)(ii) of proposed Rule 10. In addition to the disclosure to be made available to security-based swap counterparties as required by paragraph (d)(2)(ii) of proposed Rule 10, current Commission rules require that SBS Entities’ trading relationship documentation between certain counterparties address cybersecurity. Specifically, an SBS Entity’s trading relationship documentation must include valuation methodologies for purposes of complying with specified risk management requirements, which would include the risk management requirements of proposed Rule 10 (if it is adopted). See 17 CFR 250.15Fi–5(b)(4). This documentation would include a dispute resolution process or alternative methods for determining value in the event of a relevant cybersecurity incident. See also section IV.C.1.b.iii. of this release (discussing disclosure requirements of Rule 15Fh-3(b)).

information about a previously disclosed significant cybersecurity incident materially changes.³⁶⁵ The Covered Entity also would need to post a copy of the updated Part II of proposed Form SCIR promptly on its business internet website and, if it is a carrying broker-dealer or introducing broker-dealer, deliver copies of the form to its customers. Given the potential effect that significant cybersecurity incidents could have on a Covered Entity's customers, counterparties, members, registrants, or users—such as exposing their personal or other confidential information or resulting in a loss of cash or securities from their accounts—time is of the essence, and requiring a Covered Entity to update the disclosures promptly would enhance investor protection by enabling customers, counterparties, members, registrants, or users to take proactive or remedial measures to the extent appropriate. Accordingly, the timing of the filing of an updated disclosure should take into account the exigent nature of significant cybersecurity incidents which would generally militate toward swiftly filing the update. Furthermore, requiring Covered Entities to update their disclosures following the occurrence of a new significant cybersecurity incident would assist market participants in determining whether their business relationship with that particular Covered Entity remains appropriate and consistent with their goals.

A Covered Entity also would need to file an updated Part II of proposed Form SCIR if the information in the summary description of a significant cybersecurity incident included on the form is no longer within the look-back

period (*i.e.*, the current or previous calendar year). For example, the information that would need to be included in the summary description includes whether the significant cybersecurity incident is ongoing and whether the Covered Entity had remediated it. The Covered Entity would need to file an updated Part II of proposed Form SCIR if the significant cybersecurity incident was remediated and ended on a date that was beyond the look-back period. The updated Part II of proposed Form SCIR would no longer include a summary description of that specific significant cybersecurity incident. The objective is to focus the most recently filed disclosure on events within the relative near term. The history of the Covered Entity's significant cybersecurity incidents would be available in previous filings.

c. Request for Comment

The Commission requests comment on all aspects of the proposed disclosure requirements. In addition, the Commission is requesting comment on the following specific aspects of the proposals:

55. Should paragraph (d)(1)(i) of proposed Rule 10 be modified to revise the requirements that Covered Entities publicly disclose the cybersecurity risks that could materially affect their business and operations and to publicly disclose a description of how the Covered Entity assesses, prioritizes, and addresses those cybersecurity risks? If so, explain why. If not, explain why not. For example, would the public disclosures required by paragraph (d)(1)(i) of proposed Rule 10 be useful or provide meaningful information to a Covered Entity's customers, counterparties, members, registrants, or users? If so, explain why. If not, explain why not. Could the proposed disclosure requirement be modified to make it more useful? If so, explain how. Could the public disclosures required by paragraph (d)(1)(i) of proposed Rule 10 assist threat actors in engaging in cyber crime? If so, explain why. If not, explain why not. Could the proposed disclosure requirements be modified to eliminate this risk without negatively impacting the usefulness of the disclosures? If so, explain how.

56. Should paragraph (d)(1)(ii) of proposed Rule 10 be modified to revise the requirements that Covered Entities publicly disclose information about each significant cybersecurity incident that has occurred during the current or previous calendar year? If so, explain why. If not, explain why not. For example, would the public disclosures required by paragraph (d)(1)(ii) of

proposed Rule 10 be useful or provide meaningful information to a Covered Entity's customers, counterparties, members, registrants, or users? If so, explain why. If not, explain why not. Could the proposed disclosure requirement be modified to make it more useful? If so, explain how. Could the public disclosures required by paragraph (d)(1)(ii) of proposed Rule 10 assist threat actors in engaging in cyber crime? If so, explain why. If not, explain why not. Could the proposed disclosure requirements be modified to eliminate this risk without negatively impacting the usefulness of the disclosures? If so, explain how.

57. Should paragraph (d)(1)(ii) of proposed Rule 10 be modified to revise the required current and previous year look-back period for the disclosure of significant cybersecurity incidents? If so, explain why. If not, explain why not. For example, should the look-back period be a shorter period of time (*e.g.*, only the current calendar year)? If so, explain why. If not, explain why not. Alternatively, should the look-back period be longer (*e.g.*, the current calendar year and previous two calendar years)? If so, explain why. If not, explain why not. Should the look-back period be expressed in months rather than calendar years? For example, should the look-back period be 12, 18, 24, 30, or 36 months? If so, explain why. If not, explain why not.

58. Should paragraph (d)(1)(ii) of proposed Rule 10 be modified to provide that the requirement to include a summary description of each significant cybersecurity incident that occurred during the current or previous calendar year in Part II of proposed Form SCIR be prospective and, therefore, limited to significant cybersecurity incidents that occur on or after the compliance date of the disclosure requirement? If so, explain why. If not, explain why not.

59. Should the public disclosure requirements of paragraphs (d)(1)(i) and (ii) of proposed Rule 10 be modified to require the disclosure of additional or different information? If so, identify the additional or different information and explain why it would be appropriate to require its public disclosure by Covered Entities.

60. Should 17 CFR 240.15Fh-3(b) be amended to specify that required counterparty disclosure includes the information that would be required by paragraph (d)(1) of proposed Rule 10 and publicly disclosed on Part II of proposed Form SCIR? If so, explain why. If not explain why not.

61. Should paragraph (d)(2) of proposed Rule 10 be modified to revise

³⁶⁵ See paragraph (d)(4) of proposed Rule 10. See also Instruction C.2. of proposed Form SCIR. As discussed earlier, a Covered Entity would be required to file Part I of proposed Form SCIR with the Commission promptly, but no later than 48 hours, upon having a reasonable basis to conclude that a significant cybersecurity incident has occurred or is occurring. See paragraph (c)(2)(i) of proposed Rule 10; see also section II.B.2.a. of this release (discussing this requirement in more detail). Therefore, the Covered Entity would need to file a Part I and an updated Part II of proposed Form SCIR with the Commission relatively contemporaneously. Depending on the facts and circumstances, the Part I and updated Part II could be filed at the same time or one could proceed the other if the Covered Entity, for example, has the information to complete Part II first but needs more time to gather the information to complete Part I (which elicits substantially more information than Part II). However, as discussed above, Part I must be filed no later than 48 hours after the Covered Entity has a reasonable basis to conclude that a significant cybersecurity incident has occurred or is occurring and the Covered Entity must include in the initial filing the information that is known at that time and file an updated Part I as more information becomes known to the Covered Entity.

the methods of making the public disclosures? If so, explain why. If not, explain why not. For example, should Covered Entities be required to file Part II of proposed Form SCIR on EDGAR but not be required to post a copy of the form on their business internet websites? If so, explain why. If not, explain why not. Would requiring the public cybersecurity disclosures to be filed in a centralized electronic system, such as EDGAR, make it easier for investors, analysts, and others to access and gather information from the cybersecurity disclosures than if those disclosures were only posted on Covered Entity websites? Alternatively, should Covered Entities be required to post an executed copy of Part II of proposed Form SCIR on their business internet websites but not be required to file the form on EDGAR? If so, explain why. If not, explain why not. Why or why not?

62. Should paragraph (d)(2) of proposed Rule 10 be modified to revise the requirement to post a copy of Part II of proposed Form SCIR on business internet website of the Covered Entity to permit the Covered Entity to post a link to the EDGAR filing? If so, explain why. If not, explain why not.

63. Should paragraph (d)(3) of proposed Rule 10 be modified to revise the additional methods of making the public disclosures required of carrying and introducing broker-dealers? If so, explain why. If not, explain why not. For example, would filing Part II of proposed Form SCIR on EDGAR and posting a copy of the form on the Covered Entity's business internet website be sufficient to meet the objectives of the disclosure requirements discussed above and, therefore, obviate the need for a carrying broker-dealer or introducing broker-dealer to additionally send copies of the form to customers? If so, explain why. If not, explain why not. Rather than requiring the broker-dealer or introducing broker-dealer to send a copy of the Part II of proposed Form SCIR most recently filed on EDGAR to each customer, would it be sufficient that the most recently filed form as of the end of each quarter or the calendar year be sent to the customers? If so, explain why. If not, explain why not.

64. Should paragraph (d)(3) of proposed Rule 10 be modified to permit the Covered Entity to send a website link to the EDGAR filing to customers instead of a copy of the EDGAR filing? If so, explain why. If not, explain why not.

65. Should paragraph (d)(3) of proposed Rule 10 be modified to require other types of Covered Entities to send

a copy of the most recently filed Part II of proposed Form SCIR to their customers, counterparties, members, registrants, or users? If so, explain why. If not, explain why not. For example, should transfer agents be required to send the most recently filed Part II of proposed Form SCIR to their securityholders? If so, explain why. If not, explain why not.

66. Should paragraph (d)(4) of proposed Rule 10 be modified to revise the requirement that a Covered Entity must "promptly" provide an updated disclosure on Part II of proposed Form SCIR if the information on the previous disclosure materially changes to provide that the Commission shall allow registrants to delay publicly disclosing a significant cybersecurity incident where the Attorney General requests such a delay from the Commission based on the Attorney General's written determination that the delay is in the interest of national security?

67. Should paragraph (d)(4) of proposed Rule 10 be modified to revise the requirement that a Covered Entity must "promptly" provide an updated disclosure on Part II of proposed Form SCIR if the information on the previous disclosure materially changes to specify a timeframe within which the updated filing must be promptly made? If so, explain why. If not, explain why not. For example, should the rule be modified to require that the updated disclosure must be made within 24, 36, 48, or 60 hours of the information on the previous disclosure materially changing? If so, explain why. If not, explain why not. Should the timeframe for making the updated disclosure be expressed in business days? If so, explain why. If not, explain why not. For example, should the updated disclosure be required to be made within two, three, four, or five business days (or some other number of days) of the information on the previous disclosure materially changing? If so, explain why. If not, explain why not.

68. Should paragraph (d)(4) of proposed Rule 10 be modified to revise the requirement that a Covered Entity must "promptly" provide an updated disclosure on Part II of proposed Form SCIR if the information on the previous disclosure materially changes to require the update to be made within 30 days (similar to the requirement for updating Form CRS)?³⁶⁶ If so, explain why. If not, explain why not. For example, would this approach appropriately balance the objective of requiring timely disclosure with the objective of providing accurate

and complete disclosure? If so, explain why. If not, explain why not.

69. Should paragraph (d)(4) of proposed Rule 10 be modified to revise the requirements that trigger when an updated Part II of proposed Form SCIR must be filed on EDGAR, posted on the Covered Entity's business internet website, and, if applicable, sent to customers? If so, explain why. If not, explain why not. For example, should the rule require that an updated form must be publically disclosed through these methods on a quarterly, semi-annual, or annual basis if the information on the previously filed form has materially changed? If so, explain why. If not, explain why not.

70. Should Part II of proposed Form SCIR be modified to require that Covered Entities provide a UIC—such as an LEI (which would require Covered Entities without a UIC (such as an LEI) to obtain one to comply with the rule)?³⁶⁷ If so, explain why. If not, explain why not. For example, would requiring Covered Entities to provide a UIC better allow investors, analysts, and third-party data aggregators to evaluate the cyber security risk profiles of Covered Entities? If so, explain why. If not, explain why not. Should the form be modified to require Covered Entities to provide another type of standard identifier other than a CIK number and UIC (if they have a UIC)? If so, explain why. If not, explain why not.

71. If the disclosure requirements of proposed Rule 10 are adopted, what would be an appropriate compliance date for the disclosure requirements? For example, should the compliance date be three, six, nine, or twelve months after the effective date of the rule (or some other period of months)? Please suggest a compliance period and explain why it would be appropriate. Should the compliance date for the website disclosure be sooner than the compliance date for the EDGAR disclosure or vice versa? If so, explain why. If not, explain why not. Should the compliance date for the additional disclosure methods that would be required of carrying and introducing broker-dealers be different than the compliance dates for the website disclosure and the EDGAR disclosure? If so, explain why. If not, explain why not. If the requirement to provide a summary description of each significant cybersecurity incident that occurred

³⁶⁷ As mentioned previously in section II.B.2.b. of this release, the Commission approved a UIC (namely, the LEI) in a previous rulemaking. The Commission is aware that additional identifiers could be recognized as UICs in the future, but for the purposes of this release, the Commission is equating the UIC with the LEI.

³⁶⁶ See Form CRS Instructions, available at <https://www.sec.gov/files/formcrs.pdf>.

during the current and previous calendar year is prospective (*i.e.*, does not apply to incidents that occurred before the compliance date), should the compliance period be shorter than if the requirement was retrospective, given that the initial disclosure, in most cases, would be limited to a summary description of the cybersecurity risks that could materially affect the Covered Entity's business and operations and how the Covered Entity assesses, prioritizes, and addresses those cybersecurity risks? If so, explain why. If not, explain why not.

4. Filing Parts I and II of Proposed Form SCIR in EDGAR Using a Structured Data Language

a. Discussion

Proposed Rule 10 would require Covered Entities would file Parts I and II of proposed Form SCIR electronically with the Commission using the EDGAR system in accordance with the EDGAR Filer Manual, as defined in Rule 11 of Regulation S–T,³⁶⁸ and in accordance with the requirements of Regulation S–T.³⁶⁹ In addition, under the proposed requirements, Covered Entities would file Parts I and II of Form SCIR in a structured (*i.e.*, machine-readable) data language.³⁷⁰ Specifically, Covered Entities would file Parts I and II of proposed Form SCIR in an eXtensible Markup Language (“XML”)-based data language specific to the form (“custom XML,” and in this release “SCIR-specific XML”). While the majority of filings through the EDGAR system are submitted in unstructured HTML or ASCII formats, certain EDGAR-system filings are submitted using custom XML languages that are each specific to the particular form being submitted.³⁷¹ For such filings, filers are typically provided the option to either submit the filing directly to the EDGAR system in the relevant custom XML data language, or to manually input the information into a fillable web-based form developed by the Commission that converts the completed form into a custom XML document.³⁷²

Requiring Covered Entities to file Parts I and II of proposed Form SCIR through the EDGAR system would allow

the Commission to download Form SCIR information directly from a central location, thus facilitating efficient access, organization, and evaluation of the information contained in the forms. Use of the EDGAR system also would enable technical validation of the information reported on Form SCIR, which could potentially reduce the incidence of non-discretionary errors (*e.g.*, leaving required fields blank). Thus, the proposed requirement to file Parts I and II of proposed Form SCIR through the EDGAR system would allow the Commission and, in the case of Part II, the public to more effectively examine and analyze the reported information. In this regard, the proposed requirement to file Parts I and II of proposed Form SCIR through the EDGAR system using SCIR-specific XML, a machine-readable data language, is designed to facilitate more thorough review and analysis of the reported information.

b. Request for Comment

The Commission requests comment on all aspects of the proposed requirements to file Parts I and II of Form SCIR in EDGAR using a structured data language. In addition, the Commission is requesting comment on the following specific aspects of the proposals:

72. Should the Commission modify the structured data language requirement for both Parts I and II of Form SCIR in accordance with the alternatives discussed in Section IV.F. below?³⁷³ Should Covered Entities be required to file the cybersecurity risk and incident disclosures on Part II of Form SCIR in the EDGAR system in a structured data language? Why or why not? Would custom XML or Inline eXtensible Business Reporting Language (“iXBRL”) be the most suitable data language for this information? Or would another data language be more appropriate?

5. Recordkeeping

a. Amendments to Covered Entity Recordkeeping Rules

As discussed above, proposed Rule 10 would require a Covered Entity to: (1) establish, maintain, and enforce reasonably designed policies and procedures to address cybersecurity risks;³⁷⁴ (2) create written

documentation of risk assessments;³⁷⁵ (3) create written documentation of any cybersecurity incident, including its response to and recovery from the incident;³⁷⁶ (4) prepare a written report each year describing its annual review of its policies and procedures to address cybersecurity risks;³⁷⁷ (5) provide immediate electronic written notice to the Commission of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring;³⁷⁸ (6) report, not later than 48 hours, upon having a reasonable basis to conclude that a significant cybersecurity incident has occurred or is occurring on Part I of proposed Form SCIR;³⁷⁹ and (7) provide a written summary disclosure about its cybersecurity risks that could materially affect its business and operations, and how the Covered Entity assesses, prioritizes, and addresses those risks, and significant cybersecurity incidents that occurred during the current or previous calendar year on Part II of proposed Form SCIR.³⁸⁰ Consequently, proposed Rule 10 would require a Covered Entity to make several different types of records (collectively, the “Rule 10 Records”). The proposed cybersecurity rule would not include requirements specifying how long these records would need to be preserved and the manner in which they would need to be maintained. Instead, as discussed below, preservation and maintenance requirements applicable to Rule 10 Records would be imposed through amendments, as necessary, to the existing record preservation and maintenance rules applicable to the Covered Entities.

In particular, broker-dealers, transfer agents, and SBS Entities are subject to existing requirements that specify how long the records they are required to make must be preserved (*e.g.*, three or six years) and how the records must be maintained (*e.g.*, maintenance

³⁷⁵ See paragraph (b)(1)(i)(B) of proposed Rule 10. See also section II.B.1.a. of this release (discussing this proposed requirement in more detail).

³⁷⁶ See paragraph (b)(1)(v)(B) of proposed Rule 10. See also section II.B.1.e. of this release (discussing this proposed requirement in more detail).

³⁷⁷ See paragraph (b)(2)(ii) of proposed Rule 10. See also section II.B.1.f. of this release (discussing this proposed requirement in more detail).

³⁷⁸ See paragraph (c)(1) of proposed Rule 10. See also section II.B.2.a. of this release (discussing this proposed requirement in more detail).

³⁷⁹ See paragraph (c)(2) of proposed Rule 10. See also Section II.B.2.b. of this release (discussing this proposed requirement in more detail).

³⁸⁰ See paragraph (d) of proposed Rule 10. See also Section II.B.3. of this release (discussing this proposed requirement in more detail).

³⁶⁸ See 17 CFR 232.11.

³⁶⁹ See paragraphs (c) and (d) of proposed Rule 10.

³⁷⁰ Requirements related to custom-XML filings are generally covered in the EDGAR Filer Manual, which is incorporated in Commission regulations by reference via Regulation S–T. See 17 CFR 232.11; 17 CFR 232.101.

³⁷¹ See Commission, *Current EDGAR Technical Specifications* (Dec. 5, 2022), available at <https://www.sec.gov/edgar/filer-information/current-edgar-technical-specifications>.

³⁷² See Chapters 8 and 9 of the EDGAR Filer Manual (Volume II), version 64 (Dec. 2022).

³⁷³ See section IV.F. of this release.

³⁷⁴ See paragraph (b)(1) of proposed Rule 10. See also sections II.B.1.a. through II.B.1.e. of this release (discussing this proposed requirement in more detail).

requirements for electronic records).³⁸¹ The Commission is proposing to amend these record preservation and maintenance requirements to identify Rule 10 Records specifically as records that would need to be preserved and maintained pursuant to these existing requirements. In particular, the Commission is proposing to amend the record preservation and maintenance rules for: (1) broker-dealers;³⁸² (2) transfer agents;³⁸³ and (3) SBS entities.³⁸⁴ The proposed amendments would specify that the Rule 10 Records must be retained for three years. In the case of the written policies and procedures to address cybersecurity risks, the record would need to be maintained until three years after the termination of the use of the policies and procedures. These amendments would subject the Rule 10 Records to the record maintenance requirements of Rules 17a-4, 17ad-7, and 18a-6, including the requirements governing electronic records.³⁸⁵

Exchange Act Rule 17a-1 (“Rule 17a-1”)—the record maintenance and preservation rule applicable to registered clearing agencies, the MSRB, national securities associations, and national securities exchanges—as it exists today would require the preservation of the Rule 10 Records.³⁸⁶ In particular, Rule 17a-1 requires these types of Covered Entities to keep and preserve at least one copy of all documents, including all correspondence, memoranda, papers, books, notices, accounts, and other such records as shall be made or received by

³⁸¹ See 17 CFR 240.17a-4 (“Rule 17a-4”) (setting forth record preservation and maintenance requirements for broker-dealers); 17 CFR 240.17ad-7 (“Rule 17ad-7”) (setting forth record preservation and maintenance requirements for transfer agents); 17 CFR 240.18a-6 (“Rule 18a-6”) (setting forth record preservation and maintenance requirements for SBS Entities). The Commission’s proposal includes an amendment to a CFR designation in order to ensure regulatory text conforms more consistently with section 2.13 of the Document Drafting Handbook. See Office of the Federal Register, Document Drafting Handbook (Aug. 2018 Edition, Revision 1.4, dated January 7, 2022), available at <https://www.archives.gov/files/federal-register/write/handbook/ddh.pdf>. In particular, the proposal is to amend the CFR section designation for Rule 17Ad-7 (17 CFR 240.17Ad-7) to replace the uppercase letter with the corresponding lowercase letter, such that the rule would be redesignated as Rule 17ad-7 (17 CFR 240.17ad-7).

³⁸² This amendment would add a new paragraph (e)(13) to Rule 17a-4.

³⁸³ This amendment would add a new paragraph (j) to Rule 17ad-7.

³⁸⁴ This amendment would add a new paragraph (d)(6) to Rule 18a-6.

³⁸⁵ See paragraphs (f) of Rule 17a-4, (f) of Rule 17ad-7, and (e) of Rule 18a-6 (setting forth requirements for electronic records applicable to broker-dealers, transfer agents, and SBS Entities, respectively).

³⁸⁶ See 17 CFR 240.17a-1.

the Covered Entity in the course of its business as such and in the conduct of its self-regulatory activity.³⁸⁷

Furthermore, Rule 17a-1 provides that the Covered Entity must keep the documents for a period of not less than five years, the first two years in an easily accessible place, subject to the destruction and disposition provisions of Exchange Act Rule 17a-6.³⁸⁸ Consequently, under the existing provisions of Rule 17a-1, registered clearing agencies, the MSRB, national securities associations, and national securities exchanges would be required to preserve at least one copy of the Rule 10 Records for at least five years, the first two years in an easily accessible place. In the case of the written policies and procedures to address cybersecurity risks, pursuant to Rule 17a-1 the record would need to be maintained until five years after the termination of the use of the policies and procedures.³⁸⁹

Similarly, Exchange Act Rule 13n-7 (“Rule 13n-7”)—the record maintenance and preservation rule applicable to SBSDRs—as it exists today would require the preservation of the Rule 10 Records.³⁹⁰ In particular, Rule 13n-7 requires SBSDRs to, among other things, keep and preserve at least one copy of all documents, including all documents and policies and procedures required by the Exchange Act and the rules and regulations thereunder, correspondence, memoranda, papers, books, notices, accounts, and other such records as shall be made or received by it in the course of its business as such.³⁹¹ Furthermore, Rule 13n-7 provides that the SBSDR must keep the documents for a period of not less than five years, the first two years in a place that is immediately available to representatives of the Commission for inspection and examination.³⁹² Consequently, under the existing provisions of Rule 13n-7, SBSDRs would be required to preserve at least one copy of the Rule 10 Records for at

³⁸⁷ See paragraph (a) of Rule 17a-1.

³⁸⁸ See paragraph (b) of Rule 17a-1; 17 CFR 240.17a-6 (“Rule 17a-6”). Rule 17a-6 of the Exchange Act provides that an SRO may destroy such records at the end of the five year period or at an earlier date as is specified in a plan for the destruction or disposition of any such documents if such plan has been filed with the Commission by SRO and has been declared effective by the Commission.

³⁸⁹ See, e.g., *Nationally Recognized Statistical Rating Organizations*, Exchange Act Release No. 72936 (Aug. 27, 2014) [79 FR 55078, 55099–100 (Sept. 15, 2014)] (explaining why preservation periods for written policies and procedures are based on when a version of the policies and procedures is updated or replaced).

³⁹⁰ See 17 CFR 240.13n-7.

³⁹¹ See paragraph (b)(1) of Rule 13n-7.

³⁹² See paragraph (b)(2) of Rule 13n-7.

least five years, the first two years in a place that is immediately available to representatives of the Commission for inspection and examination. In the case of the written policies and procedures to address cybersecurity risks, the Commission interprets this provision of Rule 13n-7 to require that the record would need to be maintained until five years after the termination of the use of the policies and procedures.

Clearing agencies that are exempt from registration would be Covered Entities under proposed Rule 10.³⁹³ Exempt clearing agencies are not subject to Rule 17a-1. However, while exempt clearing agencies—as entities that have limited their clearing agency functions—might not be subject to the full range of clearing agency regulation, the Commission has stated that, for example, an entity seeking an exemption from clearing agency registration for matching services would be required to, among other things, allow the Commission to inspect its facilities and records.³⁹⁴ In this regard, exempt clearing agencies are subject to conditions that mirror certain of the recordkeeping requirements in Rule 17a-1,³⁹⁵ as set forth in the respective Commission orders exempting each exempt clearing agency from the requirement to register as a clearing agency (the “clearing agency exemption orders”).³⁹⁶ Pursuant to the terms and conditions of the clearing agency exemption orders, the Commission may modify by order the terms, scope, or conditions if the Commission determines that such modification is necessary or appropriate in the public interest, for the protection of investors, or otherwise in furtherance of the

³⁹³ See paragraph (a)(1)(ii) of proposed Rule 10 (defining as a “covered entity” a clearing agency (registered or exempt) under section 3(a)(23)(A) of the Exchange Act). See also section I.A.2.c. of this release (discussing the clearing agency exemptions provided by the Commission).

³⁹⁴ See *Confirmation and Affirmation of Securities Trades; Matching*, Exchange Act Release No. 39829 (Apr. 6, 1998) [63 FR 17943 (Apr. 13, 1998)] (providing interpretive guidance and requesting comment on the confirmation and affirmation of securities trades and matching).

³⁹⁵ See, e.g., BSTP SS&C Order, 80 FR at 75411 (conditioning BSTP’s exemption by requiring BSTP to, among other things, preserve a copy or record of all trade details, allocation instructions, central trade matching results, reports and notices sent to customers, service agreements, reports regarding affirmation rates that are sent to the Commission or its designee, and any complaint received from a customer, all of which pertain to the operation of its matching service and ETC service. BSTP shall retain these records for a period of not less than five years, the first two years in an easily accessible place.).

³⁹⁶ See DTCC ITP Matching Order, 66 FR 20494; BSTP SS&C Order, 80 FR 75388; Euroclear Bank Order, 81 FR 93994.

purposes of the Exchange Act.³⁹⁷ In support of the public interest and the protection of investors, the Commission is proposing to amend the clearing agency exemption orders to add a condition that each exempt clearing agency must retain the Rule 10 Records for a period of at least five years after the record is made or, in the case of the written policies and procedures to address cybersecurity risks, for at least five years after the termination of the use of the policies and procedures.

b. Request for Comment

The Commission requests comment on all aspects of the proposed recordkeeping requirements. In addition, the Commission is requesting comment on the following specific aspects of the proposals:

73. Should the proposed amendments to Rules 17a-4, 18a-6, and/or 17ad-7 be modified? If so, describe how they should be modified and explain why the modification would be appropriate. For example, should the retention periods for the records be five years (consistent with Rule 17a-1) or some other period of years as opposed to three years? If so, explain why. If not, explain why not.

74. As discussed above, the Commission is proposing to amend the clearing agency exemption orders to specifically require the exempt clearing agencies to retain the Rule 10 Records. Should the ordering language be consistent with the proposed amendments to Rules 17a-4, 17ad-7, and 18a-6? For example, should the ordering language provide that the exempt clearing agency must maintain and preserve: (1) the written policies and procedures required to be adopted and implemented pursuant to paragraph (b)(1) of proposed Rule 10 until five years after the termination of the use of the policies and procedures; (2) the written documentation of any risk assessment pursuant to paragraph (b)(1)(i)(B) of proposed Rule 10 for five years; (3) the written documentation of the occurrence of a cybersecurity incident pursuant to paragraph (b)(1)(v)(B) of proposed Rule 10, including any documentation related to any response and recovery from such an incident, for five years; (4) the written report of the annual review required to be prepared pursuant to paragraph (b)(2)(ii) of proposed Rule 10 for five years; (5) a copy of any notice transmitted to the Commission pursuant to paragraph (c)(1) of proposed Rule 10 or any Part I of proposed Form SCIR filed with the Commission pursuant to paragraph (c)(2) of proposed Rule 10 for

five years; and (6) a copy of any Part II of proposed Form SCIR filed with the Commission pursuant to paragraph (d) of proposed Rule 10 for five years? Additionally, should the ordering language provide that the exempt clearing agency must allow the Commission to inspect its facilities and records? If so, explain why. If not, explain why not.

C. Proposed Requirements for Non-Covered Broker-Dealers

1. Cybersecurity Policies and Procedures, Annual Review, Notification, and Recordkeeping

As discussed earlier, not all broker-dealers would be Covered Entities under proposed Rule 10.³⁹⁸ Consequently, these Non-Covered Broker-Dealers would not be subject to the requirements of proposed Rule 10 to: (1) include certain elements in their cybersecurity risk management policies and procedures;³⁹⁹ (2) file confidential reports that provide information about the significant cybersecurity incident with the Commission and, for some Covered Entities, other regulators;⁴⁰⁰ and (3) make public disclosures about their cybersecurity risks and the significant cybersecurity incidents they experienced during the current or previous calendar year.⁴⁰¹

In light of their limited business activities, Non-Covered Broker-Dealers would not be subject to the same requirements as would Covered Entities. Instead, Non-Covered Broker-Dealers would be required to establish, maintain, and enforce written policies and procedures that are reasonably designed to address their cybersecurity risks taking into account the size, business, and operations of the firm.⁴⁰² They also would be required to review and assess the design and effectiveness of their cybersecurity policies and procedures, including whether the policies and procedures reflect changes in cybersecurity risk over the time period covered by the review. They also would be required to make a record with respect to the annual review. In addition, they would be required to provide the Commission and their examining authority with immediate written electronic notice of a significant

³⁹⁸ See section II.A.1. of this release (discussing the definition of “covered entity” and why certain broker-dealers would not be included within the definition).

³⁹⁹ See paragraphs (b)(1)(i) through (v) of proposed Rule 10.

⁴⁰⁰ See paragraph (c)(2) of proposed Rule 10. See also paragraph (a)(10) of proposed Rule 10 (defining the term “significant cybersecurity risk”).

⁴⁰¹ See paragraph (d) of proposed Rule 10.

⁴⁰² See paragraph (e)(1) of proposed Rule 10.

cybersecurity incident affecting them.⁴⁰³ Finally, they would be required to maintain and preserve versions of their policies and procedures and the record of the annual review.

A Non-Covered Broker-Dealer could be a firm that limits its business to selling mutual funds on a subscription-way basis or a broker-dealer that limits its business to engaging in private placements for clients. Alternatively, it could be a broker-dealer that limits its business to effecting securities transactions in order to facilitate mergers, acquisitions, business sales, and business combinations or a broker-dealer that limits its business to engaging in underwritings for issuers. Moreover, a Non-Covered Broker-Dealer—because it does not meet the definition of “covered entity”—would not be a broker-dealer that: maintains custody of customer securities and cash;⁴⁰⁴ connects to a broker-dealer that maintains custody of customer securities through an introducing relationship;⁴⁰⁵ is a large proprietary trading firm;⁴⁰⁶ operates as a market maker;⁴⁰⁷ or operates an ATS.⁴⁰⁸

A broker-dealer that limits its business to one of the activities described above and that does not engage in functions that would make it a Covered Entity under proposed Rule 10 generally does not use information systems to carry out its operations to the same degree as a broker-dealer that is a Covered Entity. For example, the information systems used by a Non-Covered Broker-Dealer could be limited to smart phones and personal computers with internet and email access. Moreover, this type of firm may have a small staff of employees using these information systems. Therefore, the

⁴⁰³ See paragraph (e)(2) of proposed Rule 10.

⁴⁰⁴ See paragraph (a)(1)(i)(A) of proposed Rule 10 (defining “covered entity” to include a broker-dealer that maintains custody of cash and securities for customers or other broker-dealers and is not exempt from the requirements of Rule 15c3-3).

⁴⁰⁵ See paragraph (a)(1)(i)(B) of proposed Rule 10 (defining “covered entity” to include a broker-dealer that introduces customer accounts on a fully disclosed basis to another broker-dealer that maintains custody of cash and securities for customers or other broker-dealers and is not exempt from the requirements of Rule 15c3-3).

⁴⁰⁶ See paragraphs (a)(1)(i)(C) and (D) of proposed Rule 10 (defining “covered entity” to include a broker-dealer with regulatory capital equal to or exceeding \$50 million or total assets equal to or exceeding \$1 billion).

⁴⁰⁷ See paragraph (a)(1)(i)(E) of proposed Rule 10 (defining “covered entity” to include a broker-dealer that is a market maker under the Exchange Act or the rules thereunder (which includes a broker-dealer that operates pursuant to Rule 15c3-1(a)(6)) or is a market maker under the rules of an SRO of which the broker-dealer is a member).

⁴⁰⁸ See paragraph (a)(1)(i)(F) of proposed Rule 10 (defining “covered entity” to include a broker-dealer that is an ATS).

³⁹⁷ See Clearstream Banking Order, 62 FR 9225.

overall footprint of the information systems used by a Non-Covered Broker-Dealer may be materially smaller in scale and complexity than the footprint of the information systems used by a broker-dealer that is a Covered Entity. In addition, the amount of data stored on these information systems relating to the Non-Covered Broker-Dealer's business may be substantially less than the amount of data stored on a Covered Entity's information systems. This means the information system perimeter of these firms that needs to be protected from cybersecurity threats and vulnerabilities is significantly smaller than that of a Covered Broker-Dealer. For these reasons, proposed Rule 10 would provide that the written policies and procedures required of a Non-Covered Broker-Dealer must be reasonably designed to address the cybersecurity risks of the firm taking into account the size, business, and operations of the firm.

Therefore, unlike the requirements for a Covered Entity, proposed Rule 10 does not specify minimum elements that would need to be included in a Non-Covered Broker-Dealer's policies and procedures.⁴⁰⁹ Nonetheless, a Non-Covered Broker-Dealer may want to consider whether any of those required elements would be appropriate components of its policies and procedures for addressing cybersecurity risk.⁴¹⁰

Proposed Rule 10 also would require that the Non-Covered Broker-Dealer annually review and assess the design and effectiveness of its cybersecurity policies and procedures, including whether the policies and procedures reflect changes in cybersecurity risk over the time period covered by the review.⁴¹¹ The annual review and assessment requirement is designed to require Non-Covered Broker-Dealers to evaluate whether their cybersecurity policies and procedures continue to work as designed. Non-Covered Broker-Dealers could consider using this information to determine whether changes are needed to assure their continued effectiveness (*i.e.*, to make sure their policies and procedures continue to be reasonably designed to

address their cybersecurity risks as required by the rule).

The rule also would require the Non-Covered Broker-Dealer to make a written record that documents the steps taken in performing the annual review and the conclusions of the annual review. Therefore, Non-Covered Broker-Dealers would need to make a record of the review rather than documenting the review in a written report, as would be required of Covered Entities.⁴¹² A report is a means to communicate information within an organization. The personnel that prepare the report for the Covered Entity would be able to use it to communicate their assessment of the firm's policies and procedures to others within the organization such as senior managers. For purposes of proposed Rule 10, a record, among other things, is a means to document that an activity took place, for example, to demonstrate compliance with a requirement. As discussed above, Non-Covered Broker-Dealers generally would be smaller and less complex organizations than Covered Entities. A record of the annual review could be used by Commission examination staff to review the Non-Covered Broker-Dealer's compliance with the annual review requirement without imposing the additional process involved in creating an internal report.

As discussed earlier, Covered Entities would be subject to a requirement to give the Commission immediate written electronic notice of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring.⁴¹³ Non-Covered Broker-Dealers would be subject to the same immediate written electronic notice requirement. In particular, they would be required to give immediate written electronic notice to the Commission of a significant cybersecurity incident upon having a reasonable basis to conclude that the incident has occurred or is occurring.⁴¹⁴ The Commission would keep the notices nonpublic to the extent permitted by law. The notice would need to identify the Non-Covered Broker-Dealer, state that the notice is being given to alert the Commission of a significant cybersecurity incident impacting the Non-Covered Broker-

Dealer, and provide the name and contact information of an employee of the Non-Covered Broker-Dealer who can provide further details about the nature and scope of the significant cybersecurity incident. In addition, Non-Covered Broker-Dealers—like Covered Broker-Dealers—would need to give the notice to their examining authority.⁴¹⁵ The immediate written electronic notice is designed to alert the Commission on a confidential basis to the existence of a significant cybersecurity incident impacting a Non-Covered Broker-Dealer so the Commission staff can quickly begin to assess the event.

Finally, as discussed above, proposed Rule 10 would require the Non-Covered Broker-Dealer to: (1) establish, maintain, and enforce written policies and procedures that are reasonably designed to address the cybersecurity risks of the firm; (2) make a written record that documents its annual review; and (3) provide immediate electronic written notice to the Commission of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring.⁴¹⁶ The Commission is proposing to amend the broker-dealer record preservation and maintenance rule to identify these records specifically as being subject to the rule's requirements.⁴¹⁷ Under the amendments, the written policies and procedures would need to be maintained until three years after the termination of the use of the policies and procedures and all other records would need to be maintained for three years.

2. Request for Comment

The Commission requests comment on all aspects of the proposed requirements for non-covered broker-dealers. In addition, the Commission is requesting comment on the following specific aspects of the proposals:

75. Should paragraph (e)(1) of proposed Rule 10 be modified to specify certain minimum elements that would need to be included in the policies and procedures of Non-Covered Broker-Dealers? If so, identify the elements and explain why they should be included. For example, should paragraph (e) of proposed Rule 10 specify that the policies and procedures must include policies and procedures to address any

⁴⁰⁹ See paragraph (b)(1) of proposed Rule 10 (setting forth the elements that would need to be included in a Covered Entity's policies and procedures).

⁴¹⁰ As discussed earlier, the elements are consistent with industry standards for addressing cybersecurity risk. See section II.B.1. of this release (discussing the policies and procedures requirements for Covered Entities).

⁴¹¹ See paragraph (e)(1) of proposed Rule 10.

⁴¹² See section II.B.1.f. of this release (discussing in more detail the annual report that would be required of Covered Entities).

⁴¹³ See paragraph (c)(1) of proposed Rule 10. See also section II.B.2.a. of this release (discussing the immediate notification requirement for Covered Entities in more detail).

⁴¹⁴ See paragraph (e)(2) of proposed Rule 10. See also paragraph (a)(10) of proposed Rule 10 (defining the term "significant cybersecurity incident").

⁴¹⁵ See paragraph (e)(2) of proposed Rule 10. See also paragraph (c)(1)(i) of proposed Rule 10 (requiring Covered Broker-Dealers to provide the notice to their examining authority).

⁴¹⁶ See paragraph (e) of proposed Rule 10.

⁴¹⁷ This amendment would add a new paragraph (e)(13) to Rule 17a-4.

or all of the following: (1) risk assessment; (2) user security and access; (3) information protection; (4) cybersecurity threat and vulnerability management; and (5) cybersecurity incident response and recovery? If so, explain why. If not, explain why not.

76. Should paragraph (e)(2) of proposed Rule 10 be modified to require the notice to be given within a specific timeframe such as on the same day the requirement was triggered or within 24 hours? If so, explain why. If not, explain why not.

77. Should paragraph (e)(2) of proposed Rule 10 be modified to revise the trigger for the immediate notification requirement? If so, explain why. If not, explain why not. For example, should the trigger be when the Non-Covered Broker-Dealer “detects” a significant cybersecurity incident (rather than when it has a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring)? If so, explain why. If not, explain why not. For example, would a detection standard be a less subjective standard? If so, explain why. If not, explain why not. Is there another trigger standard that would be more appropriate? If so, identify it and explain why it would be more appropriate.

78. Should paragraph (e)(2) of proposed Rule 10 be modified to eliminate the requirement that a Non-Covered Broker-Dealer give the Commission immediate written electronic notice of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring? If so, explain why. If not, explain why not. For example, would this requirement be unduly burdensome on Non-Covered Broker-Dealers? Please explain.

79. If the immediate notification requirement of paragraph (e)(2) is adopted as proposed, it is anticipated that a dedicated email address would be established to receive these notices. Are there other methods the Commission should use for receiving these notices? If so, identify them and explain why they would be more appropriate than email. For example, should the notices be received through the EDGAR system? If so, explain why. If not, explain why not.

80. Should paragraph (e) of proposed Rule 10 be modified to include any other requirements that would be applicable to Covered Entities under proposed Rule 10 that also should be required of Non-Covered Broker-Dealers? If so, identify them and explain why they should apply to Non-Covered

Broker-Dealers. For example, should the paragraph be modified to require Non-Covered Broker-Dealers to report information about a significant cybersecurity incident confidentially on Part I of proposed Form SCIR? If so, explain why. If not, explain why not. Should the timeframe for filing Part I of Proposed Form SCIR be longer for Non-Covered Broker-Dealers? For example, should the reporting timeframe be within 72 or 96 hours instead of 48 hours? Please explain. If Non-Covered Broker-Dealers were required to file Part I of Form SCIR, should they be permitted to provide more limited information about the significant cybersecurity incident than Covered Entities? If so, identify the more limited set of information and explain why it would be appropriate to permit Non-Covered Broker-Dealers omit the additional information that Covered Entities would need to report.

81. Should Non-Covered Broker-Dealers be required to make and preserve for three years in accordance with Rule 17a-4 a record of any significant cybersecurity incident that impacts them containing some or all of the information that would be reported by Covered Entities on Part I of proposed Form SCIR? If so, explain why. If not, explain why not.

82. Should paragraph (e) of proposed Rule 10 be modified to require a Non-Covered Broker-Dealer to prepare a written report of the annual review (rather than a record, as proposed)? If so, explain why. If not, explain why not.

D. Cross-Border Application of the Proposed Cybersecurity Requirements to SBS Entities

1. Background on the Cross-Border Application of Title VII Requirements

Security-based swap transactions take place across national borders, with agreements negotiated and executed between counterparties in different jurisdictions (which might then be booked and risk-managed in still other jurisdictions).⁴¹⁸ Mindful that this global market developed prior to the enactment of the Dodd-Frank Act and the fact that the application of Title VII⁴¹⁹ to cross-border activities raises issues of potential conflict or overlap with foreign regulatory regimes,⁴²⁰ the Commission has adopted a taxonomy to classify requirements under section 15F

of the Exchange Act as applying at either the transaction-level or at the entity-level.⁴²¹ Transaction-level requirements under section 15F of the Exchange Act are those that primarily focus on protecting counterparties to security-based swap transactions by requiring SBSDs to, among other things, provide certain disclosures to counterparties, adhere to certain standards of business conduct, and segregate customer funds, securities, and other assets.⁴²² In contrast to transaction-level requirements, entity-level requirements under section 15F of the Exchange Act are those that are expected to play a role in ensuring the safety and soundness of the SBS Entity and thus relate to the entity as a whole.⁴²³ Entity-level requirements include capital and margin requirements, as well as other requirements relating to a firm’s identification and management of its risk exposure, including the risk management procedures required under section 15F(j) of the Exchange Act, a statutory basis for rules applicable to SBS Entities that the Commission is proposing in this release.⁴²⁴ Because these requirements relate to the entire entity, they apply to SBS Entities on a firm-wide basis, without exception.⁴²⁵

The Commission applied this taxonomy in 2016 when it adopted rules to implement business conduct standards for SBS Entities. At that time, the Commission also stated that the rules and regulations prescribed under section 15F(j) should be treated as entity-level requirements.⁴²⁶ The

⁴²¹ See *id.* at 31008–25. See also *Business Conduct Standards for Security-Based Swap Dealers and Major Security-Based Swap Participants*, Exchange Act Release No. 77617 (Apr. 14, 2016) [81 FR 29959, 30061–69 (May 13, 2016)] (“Business Conduct Standards Adopting Release”).

⁴²² Cross-Border Proposing Release, 78 FR at 31010.

⁴²³ See *id.* at 31011, 31035.

⁴²⁴ See *id.* at 31011–16 (addressing the classification of capital and margin requirements, as well as of the risk management requirements of section 15F(j) of the Exchange Act and other entity-level requirements applicable to SBSDs).

⁴²⁵ See *id.* at 31011, 31024–25. See also *id.* at 31035 (applying the analysis to MSBSPs). In reaching this conclusion, the Commission explained that it “preliminarily believes that entity-level requirements are core requirements of the Commission’s responsibility to ensure the safety and soundness of registered security based swap dealers,” and that “it would not be consistent with this mandate to provide a blanket exclusion to foreign security-based swap dealers from entity-level requirements applicable to such entities.” *Id.* at 31024 (footnotes omitted). The Commission further expressed the preliminary view that concerns regarding the application of entity-level requirements to foreign SBSDs would largely be addressed through the proposed approach to substituted compliance. See *id.*

⁴²⁶ See *Business Conduct Standards Adopting Release*, 81 FR at 30064–65.

⁴¹⁸ See Cross-Border Proposing Release, 78 FR at 30976, n. 48.

⁴¹⁹ Unless otherwise indicated, references to “Title VII” in this section of this release are to Subtitle B of Title VII of the Dodd-Frank Act.

⁴²⁰ See Cross-Border Proposing Release, 78 FR at 30975.

Commission has not, however, expressly addressed the entity-level treatment of the cybersecurity requirements under proposed Rule 10, except with regard to recordkeeping and reporting.⁴²⁷

2. Proposed Entity-Level Treatment

a. Proposal

Consistent with its approach to the obligations described in Section 15F(j) and to capital,⁴²⁸ margin,⁴²⁹ risk mitigation,⁴³⁰ and recordkeeping,⁴³¹ the Commission is proposing to apply the requirements of proposed Rule 10 to an SBS Entity's entire security-based swap business without exception, including in connection with any security-based swap business it conducts with foreign counterparties.⁴³²

Cybersecurity policies and procedures and the related requirements of proposed Rule 10 serve as an important mechanism for allowing SBS Entities and their counterparties to manage risks associated with their operations, including risks related to the entity's safety and soundness.⁴³³ An alternative approach that does not require an SBS Entity to take steps to manage cybersecurity risk throughout the firm's entire business could contribute to operational risk affecting the entity's security-based swap business as a whole, and not merely specific security-based swap transactions. Moreover, to the extent that these risks affect the safety and soundness of the SBS Entity, they also may affect the firm's counterparties and the functioning of

⁴²⁷ The Commission has previously stated that recordkeeping and reporting requirements are entity-level requirements. See *Recordkeeping and Reporting Requirements for Security-Based Swap Dealers, Major Security-Based Swap Participants, and Broker-Dealers*, Exchange Act Release No. 87005 (Sept. 19, 2019), 84 FR 68550, 68596–97 (Dec. 16, 2019) (“SBS Entity Recordkeeping and Reporting Adopting Release”).

⁴²⁸ See *Capital, Margin, and Segregation Requirements for Security-Based Swap Dealers and Major Security-Based Swap Participants and Capital and Segregation Requirements for Broker-Dealers*, Exchange Act Release No. 86175 (Jun. 21, 2019), 84 FR 43872, 43879 (Aug. 22, 2019) (“Capital, Margin, and Segregation Requirements Adopting Release”).

⁴²⁹ *Id.*

⁴³⁰ See *Risk Mitigation Techniques for Uncleared Security-Based Swaps*, Exchange Act Release No. 87782 (Dec. 18, 2019) [85 FR 6359, 6378 (Feb. 4, 2020)] (“SBS Entity Risk Mitigation Adopting Release”).

⁴³¹ See *SBS Entity Recordkeeping and Reporting Adopting Release*, 84 FR at 68596–97.

⁴³² As entity-level requirements, transaction-level exceptions such as in 17 CFR 3a71–3(c) and 17 CFR 3a67–10(d), would not be available for the proposed cybersecurity requirements.

⁴³³ See sections I.A. and II.B.1. of this release (discussing, respectively, cybersecurity risks and how those risks can be managed by certain policies, procedures, and controls). See also sections II.B.2–5 of this release.

the broader security-based swap market. Accordingly, the Commission proposes to apply the requirements to the entirety of an SBS Entity's business.⁴³⁴ However, as described below, the Commission is proposing that foreign SBS Entities have the potential to avail themselves of substituted compliance to satisfy the cybersecurity requirements under proposed Rule 10.

b. Request for Comment

The Commission generally requests comments on the proposed entity-level application of proposed Rule 10. In addition, the Commission requests comments on the following specific issues:

83. Does the proposed approach appropriately treat the proposed requirements as entity-level requirements applicable to the entire business conducted by foreign SBS Entities? If not, please identify any particular aspects of proposed Rule 10 that should not be applied to a foreign SBS Entity, or applied only to specific transactions, and explain how such an approach would be consistent with the goals of Title VII of the Dodd-Frank Act.

84. Should the Commission apply the same cross-border approach to the application of proposed Rule 10 for both SBSs and MSBSPs? If not, please describe how the cross-border approach for SBSs should differ from the cross-border approach for MSBSPs, and explain the reason(s) for any potential differences in approach.

⁴³⁴ The Commission has expressed the view that an entity that has registered with the Commission subjects itself to the entire regulatory system governing such registered entities. Cross-Border Proposing Release, 78 FR at 30986. See also *Business Conduct Standards Adopting Release*, 81 FR at n.1306 (determining that the requirements described in section 15F(j) of the Exchange Act should be treated as entity-level requirements, and stating that such treatment would not be tantamount to applying Title VII to persons that are “transact[ing] a business in security-based swaps without the jurisdiction of the United States,” within the meaning of section 30(c) of the Exchange Act). That treatment of section 15F(j) of the Exchange Act was also deemed necessary or appropriate as a prophylactic measure to help prevent the evasion of the provisions of the Exchange Act that were added by the Dodd-Frank Act, and thus help prevent the relevant purposes of the Dodd-Frank Act from being undermined. *Id.* (citing *Application of “Security-Based Swap Dealer” and “Major Security-Based Swap Participant” Definitions to Cross-Border Security-Based Swap Activities; Republication*, Exchange Act Release No. 72472 (June 25, 2014) [79 FR 47277, 47291–92 (Aug. 12, 2014)] (“SBS Entity Definitions Adopting Release”) (interpreting anti-evasion provisions of the Exchange Act, section 30(c)). A different approach in connection with proposed Rule 10 would not be consistent with the purposes of Title VII of the Dodd-Frank Act and could allow SBS Entities to avoid compliance with these proposed rules for portions of their business in a manner that could increase the risk to the registered entity.

85. What types of conflicts might a foreign SBS Entity face if it had to comply with proposed Rule 10 in more than one jurisdiction? In what situations would compliance with more than one of these requirements be difficult or impossible? For Market Entities that are U.S. persons, could compliance with the proposed rules create compliance challenges with requirements in a foreign jurisdiction?

86. As an alternative to treating the proposed requirements as entity-level requirements, should the Commission instead treat the proposed requirements as transaction-level requirements? If so, to which cross-border security-based swap transactions should these requirements apply and why? Please describe how these requirements would apply differently if classified as transaction-level requirements instead of as entity-level requirements.

3. Availability of Substituted Compliance

a. Existing Substituted Compliance Rule

In 2016,⁴³⁵ the Commission adopted Exchange Act Rule 3a71–6 (“Rule 3a71–6”)⁴³⁶ to provide that the Commission may, by order, make a determination that compliance with a specified requirements under a foreign financial regulatory system by non-U.S. SBS Entities⁴³⁷ may satisfy certain business conduct requirements under Exchange Act section 15F, subject to certain conditions. The rule in part provides that the Commission shall not make a determination providing for substituted compliance unless the Commission determines, among other things, that the foreign regulatory requirements are

⁴³⁵ See *Business Conduct Standards Adopting Release*, 81 FR at 30070–81. Separately, in 2015, the Commission adopted a rule making substituted compliance potentially available in connection with certain regulatory reporting and public dissemination requirements related to security-based swaps. See *Regulation SBSR-Reporting and Dissemination of Security-Based Swap Information*, Exchange Act Release No. 74244 (Feb. 11, 2015) [80 FR 14563 (Mar. 19, 2015)] (adopting 17 CFR 242.908 (“Rule 908”). Paragraph (c) of Rule 908 does not contemplate substituted compliance for the rules being proposing today.

⁴³⁶ See 17 CFR 240.3a71–6.

⁴³⁷ If the Commission makes a substituted compliance determination under paragraph (a)(1) of Rule 3a71–6, SBS Entities that are not U.S. persons (as defined in 17 CFR 240.3a71–3(a)(4) (“Rule 3a71–3(a)(4)”), but not SBS Entities that are U.S. persons, may satisfy specified requirements by complying with comparable foreign requirements and any conditions set forth in the substituted compliance determination made by the Commission. See paragraphs (b) and (d) of Rule 3a71–6.

comparable to otherwise applicable requirements.⁴³⁸

When the Commission adopted this substituted compliance rule that addressed the specified business conduct requirements, the Commission also noted that Exchange Act section 15F(j)(7) authorizes the Commission to prescribe rules governing the duties of SBS Entities.⁴³⁹ The Commission stated that it was not excluding that provision from the potential availability of substituted compliance, and that it expected to separately consider whether substituted compliance may be available in connection with any future rules promulgated pursuant to that provision.⁴⁴⁰ Further, the Commission stated that it expected to assess the potential availability of substituted compliance in connection with other requirements when the Commission considers final rules to implement those requirements.⁴⁴¹ Consistent with these statements, the Commission subsequently amended Rule 3a71–6 to provide SBS Entities that are non U.S. persons with the potential to avail themselves of substituted compliance with respect to the following Title VII requirements: (1) trade acknowledgment and verification,⁴⁴² (2) capital and margin requirements,⁴⁴³ (3) recordkeeping and reporting,⁴⁴⁴ and (4) portfolio reconciliation, portfolio compression, and trading relationship documentation.⁴⁴⁵

b. Proposed Amendment to Rule 3a71–6

The Commission is proposing to further amend Rule 3a71–6 to provide SBS Entities that are not U.S. persons (as defined in Rule 3a71–3(a)(4) of the Exchange Act) with the potential to avail themselves of substituted compliance to satisfy the cybersecurity requirements of proposed Rule 10 and Form SCIR as applicable to SBS

⁴³⁸ See paragraph (a)(2) of 3a71–6. See also Business Conduct Standards Adopting Release, 81 FR at 30074.

⁴³⁹ Business Conduct Standards Adopting Release, 81 FR at n. 1438.

⁴⁴⁰ *Id.*

⁴⁴¹ See Business Conduct Standards Adopting Release, 81 FR at 30074.

⁴⁴² See *Trade Acknowledgment and Verification of Security-Based Swap Transactions*, Exchange Act Release No. 78011 (Jun. 8, 2016) [81 FR 39807, 39827–28 (Jun. 17, 2016)] (“SBS Entity Trade Acknowledgment and Verification Adopting Release”).

⁴⁴³ See *Capital, Margin, and Segregation Requirements* Adopting Release, 84 FR at 43948–50.

⁴⁴⁴ See *SBS Entity Recordkeeping and Reporting* Adopting Release, 84 FR at 68597–99.

⁴⁴⁵ See *SBS Entity Risk Mitigation* Adopting Release, 85 FR at 6379–80.

Entities.⁴⁴⁶ In proposing to amend the rule, the Commission preliminarily believes that the principles associated with substituted compliance, as previously adopted in connection with both the business conduct requirements and the recordkeeping and reporting requirements, in large part should similarly apply to the cybersecurity risk management requirements being proposing today. The discussions in the Business Conduct Standards Adopting Release, including for example those regarding consideration of supervisory and enforcement practices,⁴⁴⁷ certain multi-jurisdictional issues,⁴⁴⁸ and application procedures⁴⁴⁹ are applicable to the proposed cybersecurity requirements. Accordingly, the proposed substituted compliance rule would apply to the cybersecurity risk management requirements in the same manner as it already applies to existing business conduct requirements and the recordkeeping and reporting requirements.

Making substituted compliance available for the cybersecurity risk management requirements would be consistent with the approach the Commission has taken with other rules applicable to SBS Entities. This approach takes into consideration the global nature of the security-based swap market and the prevalence of cross-border transactions within that market.⁴⁵⁰ The application of the cybersecurity risk management requirements may lead to requirements that are duplicative of, or in conflict with, applicable foreign requirements, even when the two sets of requirements implement similar goals and lead to similar results. Those results have the potential to disrupt existing business relationships and, more generally, to reduce competition and market efficiency. To address those effects, under certain circumstances it may be appropriate to allow the possibility of substituted compliance, whereby non-U.S. market participants may satisfy the cybersecurity risk management requirements by complying with

⁴⁴⁶ Substituted compliance would only be available to eligible SBS Entities. For example, substituted compliance would not be available to a Market Entity registered as both an SBS Entity and a broker-dealer with respect to the broker-dealer’s obligations under the proposed rules.

⁴⁴⁷ Business Conduct Standards Adopting Release, 81 FR at 30079.

⁴⁴⁸ Business Conduct Standards Adopting Release, 81 FR at 30079–80.

⁴⁴⁹ Business Conduct Standards Adopting Release, 81 FR at 30080–81.

⁴⁵⁰ See generally *Business Conduct Standards* Adopting Release, 81 FR at 30073–74 (addressing the basis for making substituted compliance available in the context of the business conduct requirements).

comparable foreign requirements. Allowing for the possibility of substituted compliance in this manner would help achieve the benefits of those particular requirements in a way that helps avoid regulatory conflict and minimizes duplication, thereby promoting market efficiency, enhancing competition, and contributing to the overall functioning of the global security-based swap market.

Accordingly, the Commission is proposing to amend paragraph (d)(1) of Rule 3a71–6 to make substituted compliance available for proposed Rule 10 and Form SCIR if the Commission determines with respect to a foreign financial regulatory system that compliance with specified requirements under such foreign financial regulatory system by a registered SBS Entity, or class thereof, satisfies the corresponding requirements of proposed Rule 10 and Form SCIR.⁴⁵¹ However, the proposal would not amend Rule 3a71–6 in connection with the proposed amendments to Rule 18a–6 regarding records to be preserved by certain SBS Entities. Rule 3a71–6 currently permits eligible applicants to seek a substituted compliance determination from the Commission with regard to the requirements of Rule 18a–6.⁴⁵²

c. Comparability Criteria, and Consideration of Related Requirements

If adopted, the proposed amendment to paragraph (d)(1) of Rule 3a71–6 would provide that eligible applicants may request that the Commission make a substituted compliance determination with respect to one or more of the requirements Rule 10 and Form SCIR.⁴⁵³ Further, existing paragraph (d)(6) of Rule 3a71–6 would permit eligible applicants to request that the Commission make a substituted compliance determination with respect to one or more of the requirements of the proposed amendments to Rule 18a–6, if adopted. A positive substituted compliance determination with respect to requirements existing before adoption of the proposed Rule 10, Form SCIR, and the related record preservation requirements would not automatically result in a positive substituted compliance determination with respect

⁴⁵¹ Paragraph (a)(1) of Rule 3a71–6 provides that the Commission may, conditionally or unconditionally, by order, make a determination with respect to a foreign financial regulatory system that compliance with specified requirements under the foreign financial system by an SBS Entity, or class thereof, may satisfy the corresponding requirements identified in paragraph (d) of the rule that would otherwise apply. See section II.D.3.c. of this release.

⁴⁵² See paragraph (d)(6) of Rule 3a71–6.

⁴⁵³ See paragraph (c) of Rule 3a71–6.

to proposed Rule 10, Form SCIR or the proposed amendments to Rule 18a–6. Before making a substituted compliance determination, the substance of each foreign regulatory system to which substituted compliance would apply should be evaluated for comparability to such newly adopted requirements. As such, if the Commission adopts the proposed amendment to Rule 3a71–6, eligible applicants⁴⁵⁴ seeking a Commission determination permitting SBS Entities that are not U.S. persons to satisfy the requirements of proposed Rule 10, Form SCIR, or the proposed amendments to Rule 18a–6 by complying with comparable foreign requirements would be required to file an application, pursuant to the procedures set forth in 17 CFR 240.0–13, requesting that the Commission make a such a determination pursuant to 17 CFR 3a71–6(a)(1).⁴⁵⁵

The Commission has taken a holistic approach in determining the comparability of foreign requirements for substituted compliance purposes, focusing on regulatory outcomes as a whole, rather than on a requirement-by-requirement comparison.⁴⁵⁶ The Commission preliminarily believes that such a holistic approach would be appropriate for determining comparability for substituted compliance purposes in connection with the requirements of proposed Rule 10, Form SCIR, and the proposed amendments to Rule 18a–6. Under the proposed amendment to Rule 3a71–6, the Commission’s comparability assessments associated with the proposed cybersecurity risk management requirements accordingly would consider whether, in the Commission’s view, the foreign regulatory system achieves regulatory

outcomes that are comparable to the regulatory outcomes associated with those requirements. Rule 3a71–6 provides that the Commission’s substituted compliance determination will take into account factors that the Commission determines appropriate, such as, for example, the scope and objectives of the relevant foreign regulatory requirements (taking into account the applicable criteria set forth in paragraph (d) of the rule), as well as the effectiveness of the supervisory compliance program administered, and the enforcement authority exercised, by a foreign financial regulatory authority or authorities in such foreign financial regulatory system to support its oversight of the SBS Entity (or class thereof) or of the activities of such SBS Entity (or class thereof).⁴⁵⁷

The Commission may determine to conduct its comparability analyses regarding Rule 10, Form SCIR, and the related record preservation requirements in conjunction with comparability analyses regarding other Exchange Act requirements that, like the requirements being proposed today, relate to risk management, recordkeeping, reporting, and notification requirements of SBS Entities. If the Commission adopts the proposed amendment to Rule 3a71–6, substituted compliance requests related to Rule 10, Form SCIR, and the related record preservation requirements may be filed by (i) applicants filing a request for a substituted compliance determination solely in connection with Rule 10, Form SCIR, and the related record preservation requirements,⁴⁵⁸ and (ii) applicants filing a request for a substituted compliance determination in connection with Rule 10, Form SCIR, and the related record preservation requirements combined with a request for a substituted compliance determination related to other eligible requirements. In either event, depending on the applicable facts and circumstances, the Commission’s comparability assessment associated with the Rule 10, Form SCIR, or the related record preservation requirements may constitute part of a broader assessment of Exchange Act risk management, recordkeeping, reporting, and notification requirements for SBS Entities, and the applicable comparability decisions may be made at the level of those risk management,

recordkeeping, reporting, and notification requirements for SBS Entities as a whole.

d. Request for Comment

The Commission generally requests comments on all aspects of the proposed amendment to Rule 3a71–6 and proposed availability of substituted compliance. In addition, the Commission requests comments on the following specific issues:

87. Should the Commission make substituted compliance available with respect to proposed Rule 10, Form SCIR, and the related record preservation requirements? Why or why not? If you believe that substituted compliance should not be available with respect to these requirements, how would you distinguish this policy decision from the Commission’s previous determination to make substituted compliance potentially available with respect to other Title VII requirements (*i.e.*, the business conduct, trade acknowledgment and verification, capital and margin, recordkeeping and reporting, and portfolio reconciliation, portfolio compression, and trading relationship documentation rules)?

88. Are there other aspects of the scope of the substituted compliance rule for which the Commission should amend or provide additional guidance in light of proposed Rule 10, Form SCIR, and the proposed amendment to Rule 18a–6? If so, what other amendments or additional guidance would be appropriate and why?

89. Are the items identified in Rule 3a71–6 as factors the Commission will consider prior to making a substituted compliance determination in connection with proposed Rule 10, Form SCIR, and the related record preservation requirements appropriate? If so, explain why. If not, explain why not. Should any of those items be modified or deleted? Should additional considerations be added? If so, please explain.

E. Amendments to Rule 18a–10

1. Proposal

Exchange Act Rule 18a–10 (“Rule 18a–10”) permits an SBS that is registered as a swap dealer and predominantly engages in a swaps business to elect to comply with the capital, margin, segregation, recordkeeping, and reporting requirements of the Commodity Exchange Act and the CFTC’s rules in lieu of complying with the capital, margin, segregation, recordkeeping, and reporting requirements of Exchange Act Rules 18a–1, 18a–3, 18a–4, 18a–5, 18a–

⁴⁵⁴ See 17 CFR 3a71–6(c).

⁴⁵⁵ Existing Commission substituted compliance determinations do not address the requirements of the proposed new rules or the proposed amendments. If the Commission adopts the requirements in the proposed new or amended rules, SBS Entities (or the relevant foreign financial regulatory authority or authorities) seeking a substituted compliance determination with respect to those requirements would be required to file an application requesting that the Commission make the determination. Applicants may not request that the Commission make a substituted compliance determination related to the new requirements by amending a previously filed application that requested a substituted compliance determination related to other Commission requirements. However, new applications may incorporate relevant information from the applicant’s previously filed requests for substituted compliance determinations if the information remains accurate.

⁴⁵⁶ See Business Conduct Standards Adopting Release, 81 FR at 30078–79. See also SBS Entity Trade Acknowledgment and Verification Adopting Release, 81 FR at 39828; SBS Entity Recordkeeping and Reporting Adopting Release, 84 FR at 68598–99.

⁴⁵⁷ See 17 CFR 240.3a71–6(a)(2)(i).

⁴⁵⁸ This category of applicants would include those who previously filed requests for the Commission to make substituted compliance determinations related to other requirements eligible for substituted compliance determinations under Rule 3a71–6.

6, 18a–7, 18a–8, and 18a–9.⁴⁵⁹ An SBSB may elect to operate pursuant to Rule 18a–10 if it meets certain conditions.⁴⁶⁰ First, the firm must be registered with the Commission as a stand-alone SBSB (*i.e.*, not also registered as a broker-dealer or an OTC derivatives dealer) and registered with the CFTC as a swap dealer. Second, the firm must be exempt from the segregation requirements of Rule 18a–4. Third, the aggregate gross notional amount of the firm’s outstanding security-based swap positions must not exceed the lesser of two thresholds as of the most recently ended quarter of the firm’s fiscal year.⁴⁶¹ The thresholds are: (1) a maximum fixed-dollar gross notional amount of open security-based swaps of \$250 billion;⁴⁶² and (2) 10% of the combined aggregate gross notional amount of the firm’s open security-based swap and swap positions.

As discussed above, Rule 18a–6 is proposed to be amended to require SBSBs to maintain and preserve the records required to be made pursuant to proposed Rule 10.⁴⁶³ However, because Rule 18a–6 is within the scope of Rule 18a–10, an SBSB operating pursuant to Rule 18a–10 would not be subject to the maintenance and preservation requirements of Rule 18a–6 with respect to the records required to be made pursuant to proposed Rule 10. Therefore, while an SBSB would be subject to proposed Rule 10 and need to make these records, the firm would not need to maintain or preserve them in accordance with Rule 18a–6. For these reasons, the Commission is proposing to amend Rule 18a–10 to exclude from its scope the record maintenance and preservation requirements of Rule 18a–6 as they pertain to the records required to be made pursuant to proposed Rule 10.⁴⁶⁴ Therefore, the records required to be made pursuant to proposed Rule 10 would need to be preserved and

maintained in accordance with Rule 18a–6, as it is proposed to be amended.

2. Request for Comment

The Commission requests comment on all aspects of the proposed amendments relating to Rule 18a–10. In addition, the Commission is requesting comment on the following specific aspects of the proposals:

90. Should the proposed amendments to Rule 18a–10 be modified? If so, describe how and explain why the modification would be appropriate. For example, would the records required to be made pursuant to proposed Rule 10 be subject to CFTC record preservation and maintenance rules? If so, identify the rules and explain the preservation and maintenance requirements they would impose on the records required to be made pursuant to proposed Rule 10. In addition, explain whether it would be appropriate to permit an SBSB operating pursuant to Rule 18a–10 to comply with these CFTC rules in terms of preserving and maintaining the records required to be made pursuant to proposed Rule 10 in lieu of the complying with the preservation and maintenance requirements that would apply to the records under the proposed amendments to Rule 18a–6.

F. Market Entities Subject to Regulation SCI, Regulation S–P, Regulation ATS, and Regulation S–ID

1. Discussion

a. Introduction

As discussed in more detail below, certain types of Market Entities are subject to Regulation SCI and Regulation S–P.⁴⁶⁵ The Commission separately is proposing to amend Regulation SCI and Regulation S–P.⁴⁶⁶ Regulation SCI and Regulation S–P (currently and as they would be amended) have or would have provisions requiring policies and procedures that address certain types of cybersecurity risks.⁴⁶⁷ Regulation SCI (currently and as it would be amended) also requires immediate written or telephonic notice and subsequent reporting to the Commission on Form

SCI of certain types of incidents.⁴⁶⁸ These notification and subsequent reporting requirements of Regulation SCI could be triggered by a “significant cybersecurity incident” as that term would be defined in proposed Rule 10.⁴⁶⁹ Finally, Regulation SCI and Regulation S–P (currently and as they would be amended) have or would have provisions requiring disclosures to persons affected by certain incidents.⁴⁷⁰ These current or proposed disclosure requirements of Regulation SCI and Regulation S–P could be triggered by a cybersecurity-related event that also would be a “significant cybersecurity incident” as that term would be defined in proposed Rule 10.⁴⁷¹ Consequently, if proposed Rule 10 is adopted (as proposed), Market Entities could be subject to requirements in that rule and in Regulation SCI and Regulation S–P that pertain to cybersecurity. While the Commission preliminarily believes that these requirements are nonetheless appropriate, it is seeking comment on the proposed amendments, given the following: (1) each proposal has a different scope and purpose; (2) the policies and procedures related to cybersecurity that would be required under each of the proposed rules would be consistent; (3) the public disclosures or notifications required by the proposed rules would require different types of information to be disclosed, largely to different audiences at different times; and (4) it should be appropriate for entities to comply with the proposed requirements.

The Commission encourages interested persons to provide comments on the discussion below, as well as on the potential related application of proposed Rule 10, Regulation SCI, and Regulation S–P. More specifically, the Commission encourages commenters: (1) to identify any areas where they believe the requirements of proposed Rule 10 and the existing or proposed requirements of Regulation SCI and Regulation S–P would be particularly costly or create practical implementation difficulties; (2) to provide details on what in particular about implementation would be difficult; and (3) to make

⁴⁵⁹ See 17 CFR 240.18a–10.

⁴⁶⁰ See Capital, Margin, and Segregation Requirements Adopting Release, 84 at 43944–46 (discussing the conditions and the reasons for them). See also SBS Entity Recordkeeping and Reporting Adopting Release, 84 FR at 68549.

⁴⁶¹ The gross notional amount is based on the notional amounts of the firm’s security-based swaps and swaps that are outstanding as of the quarter end. It is not based on transaction volume during the quarter.

⁴⁶² The maximum fixed-dollar threshold of \$250 billion is set for a transition period of 3 years from the compliance date of the rule. Three years after that date it will drop to \$50 billion (unless the Commission issues an order retaining the \$250 billion threshold or lesser amount that is greater than \$50 billion).

⁴⁶³ See section II.B.5. of this release (discussing these proposals in more detail).

⁴⁶⁴ See proposed paragraph (g) of Rule 18a–10.

⁴⁶⁵ See 17 CFR 242.1000 through 1007 (Regulation SCI); 17 CFR 248.1 through 248.30 (Regulation S–P). See also section II.F.1.b. of this release (discussing the types of Market Entities that are or would be subject to Regulation SCI and/or Regulation S–P).

⁴⁶⁶ See Regulation SCI 2023 Proposing Release; Regulation S–P 2023 Proposing Release.

⁴⁶⁷ See section II.F.1.c. of this release (discussing the existing and proposed requirements of Regulation SCI and Regulation S–P to have policies and procedures that address certain cybersecurity risks).

⁴⁶⁸ See section II.F.1.d. of this release (discussing the existing and proposed immediate notification and subsequent reporting requirements of Regulation SCI).

⁴⁶⁹ See paragraph (a)(10) of proposed Rule 10 (defining the term “significant cybersecurity incident”).

⁴⁷⁰ See section II.F.1.e. of this release (discussing the existing and proposed disclosure requirements of Regulation SCI and Regulation S–P).

⁴⁷¹ See paragraph (a)(10) of proposed Rule 10 (defining the term “significant cybersecurity incident”).

recommendations on how to minimize these potential impacts. To assist this effort, the Commission is seeking specific comment below on these topics.⁴⁷²

b. Market Entities That Are or Would Be Subject to Regulation SCI and Regulation S–P

Certain Market Entities that would be subject to the requirements of proposed Rule 10 applicable to Covered Entities are subject to the existing requirements of Regulation SCI. In particular, SCI entities include the following Covered Entities that also would be subject to the requirements of proposed Rule 10: (1) ATs that trade certain stocks exceeding specific volume thresholds; (2) registered clearing agencies; (3) certain exempt clearing agencies; (4) the MSRB; (5) FINRA; and (6) national securities exchanges.⁴⁷³ Therefore, if proposed Rule 10 is adopted (as proposed), these Covered Entities would be subject to its requirements and the requirements of Regulation SCI (currently and as it would be amended). The Commission is separately proposing to revise Regulation SCI to expand the definition of “SCI entity” to include the following Covered Entities that also would be subject to the requirements of proposed Rule 10: (1) broker-dealers that exceed an asset-based size threshold or a volume-based trading threshold in NMS stocks, exchange-listed options, agency securities, or U.S. treasury securities; (2) *all* exempt clearing agencies; and (3) SBSDRs.⁴⁷⁴ Therefore, if these

amendments to Regulation SCI are adopted and proposed Rule 10 is adopted (as proposed), these additional Covered Entities would be subject to the requirements of proposed Rule 10 and also to the requirements of Regulation SCI. Additionally, broker-dealers and transfer agents that would be subject to proposed Rule 10 also would be subject to some or all of the existing or proposed requirements of Regulation S–P.⁴⁷⁵

c. Policies and Procedures to Address Cybersecurity Risks

i. Different Scope and Purpose of the Policies and Procedures Requirements

Each of the policies and procedures requirements has a different scope and purpose. Regulation SCI (currently and as it would be amended) limits the scope of its requirements to certain systems of the SCI Entity that support securities market related functions. Specifically, it does and would require an SCI Entity to have reasonably designed policies and procedures applicable to its SCI systems and, for purposes of security standards, its indirect SCI systems.⁴⁷⁶ While certain

\$50 million, have total assets equal to or exceeding \$1 billion, or operate as a market maker. See paragraphs (a)(1)(i)(A), (C), (D), and (E) of proposed Rule 10. The Commission is seeking comment above on whether a broker-dealer that is an SCI entity should be defined specifically as a “covered entity” under proposed Rule 10.

⁴⁷⁵ Broadly, Regulation S–P’s requirements apply to all broker-dealers, except for “notice-registered broker-dealers” (as defined in 17 CFR 248.30), who in most cases will be deemed to be in compliance with Regulation S–P if they instead comply with the financial privacy rules of the CFTC, and are otherwise explicitly excluded from certain of Regulation S–P’s obligations. See 17 CFR 248.2(c). For the purposes of this section I.F. of this release, the term “broker-dealer” when used to refer to broker-dealers that are subject to Regulation S–P (currently and as it would be amended) excludes notice-registered broker-dealers. Currently, transfer agents registered with the Commission (“SEC-registered transfer agents”) (but not transfer agents registered with another appropriate regulatory agency) are subject to Regulation S–P’s “disposal rule” (“Regulation S–P Disposal Rule”). See 17 CFR 248.30(b). However, no transfer agent is currently subject to any other portion of Regulation S–P, including the “safeguards rule” under Regulation S–P (“Regulation S–P Safeguards Rule”). See 17 CFR 248.30(a). Under the proposed amendments to Regulation S–P, SEC-registered transfer agents and transfer agents registered with another appropriate regulatory agency (as defined in 15 U.S.C. 78c(34)(B)) would be subject to the Regulation S–P Safeguards Rule and the Regulation S–P Disposal Rule. Regulation S–P also applies to additional financial institutions that would not be subject to proposed Rule 10. See 17 CFR 248.3.

⁴⁷⁶ See 17 CFR 242.1001(a)(1). “SCI systems” are defined as electronic or similar systems of, or operated by or on behalf of, an SCI entity that directly support at least one of six market functions: (1) trading; (2) clearance and settlement; (3) order routing; (4) market data; (5) market regulation; or (6) market surveillance. 17 CFR 242.1000. “Indirect SCI systems” are defined as those of, or operated by or

aspects of the policies and procedures required by Regulation SCI (as it exists today and as proposed to be amended) are designed to address certain cybersecurity risks (among other things),⁴⁷⁷ the policies and procedures required by Regulation SCI focus on the SCI entities’ operational capability and the maintenance of fair and orderly markets.

Similarly, Regulation S–P (currently and as it would be amended) also has a distinct focus. The policies and procedures required under Regulation S–P, both currently and as proposed to be amended, are limited to protecting a certain type of information—customer records or information and consumer report information⁴⁷⁸—and they apply to such information even when stored outside of SCI systems or indirect SCI systems. Furthermore, these policies and procedures need not address other types of information stored on the systems of the broker-dealer or transfer agent.

Proposed Rule 10 would have a broader scope than Regulation SCI and Regulation S–P (currently and as they would be amended) because it would require Market Entities to establish, maintain, and enforce written policies

on behalf of, an SCI entity that, if breached, would be reasonably likely to pose a security threat to SCI systems. 17 CFR 242.1000. The distinction between SCI systems and indirect SCI systems seeks to encourage SCI Entities that their SCI systems, which are core market-facing systems, should be physically or logically separated from systems that perform other functions (e.g., corporate email and general office systems for member regulation and recordkeeping). See *Regulation Systems Compliance and Integrity*, Release No. 34–73639 79 FR 72251 (Dec. 5, 2014), at 79 FR at 72279–81 (“Regulation SCI 2014 Adopting Release”). Indirect SCI systems are subject to Regulation SCI’s requirements with respect to security standards. Further, “critical SCI systems” (a subset of SCI systems) are defined as those that directly support functionality relating to: (1) clearance and settlement systems of clearing agencies; (2) openings, reopenings, and closings on the primary listing market; (3) trading halts; (4) initial public offerings; (5) the provision of market data by a plan processor; or (6) exclusively-listed securities; and as a catchall, systems that provide functionality to the securities markets for which the availability of alternatives is significantly limited or nonexistent and without which there would be a material impact on fair and orderly markets. 17 CFR 242.1000.

⁴⁷⁷ See 17 CFR 242.1000 (defining “indirect SCI systems”). The distinction between SCI systems and indirect SCI systems seeks to encourage SCI Entities that their SCI systems, which are core market-facing systems, should be physically or logically separated from systems that perform other functions (e.g., corporate email and general office systems for member regulation and recordkeeping). See *Regulation SCI 2014 Adopting Release*, 79 FR at 72279–81. Indirect SCI systems are subject to Regulation SCI’s requirements with respect to security standards.

⁴⁷⁸ Or as proposed herein, “customer information” and “consumer information.” See proposed rules 248.30(e)(5) and (e)(1), respectively.

⁴⁷² See section I.F.2. of this release.

⁴⁷³ See 17 CFR 242.1000 (defining the terms “SCI alternative trading system,” “SCI self-regulatory system,” and “Exempt clearing agency subject to ARP,” and including all of those defined terms in the definition of “SCI Entity”). The definition of “SCI entities” includes additional Commission registrants that would not be subject to the requirements of proposed Rule 10: plan processors and SCI competing consolidators. However, the Commission is seeking comment on whether these registrants should be subject to the requirements of proposed Rule 10.

⁴⁷⁴ All exempt clearing agencies and SBSDRs would be subject to the requirements of proposed Rule 10 applicable to Covered Entities. See paragraphs (a)(1)(ii) and (vii) of proposed Rule 10 (defining these registrants as “covered entities”). Broker-dealers that exceed the asset-based size threshold under the proposed amendments to Regulation SCI (which would be several hundred billion dollars) also would be subject to the requirements of proposed Rule 10 applicable to Covered Entities, as they would exceed the \$1 billion total assets threshold in the broker-dealer definition of “covered entity.” See paragraph (a)(1)(i)(D) of proposed Rule 10. A broker-dealer that exceeds one or more of the volume-based trading thresholds under the proposed amendments to Regulation SCI likely would meet one of the broker-dealer definitions of “covered entity” in proposed Rule 10 given their size and activities. For example, it would either be a carrying broker-dealer, have regulatory capital equal to or exceeding

and procedures that are reasonably designed to address their cybersecurity risks.⁴⁷⁹ Unlike Regulation SCI, these requirements would therefore cover SCI systems, indirect SCI systems, and information systems that are not SCI systems or indirect SCI systems. And, unlike Regulation S–P, the proposed requirements would also encompass information beyond customer information and consumer information.

To illustrate, a Market Entity could use one comprehensive set of policies and procedures to satisfy the requirements of proposed Rule 10 and the existing and proposed cybersecurity-related requirements of Regulation SCI and Regulation S–P, so long as: (1) the cybersecurity-related policies and procedures required under Regulation S–P and Regulation SCI fit within and are consistent with the scope of the policies and procedures required under proposed Rule 10; and (2) and the policies and procedures requirements of proposed Rule 10 also address the more narrowly-focused existing and proposed cybersecurity-related policies and procedures requirements under Regulation SCI and Regulation S–P.

ii. Consistency of the Policies and Procedures Requirements

Covered Entities

As discussed above, the Market Entities that would be SCI Entities under the existing and proposed requirements of Regulation SCI would be subject to the policies and procedures requirements of proposed Rule 10 applicable to Covered Entities. In addition, broker-dealers and transfer agents are subject to the requirements of Regulation S–P (currently and as it would be amended).⁴⁸⁰ Transfer agents would be Covered Entities under proposed Rule 10 and, therefore, subject to the policies and procedures requirements of that rule applicable to Covered Entities.⁴⁸¹ Further, the two categories of broker-dealers that likely would have the largest volume of customer information and consumer information subject to the existing or proposed requirements of Regulation S–

P would be Covered Entities under proposed Rule 10: carrying broker-dealers and introducing broker-dealers.⁴⁸² For these reasons, the Commission first analyzes the potential overlap between proposed Rule 10 and the current and proposed requirements of Regulation SCI and Regulation S–P by taking into account the policies and procedures requirements of proposed Rule 10 that would apply to Covered Entities.

Regulation SCI and Regulation S–P General Policies and Procedures Requirements

Regulation SCI, Regulation S–P, and proposed Rule 10 all include requirements that address certain cybersecurity-related risks. Regulation SCI requires an SCI Entity to have reasonably designed policies and procedures to ensure that its SCI systems and, for purposes of security standards, indirect SCI systems, have levels of capacity, integrity, resiliency, availability, and security, adequate to maintain the SCI entity's operational capability and promote the maintenance of fair and orderly markets.⁴⁸³

The Regulation S–P Safeguards Rule requires broker-dealers (but not transfer agents) to adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information.⁴⁸⁴ The Regulation S–P Safeguards Rule further provides that these policies and procedures must: (1) insure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (3) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.⁴⁸⁵ Additionally, the Regulation S–P Disposal Rule requires broker-dealers and SEC-registered transfer agents that maintain or otherwise possess consumer report information for a business purpose to properly dispose of the information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.⁴⁸⁶

⁴⁸² See paragraphs (a)(1)(i)(A) and (B) of proposed Rule 10 (defining, respectively, carrying broker-dealers and introducing broker-dealers as Covered Entities).

⁴⁸³ See 17 CFR 242.1001(a)(1).

⁴⁸⁴ See 17 CFR 248.30(a).

⁴⁸⁵ See 17 CFR 248.30(a)(1) through (3).

⁴⁸⁶ See 17 CFR 248.30(b)(2). Regulation S–P currently defines the term “disposal” to mean: (1) the discarding or abandonment of consumer report

Proposed Rule 10 would require a Covered Entity to establish, maintain, and enforce written policies and procedures that are reasonably designed to address the Covered Entity's cybersecurity risks. In addition, Covered Entities would be required to include the following elements in their policies and procedures: (1) periodic assessments of cybersecurity risks associated with the Covered Entity's information systems and written documentation of the risk assessments; (2) controls designed to minimize user-related risks and prevent unauthorized access to the Covered Entity's information systems; (3) measures designed to monitor the Covered Entity's information systems and protect the Covered Entity's information from unauthorized access or use, and oversight of service providers that receive, maintain, or process information, or are otherwise permitted to access the Covered Entity's information systems; (4) measures to detect, mitigate, and remediate any cybersecurity threats and vulnerabilities with respect to the Covered Entity's information systems; and (5) measures to detect, respond to, and recover from a cybersecurity incident and written documentation of any cybersecurity incident and the response to and recovery from the incident.⁴⁸⁷

As discussed earlier, the inclusion of these elements in proposed Rule 10 is designed to enumerate the core areas that Covered Entities would need to address when designing, implementing, and assessing their policies and procedures.⁴⁸⁸ Taken together, these requirements are designed to position Covered Entities to be better prepared to protect themselves against cybersecurity risks, to mitigate cybersecurity threats and vulnerabilities, and to recover from cybersecurity incidents. They are also designed to help ensure that Covered Entities focus their efforts and resources on the cybersecurity risks associated with their operations and business practices.

A Covered Entity that implements reasonably designed policies and procedures in compliance with the requirements of proposed Rule 10 described above that cover its SCI systems and indirect SCI systems should generally satisfy the existing general policies and procedures

information; or (2) the sale, donation, or transfer of any medium, including computer equipment, on which consumer report information is stored. See 17 CFR 248.30(b)(1)(iii).

⁴⁸⁷ See sections II.B.1.a. through II.B.1.e. of this release (discussing these proposed requirements in more detail).

⁴⁸⁸ See section II.B.1. of this release.

⁴⁷⁹ See paragraphs (b) and (e) of proposed Rule 10 (setting forth the requirements of Covered Entities and Non-Covered Entities, respectively, to have policies and procedures to address their cybersecurity risks).

⁴⁸⁰ As discussed above, SEC-registered transfer agents are subject to the Regulation S–P Disposal Rule but not to the Regulation S–P Safeguards Rule. The proposed amendments to Regulation S–P would apply the Regulation S–P Safeguards Rule and the Regulation S–P Disposal Rule to all transfer agents.

⁴⁸¹ See paragraph (b)(1) of proposed Rule 10 (setting forth the policies and procedures requirements for Covered Entities).

requirements of Regulation SCI that pertain to cybersecurity.⁴⁸⁹ Similarly, policies and procedures implemented by a Covered Broker-Dealer that are reasonably designed in compliance with the requirements of proposed Rule 10 should generally satisfy the existing general policies and procedures requirements of the Regulation S–P Safeguards Rule discussed above that pertain to cybersecurity, to the extent that such information is stored electronically and, therefore, falls within the scope of proposed Rule 10. In addition, reasonably designed policies and procedures implemented by a Covered Broker-Dealer or SEC-registered transfer agent in compliance with the requirements of proposed Rule 10 should generally satisfy the existing requirements of the Regulation S–P Disposal Rule discussed above.

Regulation SCI and Regulation S–P Requirements to Oversee Service Providers. Under the amendments to Regulation SCI, the policies and procedures required of SCI entities would need to include a program to manage and oversee third party providers that provide functionality, support or service, directly or indirectly, for SCI systems and indirect SCI systems.⁴⁹⁰ In addition, proposed amendments to the Regulation S–P Safeguards Rule would require broker-dealers and transfer agents to include written policies and procedures within their response programs that require their service providers, pursuant to a

written contract, to take appropriate measures that are designed to protect against unauthorized access to or use of customer information, including notification to the broker-dealer or transfer agent as soon as possible, but no later than 48 hours after becoming aware of a breach, in the event of any breach in security resulting in unauthorized access to customer information maintained by the service provider to enable the broker-dealer or transfer agent to implement its response program expeditiously.⁴⁹¹

Proposed Rule 10 would have several policies and procedures requirements that are designed to address similar cybersecurity risks as these proposed amendments to Regulation SCI and Regulation S–P. First, a Covered Entity's policies and procedures under proposed Rule 10 would need to require periodic assessments of cybersecurity risks associated with the Covered Entity's information systems and information residing on those systems.⁴⁹² This element of the policies and procedures would need to include requirements that the Covered Entity identify its service providers that receive, maintain, or process information, or are otherwise permitted to access its information systems and any of its information residing on those systems, and assess the cybersecurity risks associated with its use of these service providers.⁴⁹³ Second, under proposed Rule 10, a Covered Entity's policies and procedures would need to require oversight of service providers that receive, maintain, or process its information, or are otherwise permitted to access its information systems and the information residing on those systems, pursuant to a written contract between the Covered Entity and the service provider, through which the service providers would need to be required to implement and maintain appropriate measures that are designed to protect the Covered Entity's information systems and information residing on those systems.⁴⁹⁴

A Covered Entity that implements these requirements of proposed Rule 10 with respect to its SCI systems and indirect SCI systems generally should satisfy the proposed requirements of Regulation SCI that the SCI entity's policies and procedures include a

program to manage and oversee third party providers that provide functionality, support or service, directly or indirectly, for SCI systems and indirect SCI systems. Similarly, a broker-dealer or transfer agent that implements these requirements of proposed Rule 10 generally would comply with the proposed requirements of the Regulation S–P Safeguards Rule relating to the oversight of service providers.

Regulation SCI and Regulation S–P Unauthorized Access Requirements. Under the proposed amendments to Regulation SCI, SCI entities would be required to have a program to prevent the unauthorized access to their SCI systems and indirect SCI systems, and information residing therein.⁴⁹⁵ The proposed amendments to the Regulation S–P Disposal Rule would require broker-dealers and transfer agents that maintain or otherwise possess consumer information or customer information for a business purpose to properly dispose of this information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.⁴⁹⁶ The broker-dealer or transfer agent would be required to adopt and implement written policies and procedures that address the proper disposal of consumer information and customer information in accordance with this standard.⁴⁹⁷

Proposed Rule 10 would have several policies and procedures requirements that are designed to address similar cybersecurity-related risks as these proposed requirements of Regulation SCI and the Regulation S–P Disposal Rule. First, a Covered Entity's policies and procedures under proposed Rule 10 would need to require controls: (1) requiring standards of behavior for individuals authorized to access the Covered Entity's information systems and the information residing on those systems, such as an acceptable use policy; (2) identifying and authenticating individual users, including but not limited to implementing authentication measures that require users to present a combination of two or more credentials for access verification; (3) establishing procedures for the timely distribution,

⁴⁸⁹ As noted above, the CAT System is a facility of each of the Participants and an SCI system. See also CAT NMS Plan Approval Order, 81 FR at 84758. It would also qualify as an "information system" of each national securities exchange and each national securities association under proposed Rule 10. The CAT NMS Plan requires the CAT's Plan Processor to follow certain security protocols and industry standards, including the NIST Cyber Security Framework, subject to Participant oversight. See, e.g., CAT NMS Plan at appendix D, section 4.2. For the reasons discussed above and below with respect to SCI systems, the policies and procedures requirements of proposed Rule 10 are not intended to be inconsistent with the security protocols set forth in the CAT NMS Plan. Moreover, to the extent the CAT NMS Plan requires security protocols beyond those that would be required under proposed Rule 10, those additional security protocols should generally fit within and be consistent with the policies and procedures required under proposed Rule 10 to address all cybersecurity risks.

⁴⁹⁰ See Regulation SCI 2023 Proposing Release. These policies and procedures would need to include initial and periodic review of contracts with such vendors for consistency with the SCI entity's obligations under Regulation SCI; and a risk-based assessment of each third party provider's criticality to the SCI entity, including analyses of third party provider concentration, of key dependencies if the third party provider's functionality, support, or service were to become unavailable or materially impaired, and of any potential security, including cybersecurity, risks posed. *Id.*

⁴⁹¹ See Regulation S–P 2023 Proposing Release.

⁴⁹² See paragraph (b)(1)(i)(A) of proposed Rule 10; see also section II.B.1.a. of this release (discussing this requirement in more detail).

⁴⁹³ See paragraph (b)(1)(i)(A)(2) of proposed Rule 10.

⁴⁹⁴ See paragraphs (b)(1)(iii)(B) of proposed Rule 10; see also section II.B.1.c. of this release (discussing this requirement in more detail).

⁴⁹⁵ See Regulation SCI 2023 Proposing Release.

⁴⁹⁶ See Regulation S–P 2023 Proposing Release.

As discussed above, the general policies and procedures requirements of the Regulation S–P Safeguards Rule require the policies and procedures—among other things—to protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer. See 17 CFR 248.30(a)(3).

⁴⁹⁷ See Regulation S–P 2023 Proposing Release.

replacement, and revocation of passwords or methods of authentication; (4) restricting access to specific information systems of the Covered Entity or components thereof and the information residing on those systems solely to individuals requiring access to the systems and information as is necessary for them to perform their responsibilities and functions on behalf of the Covered Entity; and (5) securing remote access technologies.⁴⁹⁸

Second, under proposed Rule 10, a Covered Entity's policies and procedures would need to include measures designed to protect the Covered Entity's information systems and protect the information residing on those systems from unauthorized access or use, based on a periodic assessment of the Covered Entity's information systems and the information that resides on the systems.⁴⁹⁹ The periodic assessment would need to take into account: (1) the sensitivity level and importance of the information to the Covered Entity's business operations; (2) whether any of the information is personal information; (3) where and how the information is accessed, stored and transmitted, including the monitoring of information in transmission; (4) the information systems' access controls and malware protection; and (5) the potential effect a cybersecurity incident involving the information could have on the Covered Entity and its customers, counterparties, members, registrants, or users, including the potential to cause a significant cybersecurity incident.⁵⁰⁰

A Covered Entity that implements these requirements of proposed Rule 10 with respect to its SCI systems and indirect SCI systems generally should satisfy the proposed requirements of Regulation SCI that the SCI entity's policies and procedures include a program to prevent the unauthorized access to their SCI systems and indirect SCI systems, and information residing therein. Similarly, a broker-dealer or transfer agent that implements these requirements of proposed Rule 10 should generally satisfy the proposed requirements of the Regulation S-P Disposal Rule to adopt and implement written policies and procedures that address the proper disposal of consumer information and customer information.

⁴⁹⁸ See paragraphs (b)(1)(iii)(A) through (E) of proposed Rule 10; see also section II.B.1.b. of this release (discussing these requirements in more detail).

⁴⁹⁹ See paragraph (b)(1)(iii)(A) of proposed Rule 10; see also section II.B.1.c. of this release (discussing these requirements in more detail).

⁵⁰⁰ See paragraphs (b)(1)(iii)(A)(i) through (5) of proposed Rule 10.

Regulation SCI and Regulation S-P Response Programs. Regulation SCI requires SCI entities to have policies and procedures to monitor its SCI systems and indirect SCI systems for SCI events, which include systems intrusions for unauthorized access, and also requires them to have policies and procedures that include escalation procedures to quickly inform responsible SCI personnel of potential SCI events.⁵⁰¹

The amendments to Regulation S-P's safeguards provisions would require the policies and procedures to include a response program for unauthorized access to or use of customer information. Further, the response program would need to be reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information, including procedures, among others: (1) to assess the nature and scope of any incident involving unauthorized access to or use of customer information and identify the customer information systems and types of customer information that may have been accessed or used without authorization;⁵⁰² and (2) to take appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information.⁵⁰³

The amendments to the Regulation S-P Safeguards Rule would require the policies and procedures to include a response program for unauthorized access to or use of customer information. Further, the response program would need to be reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information, including procedures, among others: (1) to assess the nature and scope of any incident involving unauthorized access to or use of customer information and identify the customer information systems and types of customer information that may have been accessed or used without

⁵⁰¹ See 17 CFR 242.1001(a)(2)(vii) and (c)(1), respectively.

⁵⁰² Regulation SCI's obligation to take corrective action may include a variety of actions, such as determining the scope of the SCI event and its causes, among others. See Regulation SCI 2014 Adopting Release, 79 FR at 72251, 72317. See also 17 CFR 242.1002(a).

⁵⁰³ See Regulation S-P 2023 Proposing Release. The response program also would need to have procedures to notify each affected individual whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization unless the covered institution determines, after a reasonable investigation of the facts and circumstances of the incident of unauthorized access to or use of sensitive customer information, the sensitive customer information has not been, and is not reasonably likely to be, used in a manner that would result in substantial harm or inconvenience. See *id.*

authorization; and (2) to take appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information.⁵⁰⁴

Proposed Rule 10 would have several policies and procedures requirements that are designed to address similar cybersecurity-related risks as these proposed requirements of the Regulation S-P Safeguards Rule. First, under proposed Rule 10, a Covered Entity's policies and procedures would need to require measures designed to detect, mitigate, and remediate any cybersecurity threats and vulnerabilities with respect to the Covered Entity's information systems and the information residing on those systems.⁵⁰⁵ Second, under proposed Rule 10, a Covered Entity's policies and procedures would need to have measures designed to detect, respond to, and recover from a cybersecurity incident, including policies and procedures that are reasonably designed to ensure (among other things): (1) the continued operations of the Covered Entity; (2) the protection of the Covered Entity's information systems and the information residing on those systems; and (3) external and internal cybersecurity incident information sharing and communications.⁵⁰⁶

A Covered Entity that implements reasonably designed policies and procedures in compliance with these requirements of proposed Rule 10 generally should satisfy the proposed requirements of the Regulation SCI and Regulation S-P Safeguards Rule to have a response program relating to response programs for unauthorized access.

Regulation SCI Review Requirements. Regulation SCI currently prescribes certain elements that must be included in each SCI entity's policies and procedures.⁵⁰⁷ These required elements include policies and procedures that must provide for regular reviews and

⁵⁰⁴ See Regulation S-P 2023 Proposing Release. As discussed below, the response program also would need to have procedures to notify each affected individual whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization unless the covered institution determines, after a reasonable investigation of the facts and circumstances of the incident of unauthorized access to or use of sensitive customer information, the sensitive customer information has not been, and is not reasonably likely to be, used in a manner that would result in substantial harm or inconvenience. See *id.*

⁵⁰⁵ See paragraph (b)(1)(iv) of proposed Rule 10; see also section II.B.1.d. of this release (discussing this requirement in more detail).

⁵⁰⁶ See paragraph (b)(1)(v) of proposed Rule 10; see also section II.B.1.e. of this release (discussing this requirement in more detail).

⁵⁰⁷ See 17 CFR 242.1001(a)(2).

testing of SCI systems and indirect SCI systems, including backup systems, to identify vulnerabilities from internal and external threats.⁵⁰⁸ In addition, Regulation SCI requires SCI entities to conduct penetration tests as part of a review of their compliance with Regulation SCI.⁵⁰⁹ While these reviews must be conducted not less than once each calendar year, the penetration tests currently need to be conducted not less than once every three years.⁵¹⁰ The amendments to Regulation SCI would increase the required frequency of the penetration tests to not less than once each calendar year.⁵¹¹ The amendments to Regulation SCI also would require that the penetration tests include tests of any vulnerabilities of the SCI entity's SCI systems and indirect SCI systems identified under the existing requirement to perform regular reviews and testing of SCI systems and indirect SCI systems, including backup systems, to identify vulnerabilities from internal and external threats.⁵¹²

Proposed Rule 10 would have several policies and procedures requirements that are designed to address similar cybersecurity-related risks as these existing and proposed requirements of Regulation SCI. First, a Covered Entity's policies and procedures under proposed Rule 10 would need to require periodic assessments of cybersecurity risks associated with the Covered Entity's information systems and information residing on those systems.⁵¹³ Moreover, this element of the policies and procedures would need to include requirements that the Covered Entity categorize and prioritize cybersecurity risks based on an inventory of the components of the Covered Entity's information systems and information residing on those systems and the potential effect of a cybersecurity incident on the Covered Entity.⁵¹⁴ Second, under proposed Rule 10, a Covered Entity's policies and procedures would need to require measures designed to detect, mitigate, and remediate any cybersecurity threats and vulnerabilities with respect to the Covered Entity's information systems

and the information residing on those systems.⁵¹⁵

A Covered Entity that implements these requirements of proposed Rule 10 with respect to its SCI systems and indirect SCI systems generally should satisfy the current requirements of Regulation SCI that the SCI entity's policies and procedures require regular reviews and testing of SCI systems and indirect SCI systems, including backup systems, to identify vulnerabilities from internal and external threats.

Further, while proposed Rule 10 does not require penetration testing, the proposed rule—as discussed above—requires measures designed to protect the Covered Entity's information systems and protect the information residing on those systems from unauthorized access or use, based on a periodic assessment of the Covered Entity's information systems and the information that resides on the systems.⁵¹⁶ As discussed earlier, penetration testing could be part of these measures.⁵¹⁷ Therefore, the existing and proposed requirements of Regulation SCI requiring penetration testing could be incorporated into and should fit within a Covered Entity's policies and procedures to address cybersecurity risks under proposed Rule 10.

Non-Covered Broker-Dealers

Non-Covered Broker-Dealers—which would be subject to Regulation S-P but not Regulation SCI—are smaller firms whose functions do not play as significant a role in the U.S. securities markets, as compared to Covered Broker-Dealers.⁵¹⁸ For example, Non-Covered Broker-Dealers tend to offer a more focused and limited set of services such as facilitating private placements of securities, selling mutual funds and

variable contracts, underwriting securities, and participating in direct investment offerings.⁵¹⁹ Further, they do not hold customer securities and cash or serve as a conduit (*i.e.*, an introducing broker-dealer) for customers to access their accounts at a carrying broker-dealer that holds the customers' securities and cash. If these Non-Covered Broker-Dealers do not possess or maintain any customer information or consumer information for a business purpose in connection with the services they provide, they would not be subject to either the current or proposed requirements of Regulation S-P, including those that pertain to cybersecurity.

However, Non-Covered Broker-Dealers under proposed Rule 10 that do possess or maintain customer information or consumer information for a business purpose would be subject to the current and proposed requirements of Regulation S-P. Given their smaller size, some of these Non-Covered Broker-Dealers may store and dispose of the information in paper form and, therefore, under the existing and proposed requirements of Regulation S-P would need to address the physical security aspects of storing and disposing of this information. These paper records would not be subject to proposed Rule 10.

Some Non-Covered Broker-Dealers likely would store customer information and consumer information for a business purpose electronically on an information system. Under the existing and proposed requirements of Regulation S-P, these Non-Covered Broker-Dealers would need to address the cybersecurity risks of storing this information on an information system. These Non-Covered Broker-Dealers would be subject the requirements of proposed Rule 10 to establish, maintain, and enforce written policies and procedures that are reasonably designed to address their cybersecurity risks taking into account the size, business, and operations of the firm.⁵²⁰ Under proposed Rule 10, they also would be required to review and assess the design and effectiveness of their cybersecurity policies and procedures, including whether the policies and procedures reflect changes in cybersecurity risk over the time period covered by the

⁵¹⁵ See paragraph (b)(1)(iv) of proposed Rule 10; see also section II.B.1.d. of this release (discussing this requirement in more detail).

⁵¹⁶ See paragraph (b)(1)(iii)(A) of proposed Rule 10.

⁵¹⁷ See also section II.B.1.c. of this release. The Commission also is requesting comment above on whether proposed Rule 10 should be modified to specifically require penetration testing.

⁵¹⁸ See section IV.C.2. of this release (discussing the activities of broker-dealers that would not meet the definition of "covered entity" in proposed Rule 10). As discussed below in section IV.C.2. of this release, the 1,541 broker-dealers that would meet the definition of "covered entity" in proposed Rule 10 had average total assets of \$3.5 billion and average regulatory equity of \$325 million; whereas the 1,969 that would not meet the definition of "covered entity" had average total assets of \$4.7 million and regulatory equity of \$3 million. This means that broker-dealers that would not meet the definition of "covered entity" in proposed Rule 10 accounted for about 0.2% of the total assets of all broker-dealers and 0.1% of total capital for all broker-dealers.

⁵¹⁹ See section IV.C.2. of this release (discussing the activities of broker-dealers that would not meet the definition of "covered entity" in proposed Rule 10).

⁵²⁰ See paragraph (e) of proposed Rule 10 (setting forth the policies and procedures requirements for Market Entities that are not broker-dealers). See also section II.C. of this release (discussing these proposed requirements in more detail).

⁵⁰⁸ 17 CFR 242.1001(a)(2)(iv).

⁵⁰⁹ See 17 CFR 242.1003(b)(1)(i).

⁵¹⁰ *Id.*

⁵¹¹ See Regulation SCI 2023 Proposing Release.

⁵¹² See Regulation SCI 2023 Proposing Release; 17 CFR 242.1001(a)(2)(iv).

⁵¹³ See paragraph (b)(1)(i)(A) of proposed Rule 10; see also section II.B.1.a. of this release (discussing this requirement in more detail).

⁵¹⁴ See paragraph (b)(1)(i)(A)(1) of proposed Rule 10.

review. This means the Non-Covered Broker-Dealer would need to comprehensively address all of its cybersecurity risks. The policies and procedures to address cybersecurity risks required under proposed Rule 10 would need to address cybersecurity risks involving information systems on which customer information and consumer information is stored. Therefore, complying with this requirement of proposed Rule 10 would be consistent with complying with the existing and proposed requirements of Regulation S-P that relate to cybersecurity.

As discussed above, Regulation S-P (currently and as it would be amended) sets forth certain specific requirements that pertain to cybersecurity risk; whereas the requirements of proposed Rule 10 applicable to Non-Covered Broker-Dealers more generally require the firm to establish, maintain, and enforce written policies and procedures that are reasonably designed to address its cybersecurity risks taking into account the size, business, and operations of the firm. As explained above, those more specific existing and proposed requirements of Regulation S-P are consistent with certain of the elements—which are based on industry standards for addressing cybersecurity risk—that Covered Entities would be required to include in their policies and procedures under proposed Rule 10.⁵²¹ Further, proposed Rule 10 would require a Non-Covered Broker-Dealer to take into account its size, business, and operations when designing its policies and procedures to address its cybersecurity risks. Storing customer information and consumer information on an information system is the type of operation a Non-Covered Broker-Dealer would need to take into account. Consequently, the specific existing and proposed requirements of Regulation S-P should fit within and be consistent with a Non-Covered Broker-Dealer's reasonably designed policies and procedures to address its cybersecurity risks under proposed Rule 10, including the risks associated with storing customer information and consumer information on an information system.

iii. Regulation ATS and Regulation S-ID

Certain broker-dealers that operate an ATS are subject to Regulation ATS and certain broker-dealers that offer and maintain certain types of accounts for customers are subject to requirements of Regulation S-ID to establish an identity

theft program.⁵²² Additionally, SBS Entities and transfer agents could be subject to Regulation S-ID if they are “financial institutions” or “creditors.”⁵²³ As discussed below, Regulation ATS and Regulation S-ID are more narrowly focused on certain cybersecurity risks as compared to proposed Rule 10, which focuses on all cybersecurity risks of a Market Entity. In addition, the current requirements of Regulation ATS and Regulation S-ID should fit within and be consistent with the broader policies and procedures required under proposed Rule 10 to address all cybersecurity risks.

Regulation ATS requires certain broker-dealers that operate an ATS to review the vulnerability of its systems and data center computer operations to internal and external threats, physical hazards, and natural disasters if during at least four of the preceding six calendar months, such ATS had: (1) with respect to municipal securities, 20 percent or more of the average daily volume traded in the United States; or (2) with respect to corporate debt securities, 20 percent or more of the average daily volume traded in the United States.⁵²⁴ Therefore, in addition to other potential systems issues, the broker-dealer would need to address cybersecurity risk of relating to its ATS system. Further, this requirement applies to systems that support order entry, order handling, execution, order routing, transaction reporting, and trade comparison in the particular security.⁵²⁵ Therefore, it has a narrower focus than proposed Rule 10.

Regulation ATS also requires all broker-dealers that operate an ATS to establish adequate written safeguards and written procedures to protect subscribers' confidential trading information.⁵²⁶ The written safeguards and procedures must include, among other things, limiting access to the confidential trading information of subscribers to those employees of the

alternative trading system who are operating the system or responsible for its compliance with these or any other applicable rules.⁵²⁷ These requirements apply to all broker-dealers that operate an ATS and, as indicated, apply to a narrow set of information stored on their information systems: the confidential trading information of the subscribers to the ATS.

As discussed above, Covered Entities under proposed Rule 10—which would include broker-dealers that operate as an ATS—would be required to establish, maintain, and enforce written policies and procedures that are reasonably designed to address the Covered Entity's cybersecurity risks. In addition, Covered Entities would be required to include the following elements in their policies and procedures: (1) periodic assessments of cybersecurity risks associated with the Covered Entity's information systems and written documentation of the risk assessments; (2) controls designed to minimize user-related risks and prevent unauthorized access to the Covered Entity's information systems; (3) measures designed to monitor the Covered Entity's information systems and protect the Covered Entity's information from unauthorized access or use, and oversight of service providers that receive, maintain, or process information, or are otherwise permitted to access the Covered Entity's information systems; (4) measures to detect, mitigate, and remediate any cybersecurity threats and vulnerabilities with respect to the Covered Entity's information systems; and (5) measures to detect, respond to, and recover from a cybersecurity incident and written documentation. Consequently, a broker-dealer operates an ATS and that implements reasonably designed policies and procedures in compliance with the requirements of proposed Rule 10 should generally satisfy the current requirements of Regulation ATS to review the vulnerability of its systems and data center computer operations to internal and external threats and to protect subscribers' confidential trading information to the extent these requirements pertain to cybersecurity.

Regulation S-ID requires—among other things—a financial institution or creditor within the scope of the regulation that offers or maintains one or more covered accounts to develop and implement a written identity theft prevention program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing

⁵²² See 17 CFR 242.301 through 304 (conditions to the Regulation ATS exemption); 17 CFR 248.201 and 202 (Regulation S-ID identity theft program requirements).

⁵²³ See 17 CFR 248.201 and 202. The scope of Regulation S-ID includes any financial institution or creditor, as defined in the Fair Credit Reporting Act (15 U.S.C. 1681) that is required to be “registered under the Securities Exchange Act of 1934.” See 17 CFR 248.201(a).

⁵²⁴ See 17 CFR 242.301(b)(6). Currently, no ATS has crossed the either of the volume-based thresholds and, therefore, no ATS is subject to the requirements pertaining, in part, to cybersecurity. See also Amendments Regarding the Definition of “Exchange” and ATSs Release, 87 FR 15496.

⁵²⁵ See *Regulation of Exchanges and Alternative Trading Systems*, Exchange Act Release No. 40760 (Dec. 8, 1998) [63 FR 70844, 70876 (Dec. 22, 1998)].

⁵²⁶ See 17 CFR 242.301(b)(10).

⁵²⁷ See 17 CFR 242.301(b)(10)(i)(A).

⁵²¹ See section II.B.1. of this release (discussing the policies and procedures requirements for Covered Entities).

covered account.⁵²⁸ Regulation S-ID defines the term “covered account”—in pertinent part—as an account that the financial institution or creditor maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a brokerage account with a broker-dealer, and any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.⁵²⁹ Therefore, Regulation S-ID is narrowly focused on one cybersecurity risk—identity theft. Identity theft—as discussed earlier—is one of the tactics threat actors use to cause harm after obtaining unauthorized access to personal information.⁵³⁰ As a cybersecurity risk, Market Entities would need to address it as part of their policies and procedures under proposed Rule 10. Consequently, the requirement of Regulation S-ID should fit within and be consistent with a Market Entity’s reasonably designed policies and procedures to address its cybersecurity risks under proposed Rule 10, including the risks associated with identity theft.

d. Notification and Reporting to the Commission

Regulation SCI (currently and as it would be amended) provides the framework for notifying the Commission of SCI events including, among other things, to: immediately notify the Commission of the event; provide a written notification on Form SCI within 24 hours that includes a description of the SCI event and the system(s) affected, with other information required to the extent available at the time; provide regular updates regarding the SCI event until the event is resolved; and submit a final detailed written report regarding the SCI event.⁵³¹ If proposed Rule 10 is

adopted as proposed, it would require Market Entities that are Covered Entities to provide the Commission (and other regulators, if applicable) with immediate written electronic notice of a significant cybersecurity incident affecting the Covered Entity and, thereafter, report and update information about the significant cybersecurity incident by filing Part I of proposed Form SCIR with the Commission (and other regulators, if applicable).⁵³² Part I of proposed Form SCIR would elicit information about the significant cybersecurity incident and the Covered Entity’s efforts to respond to, and recover from, the incident.

Consequently, a Covered Entity that is also an SCI entity that experiences a significant cybersecurity incident under proposed Rule 10 that also is an SCI event would be required to make two filings for the single incident: one on Part I of proposed Form SCIR and the other on Form SCI. The Covered Entity also would be required to make additional filings on Forms SCIR and SCI pertaining to the significant cybersecurity incident (*i.e.*, to provide updates and final reports). The approach of having two separate notification and reporting programs—one under proposed Rule 10 and the other under Regulation SCI—would be appropriate for the following reasons.

As discussed earlier, certain broker-dealers and all transfer agents would not be SCI entities under the current and proposed requirements of Regulation SCI.⁵³³ Certain of the broker-dealers that are not SCI entities (currently and as it

terms in the definition of “SCI event”). The amendments to Regulation SCI would broaden the definition of “system intrusion” to include a cybersecurity event that disrupts, or significantly degrades, the normal operation of an SCI system, as well as a material attempted unauthorized entry into the SCI systems or indirect SCI systems of an SCI entity. Regulation SCI 2023 Proposing Release.

⁵³² See paragraphs (c)(1) and (2) of proposed Rule 10 (requiring Covered Entities to provide immediate written notice and subsequent reporting on Part I of proposed Form SCIR of significant cybersecurity incidents); sections II.B.2. and II.B.4. of this release (discussing the requirements of paragraphs (c)(1) and (2) of proposed Rule 10 and Part I of Form SCIR in more detail). Non-Covered Broker-Dealers also would be subject to an immediate written electronic notice requirement under paragraph (e)(2) of proposed Rule 10. However, as discussed above, a Non-Covered Broker-Dealer likely would not be an SCI Entity.

⁵³³ See section II.F.1.b. of this release. Currently, broker-dealers that operate as ATs and trade certain stocks exceeding specific volume thresholds are SCI entities. The proposed amendments to Regulation SCI would expand the definition of “SCI entity” to include broker-dealers that exceed an asset-based size threshold or a volume-based trading threshold in NMS stocks, exchange-listed options, agency securities, or U.S. treasury securities. See Regulation SCI 2023 Proposing Release.

would be amended) would be Covered Entities and all transfer agents would be Covered Entities.⁵³⁴ In addition, the current and proposed reporting requirements of Regulation SCI are or would be triggered by events impacting SCI systems and indirect SCI systems. The Covered Entities that are or would be SCI entities use and rely on information systems that are not SCI systems or indirect SCI systems under the current and proposed amendments to Regulation SCI. For these reasons, Covered Entities could be impacted by significant cybersecurity incidents that do not trigger the current and proposed notification requirements of Regulation SCI either because they do not meet the current or proposed definitions of “SCI entity” or the significant cybersecurity incident does not meet the current or proposed definitions of “SCI event.”

As discussed earlier, the objective of the notification and reporting requirements of proposed Rule 10 is to improve the Commission’s ability to monitor and evaluate the effects of a significant cybersecurity incident on Covered Entities and their customers, counterparties, members, registrants, or users, as well as assess the potential risks affecting financial markets more broadly.⁵³⁵ For this reason, Part I of proposed Form SCIR is tailored to elicit information relating specifically to cybersecurity, such as information relating to the threat actor, and the impact of the incident on any data or personal information that may have been accessed.⁵³⁶ The Commission and its staff could use the information reported on Part I of Form SCIR to monitor the U.S. securities markets and the Covered Entities that support those markets broadly from a cybersecurity perspective, including identifying cybersecurity threats and trends from a market-wide view. By requiring all Covered Entities to report information about a significant cybersecurity incident on a common form, the information obtained from these filings over time would create a comprehensive set of data of all significant cybersecurity incidents impacting Covered Entities that is based on these entities responding to the same check boxes and questions on the form. This would facilitate analysis of the data, including analysis across different Covered Entities and significant cybersecurity incidents. Eventually, this

⁵³⁴ See paragraphs (a)(1)(i)(A) and (F) proposed Rule 10 (defining the categories of broker-dealers that would be Covered Entities); paragraph (a)(1)(ix) proposed Rule 10 (defining transfer agents as “covered entities”).

⁵³⁵ See section II.B.2.a. of this release.

⁵³⁶ See section II.B.2.b. of this release.

⁵²⁸ See 17 CFR 248.201(d)(1).

⁵²⁹ See 17 CFR 248.201(b)(3).

⁵³⁰ See section I.A. of this release.

⁵³¹ See 17 CFR 242.1002(b). An “SCI event” is an event at an SCI entity that is: (1) a “systems disruption,” which is an event in an SCI entity’s SCI systems that disrupts, or significantly degrades, the normal operation of an SCI system; (2) a “systems intrusion,” which is any unauthorized entry into the SCI systems or indirect SCI systems of an SCI entity; or (3) a “systems compliance issue,” which is an event at an SCI entity that has caused any SCI system of such entity to operate in a manner that does not comply with the Exchange Act and the rules and regulations thereunder or the entity’s rules or governing documents, as applicable. See 17 CFR 242.1000 (defining the terms “systems disruption,” “system intrusion,” and “system compliance issue” and including those

set of data and the ability to analyze it by searching and sorting how different Covered Entities responded to the same questions on the form could be used to spot common trending risks and vulnerabilities as well as best practices employed by Covered Entities to respond to and recover from significant cybersecurity incidents.

The current and proposed definitions of “SCI event” include events that are not related to significant cybersecurity incidents.⁵³⁷ For example, under the current and proposed requirements of Regulation SCI, the definition of “SCI event” includes an event in an SCI entity’s SCI systems that disrupts, or significantly degrades, the normal operation of an SCI system.⁵³⁸ Therefore, the definitions are not limited to events in an SCI entity’s SCI systems that disrupt, or significantly degrade, the normal operation of an SCI system caused by a significant cybersecurity incident. The information elicited in Form SCI reflects the broader scope of the reporting requirements of Regulation SCI (as compared to the narrower focus of proposed Rule 10 on reporting about significant cybersecurity incidents). For example, the form requires the SCI entity to identify the type of SCI event: systems compliance issue, systems disruption, and/or systems intrusion. In addition, Form SCI is tailored to elicit information specifically about SCI systems. For example, the form requires the SCI entity to indicate whether the type of SCI system impacted by the SCI event directly supports: (1) trading; (2) clearance and settlement; (3) order routing; (4) market data; (5) market regulation; and/or (6) market surveillance. If the impacted system is a critical SCI system, the SCI entity must indicate whether it directly supports functionality relating to: (1) clearance and settlement systems of clearing agencies; (2) openings, reopenings, and closings on the primary listing market; (3) trading halts; (4) initial public offerings; (5) the provision of consolidated market data; and/or (6) exclusively-listed securities. The form also requires the SCI entity to indicate if the systems that provide functionality to the securities markets for which the availability of alternatives is significantly limited or nonexistent and without which there would be a

⁵³⁷ See 17 CFR 242.1000 (defining the term “SCI event”); Regulation SCI 2023 Proposing Release.

⁵³⁸ See 17 CFR 242.1000 (defining the term “system disruption” and including that term in the definition of “SCI event”); Regulation SCI 2023 Proposing Release.

material impact on fair and orderly markets.

e. Disclosure

Proposed Rule 10 and the existing and proposed requirements of Regulation SCI and the proposed requirements of Regulation S–P also have similar, but distinct, requirements related to notification about certain cybersecurity incidents. Regulation SCI requires that SCI entities disseminate information to their members, participants, or customers (as applicable) regarding SCI events.⁵³⁹ The proposed amendments to Regulation S–P would require broker-dealers and transfer agents to notify affected individuals whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization.⁵⁴⁰ Proposed Rule 10 would require a Covered Entity to make two types of public disclosures relating to cybersecurity on Part II of proposed Form SCIR.⁵⁴¹ Covered Entities would be required to make the disclosures by filing Part II of proposed Form SCIR on EDGAR and posting a copy of the filing on their business internet websites.⁵⁴² In addition, a Covered Entity that is either a carrying or introducing broker-dealer would be required to provide a copy of the most recently filed Part II of Form SCIR to a customer as part of the account opening process. Thereafter, the carrying or introducing broker-dealer would need to provide the customer with the most recently filed form annually. The copies of the form would need to be provided to the customer using the same means that the customer elects to receive account statements (e.g., by email or through the postal service). Finally, a Covered Entity would be required to promptly make updated disclosures through each of the methods described above (as applicable) if the information required to be disclosed about cybersecurity risk or significant cybersecurity incidents materially changes, including, in the case of the disclosure about significant cybersecurity incidents, after the occurrence of a new significant cybersecurity incident or when

⁵³⁹ See 17 CFR 242.1002(c).

⁵⁴⁰ See Regulation S–P 2023 Proposing Release. The proposed amendments to Regulation S–P would define “sensitive customer information” to mean any component of customer information alone or in conjunction with any other information, the compromise of which could create a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information. *Id.* The proposed amendments would provide example of sensitive customer information. *Id.*

⁵⁴¹ See paragraph (d)(1) of proposed Rule 10.

⁵⁴² See section II.B.3.b. of this release (discussing these proposed requirements in more detail).

information about a previously disclosed significant cybersecurity incident materially changes.

Consequently, a Covered Entity would—if it experiences a “significant cybersecurity incident”—be required to make updated disclosures under proposed Rule 10 by filing Part II of proposed Form SCIR on EDGAR, posting a copy of the form on its business internet website, and, in the case of a carrying or introducing broker-dealer, by sending the disclosure to its customers using the same means that the customer elects to receive account statements. Moreover, if Covered Entity is an SCI entity and the significant cybersecurity incident is or would be an SCI event under the current or proposed requirements of Regulation SCI, the Covered Entity also could be required to disseminate certain information about the SCI event to certain of its members, participants, or customers (as applicable). Further, if the Covered Entity is a broker-dealer or transfer agent and, therefore, subject to Regulation S–P (as it is proposed to be amended), the broker-dealer or transfer agent also could be required to notify individuals whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization.

However, despite these similarities, there are distinct differences. First, proposed Rule 10, Regulation SCI, and Regulation S–P (as proposed to be amended) require different types of information to be disclosed. Second, the disclosures, for the most part, would be made to different persons: (1) the public at large in the case of proposed Rule 10;⁵⁴³ (2) affected members, participants, or customers (as applicable) of the SCI entity in the case of Regulation SCI;⁵⁴⁴ and (3) affected individuals whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization or, in some cases, all individuals whose information resides in the customer information system that was accessed or used without authorization in the case of Regulation S–P (as proposed to be amended).

Additionally, the disclosure or notification provided about certain cybersecurity incidents is different

⁵⁴³ A carrying broker-dealer would be required to make the disclosures to its customers as well through the means by which they receive account statements.

⁵⁴⁴ Information regarding major SCI events is and would be required to be disseminated by an SCI entity to all of its members, participants, or customers (as applicable) under the existing and proposed requirements of Regulation SCI. See Regulation SCI 2023 Proposing Release.

under proposed Rule 10 and the existing and/or proposed requirements of Regulation SCI and Regulation S–P, given their distinct goals. For example, the requirement to disclose summary descriptions of certain cybersecurity incidents from the current or previous calendar year publicly on EDGAR, among other methods, under proposed Rule 10 serves a different purpose than: (1) the member, participant, or customer (as applicable) dissemination of information regarding SCI events under Regulation SCI; and (2) the customer notification obligation under the proposed amendments to Regulation S–P, which would provide more specific information to individuals affected by a security compromise involving their sensitive customer information, so that those individuals may take remedial actions if they so choose.

2. Request for Comment

The Commission requests comment on the potential duplication or overlap between the requirements of proposed Rule 10, Regulation SCI (as it currently exists and as it is proposed to be amended), and Regulation S–P (as it currently exists and as it is proposed to be amended). In addition, the Commission is requesting comment on the following matters:

91. Should the policies and procedures requirements of proposed Rule 10 be modified to address Market Entities that also would be subject to the existing and proposed requirements of Regulation SCI and/or Regulation S–P? For example, would it be particularly costly or create practical implementation difficulties to apply the requirements of proposed Rule 10 (if it is adopted) to have policies and procedures to address cybersecurity risks to Market Entities even if they also would be subject to requirements to have policies and procedures under Regulation SCI and/or Regulation S–P that address certain cybersecurity risks (currently and as they would be amended)? If so, explain why. If not, explain why not. Are there ways the policies and procedures requirements of proposed Rule 10 could be modified to minimize these potential impacts while achieving the separate goals of this proposal to protect participants in the U.S. securities markets and the markets themselves from cybersecurity risks? If so, explain how and suggest specific modifications.

92. Would it be appropriate to modify proposed Rule 10 to exempt SCI systems or indirect SCI systems from its policies and procedures requirements and instead rely on the policies and procedures requirements of Regulation

SCI to address cybersecurity risks to these information systems of Covered Entities? If so, explain why. If not, explain why not. What would be the costs and benefits of this approach? For example, if one set of policies and procedures generally would satisfy the requirements of both rules, would this approach result in incremental costs or benefits? Please explain. Would this approach achieve the objectives of this rulemaking to address cybersecurity risks to Covered Entities, given that Rule 10 is specifically designed to address cybersecurity risks and Regulation SCI is designed to address a broader range of risks to certain information systems? Please explain. Would this approach create practical implementation and compliance complexities inasmuch as one set of the Covered Entity's systems would be subject to Regulation SCI (*i.e.*, SCI systems and indirect SCI systems) and the other set would be subject to Rule 10? Please explain. If it would create practical implementation and compliance difficulties, would Covered Entities nonetheless apply separate policies and procedures requirements to their information systems based on whether they are or are not SCI systems and indirect SCI Systems or would they develop a single set of policies and procedures that comprehensively addresses the requirements of Regulation SCI and Rule 10? Please explain. Would a comprehensive set of policies and procedures result in stronger measures to protect SCI systems and indirect SCI systems from cybersecurity risks? Please explain. If so, would this be appropriate given the nature of SCI systems and indirect SCI systems and the roles these systems play in the U.S. securities markets? Please explain.

93. Should the policies and procedures requirements of proposed Rule 10 be modified to address Market Entities that also would be subject to the requirements of Regulation ATS? If so, explain why. If not, explain why not.

94. Should the immediate notification and reporting requirements of proposed Rule 10 be modified to address Covered Entities that also would be subject to the existing and proposed requirements of Regulation SCI? For example, would it be particularly costly or create practical implementation difficulties to apply the immediate notification and subsequent reporting requirements of proposed Rule 10 and Part I of proposed Form SCIR (if they are adopted) to Covered Entities even if they also would be subject to immediate notification and subsequent reporting requirements under Regulation SCI (as it currently exists and would be amended)? If so, explain

why. If not, explain why not. Are there ways the notification and reporting requirements of proposed Rule 10 and Part I of proposed Form SCIR could be modified to minimize these potential impacts while achieving the separate goals of this proposal to protect participants in the U.S. securities markets and the markets themselves from cybersecurity risks? If so, explain how and suggest specific modifications. For example, should Part I of proposed Form SCIR be modified to include a section that incorporates the check boxes and questions of Form SCI so that a single form could be filed to meet the reporting requirements of proposed Rule 10 and Regulation SCI? If so, explain why. If not, explain why not. Are there other ways Part I of proposed Form SCIR could be modified to combine the elements of Form SCI? If so, explain how. Should Rule 10 be modified to require that the initial Part I of Form SCIR must be filed within 24 hours (instead of promptly but not later than 48 hours) to align the filing timeframe with Regulation SCI? If so, explain why. If not, explain why not.

95. Should the public disclosure requirements of proposed Rule 10 be modified to address Covered Entities that also would be subject to the existing and proposed requirements of Regulation SCI and/or Regulation S–P? For example, would it be particularly costly or create practical implementation difficulties to apply the public disclosure requirements of proposed Rule 10 and Part II of proposed form SCIR (if they are adopted) to Covered Entities even if they also would be subject to the current and proposed disclosure requirements of Regulation SCI and Regulation S–P? If so, explain why. If not, explain why not. Are there ways the public disclosure requirements of proposed Rule 10 could be modified to minimize these potential impacts while achieving the separate goals of this proposal to protect participants in the U.S. securities markets and the markets themselves from cybersecurity risks? If so, explain how and suggest specific modifications. For example, should proposed Rule 10 be modified to permit the customer notification that would be required under the amendments to Regulation S–P to satisfy the requirement of proposed Rule 10 that a Covered Entity that is a carrying broker-dealer or introducing broker-dealer send a copy of an updated Part II of proposed Form SCIR to its customers? If so, explain why. If not, explain why not. Would sending the notification required by proposed Rule 10 and the

notification required by the proposed amendments to Regulation S-P to the same customer be confusing to the customer? If so, explain why. If not, explain why not.

G. Cybersecurity Risk Related to Crypto Assets

The creation, distribution, custody, and transfer of crypto assets depends almost exclusively on the operations of information systems.⁵⁴⁵ Crypto assets, therefore, are exposed to cybersecurity risks.⁵⁴⁶ Further, crypto assets are attractive targets for threat actors.⁵⁴⁷ Therefore, information systems that involve crypto assets may be subject to heightened cybersecurity risks. If Market Entities engage in business activities involving crypto assets, they could be exposed to these heightened cybersecurity risks.⁵⁴⁸

Crypto assets are an attractive target for unlawful activity due, in large part, to the unique nature of distributed ledger technology. Possession or control of crypto assets on a distributed ledger is based on ownership or knowledge of public and private cryptographic key

⁵⁴⁵ The term “digital asset” or “crypto asset” refers to an asset that is issued and/or transferred using distributed ledger or blockchain technology (“distributed ledger technology”), including, but not limited to, so-called “virtual currencies,” “coins,” and “tokens.” See *Custody of Digital Asset Securities by Special Purpose Broker-Dealers*, Exchange Act Release No. 90788 (Dec. 23, 2020) [86 FR 11627, 11627, n.1 (Feb. 26, 2021)]. To the extent digital assets rely on cryptographic protocols, these types of assets are commonly referred to as “crypto assets.” A crypto asset may or may not meet the definition of a “security” under the federal securities laws. See, e.g., *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO*, Securities Exchange Act Release No. 81207 (July 25, 2017), available at <https://www.sec.gov/litigation/investreport/34-81207.pdf>. See also *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946). “Digital asset securities” can be referred to as “crypto asset securities” and for purposes of this release, the Commission does not distinguish between the terms “digital asset securities” and “crypto asset securities.”

⁵⁴⁶ See KPMG, *Assessing crypto and digital asset risks* (May 2022), available at <https://advisory.kpmg.us/content/dam/advisory/en/pdfs/2022/assessing-crypto-and-digital-asset-risks.pdf> (“Properly securing digital assets[] is typically viewed as the biggest risk that companies must address.”).

⁵⁴⁷ See U.S. Department of Treasury, *Crypto-Assets: Implications for Consumers, Investors, and Businesses* (Sept. 2022), available at https://home.treasury.gov/system/files/136/CryptoAsset_EO5.pdf (“Treasury Crypto Report”) (“Moreover, the crypto-asset ecosystem has unique features that make it an increasingly attractive target for unlawful activity, including the ongoing evolution of the underlying technology, pseudonymity, irreversibility of transactions, and the current asymmetry of information between issuers of crypto-assets and consumers and investors.”).

⁵⁴⁸ Moreover, if the Market Entity’s activities involving crypto asset securities involve its information systems, the requirements being proposed in this release would be implicated.

pairings. These key pairings are somewhat analogous to user names and passwords and consist of strings of letters and numbers used to sign transactions on a distributed ledger and to prove ownership of a blockchain address, which is commonly known as a “digital wallet.”⁵⁴⁹ Digital wallets, in turn, generally require the use of internet-connected hardware and software to receive and transmit information about crypto asset holdings.

A digital wallet can be obtained by anyone, including a potential threat actor. If a victim’s digital wallet is connected to the internet, and a threat actor obtains access to the victim’s private key, the threat actor can transfer the contents of the wallet to another blockchain address (such as the threat actor’s own digital wallet) without authorization from the true owner. It may be difficult to subsequently track down the identity of the threat actor because the owner of a digital wallet can remain anonymous (absent additional attribution information) and because intermediaries involved in the transfer of crypto assets, such as trading platforms, may not comply with or may actively claim not to be subject to applicable “know your customer” or related diligence requirements.⁵⁵⁰

The current state of distributed ledger technology may present other challenges to defending against cybercriminal activity. First, there is no centralized information technology (“IT”) infrastructure that can dynamically detect and prevent cyberattacks on wallets or prevent the transfer of illegitimately obtained crypto assets by threat actors.⁵⁵¹ This is unlike traditional infrastructures, such as those used by banks and broker-dealers, where behavioral and historic

⁵⁴⁹ See, e.g., NIST Glossary (defining “private key”).

⁵⁵⁰ See, e.g., Treasury Crypto Report (“Compared to registered financial market intermediaries—which are subject to rules and laws that promote market integrity and govern risks and business conduct, including identifying, disclosing, and mitigating conflicts of interest and adhering to AML/CFT requirements—many crypto-asset platforms may either not yet be in compliance with, or may actively claim not to be subject to, existing applicable U.S. laws and regulations, including registration requirements. . . . When the onboarding process used by platforms is limited or opaque, the risk that the platform may be used for illegal activities increases.”).

⁵⁵¹ See CipherTrace, *Cryptocurrency crime and anti-money laundering report* (June 2022), available at https://4345106.fs1.hubspotusercontent-na1.net/hubs/4345106/CAML%20Reports/CipherTrace%20Cryptocurrency%20Crime%20and%20Anti-Money%20Laundering%20Report%2c%20June%202022.pdf?_hstc=56248308.2ea6daf13b00f00afe4d9acf0886eddff.1667865330143.1667865330143.1667917991763.2&_hssc=56248308.1.1667917991763&_hsfp=247897319 (“CipherTrace 2022 Report”).

transaction patterns can be used to detect and prevent account takeovers in real-time. Furthermore, distributed ledger technology often makes it difficult or impossible to reverse erroneous or fraudulent crypto asset transactions, whereas processes and protocols exist to reverse erroneous or fraudulent transactions when trading more traditional assets.⁵⁵² In addition, certain code that governs the operation of a blockchain and that governs so-called “smart contracts” are often transparent to the public. This provides threat actors with visibility into potential vulnerabilities associated with the code, though developers may have limited ability to patch those vulnerabilities.⁵⁵³ These characteristics of distributed ledger technology, and others, present cybersecurity vulnerabilities that, if taken advantage of by a threat actor, could lead to financial harm without meaningful recourse to reverse fraudulent transactions, recover or replace lost crypto assets, or correct errors.

The amount of crypto assets stolen by threat actors annually continues to increase.⁵⁵⁴ Threat actors looking to

⁵⁵² For example, this is the case with Bitcoin and Ether, the two crypto assets with the largest market values. See CoinMarketCap, *Today’s Cryptocurrency Prices by Market Cap*, available at <https://coinmarketcap.com/> (“Crypto Asset Market Value Chart”). See also, e.g., Kaili Wang, Qinchen Wang, and Dan Boneh, *ERC-20R and ERC-721R: Reversible Transactions on Ethereum* (Oct. 11, 2022), available at <https://arxiv.org/pdf/2208.00543.pdf#page=16&zoom=100,96,233> (Stanford University proposal discussing the immutability of Ethereum-based tokens, and proposing that reversible Ethereum transactions may facilitate more wide-spread adoption of these crypto assets). With respect to securities, the clearance and settlement of securities that are not crypto assets are characterized by infrastructure whereby intermediaries such as clearing agencies and securities depositories serve as key participants in the process. The clearance and settlement of crypto asset securities, on the other hand, may rely on fewer, if any, intermediaries and remain evolving areas of practices and procedures.

⁵⁵³ See Treasury Crypto Report (“Smart contracts, which are widely used by many permissionless blockchains, also present risks as they combine the features of generally being immutable and publicly viewable. Taken together, these attributes pose several vulnerabilities that may be exploited by illicit actors to steal customer funds: once an attacker finds a bug in a smart contract and exploits it, immutable smart contract protocols limit developers’ ability to patch the exploited vulnerability, giving attackers more time to exploit the vulnerability and steal assets.”).

⁵⁵⁴ See Treasury Crypto Report (noting that of the total amount of crypto asset based crime in 2021, theft rose by over 500% year-over-year to \$3.2 billion in total); Chainalysis, *The 2022 Crypto Crime Report* (Feb. 2022), available at <https://go.chainalysis.com/2022-Crypto-Crime-Report.html> (“Chainalysis 2022 Report”) (predicting that illicit transaction activity will reach an all-time high in terms of value in 2022, and noting that crypto asset based crime hit a new all-time high in 2021, with illicit addresses receiving \$14 billion over the course of the year, up from \$7.8 billion in 2020).

exploit the vulnerabilities associated with crypto assets often employ social engineering techniques, such as phishing to acquire a user's cryptographic key pairing information. Phishing tactics that have been employed to reach and trick crypto asset users into disclosing their private keys include: (1) monitoring social media for users reaching out to wallet software support, intervening with direct messages, and impersonating legitimate support staff who need the user's private key to fix the problem; (2) distributing new crypto assets at no cost to a set of wallets in an "airdrop," and then failing transactions on those assets with an error message to redirect the owner to a phishing website or a website that installs plug-in software and steals the user's credentials from a local device; and (3) impersonating a wallet software provider and stealing private keys directly from the user.⁵⁵⁵ To the extent that the activities of Market Entities involve crypto assets, these types of phishing tactics could be used against their employees.

Another related variation of a social engineering attack that is similar to phishing, but does not involve stealing private keys directly, is called "ice phishing." In this scheme, the threat actor tricks the user into signing a digital transaction that delegates approval and control of the user's wallet to the attacker, allowing the threat actor to become the so-called "spender" of the wallet. Once the threat actor obtains control over the user's wallet, the threat actor can transfer all of the crypto assets to a new wallet controlled by the threat actor.⁵⁵⁶

Threat actors also target private keys and crypto assets through other means, such as installing key logging software,⁵⁵⁷ exploiting vulnerabilities in

code used in connection with crypto assets (such as smart contracts), and deploying flash loan attacks.⁵⁵⁸ Installing key logging software, in particular, is an example of malware that threat actors looking to exploit the vulnerabilities associated with crypto assets often employ. Other common types of crypto asset-focused malware techniques include info stealers, clippers, and cryptojackers.⁵⁵⁹

The size and growth of the crypto asset markets, along with the fact that many participants in these markets (such as issuers, intermediaries, trading platforms, and service providers) may be acting in noncompliance with applicable law, continue to make them an attractive target for threat actors looking for quick financial gain. The crypto asset ecosystem has exhibited rapid growth in the past few years. For example, industry reports have suggested that the total crypto asset market value increased from approximately \$135 billion on January 1, 2019 to just under \$2.1 trillion on March 31, 2022.⁵⁶⁰ According to these reports, the crypto asset market value peaked at almost \$3 trillion in November 2021.⁵⁶¹ Various sources also report that the market value remains over \$1 trillion today.⁵⁶²

disguised as a legitimate file or application, or is directed to a phony website.

⁵⁵⁸ See Treasury Crypto Report ("In an innovation unique to DeFi lending, some protocols may support 'flash loans,' which enable users to borrow, use, and repay crypto assets in a single transaction that is recorded on the blockchain in the same data block. Because there is no default risk associated with flash loans, users can borrow without posting collateral and without risk of being liquidated. A 'flash loan attack' can occur when the temporary surge of funds obtained in a flash loan is used to manipulate prices of crypto-assets, often through the interaction of multiple DeFi services, enabling attackers to take over the governance of a protocol, change the code, and drain the treasury."). In 2021, code exploits and flash loan attacks accounted for 49.8% of all crypto asset value stolen across all crypto asset services. See Chainalysis 2022 Report.

⁵⁵⁹ Specifically, "info stealers" collect saved credentials, files, autocomplete history, and crypto asset wallets from compromised computers. "Clippers" can insert new text into the victim's clipboard, replacing text the user has copied. Hackers can use clippers to replace crypto asset addresses copied into the clipboard with their own, allowing them to reroute planned transactions to their own wallets. "Cryptojackers" make unauthorized use of the computing power of a victim's device to mine crypto assets. See Chainalysis 2022 Report.

⁵⁶⁰ See CipherTrace June 2022 Report. The amount of total activity in the crypto asset markets has increased as well. According to the CipherTrace June 2022 Report, while the total activity in 2020 was around \$4.3 trillion, there was approximately \$16 trillion of total activity in the first half of 2021 alone. See *id.*

⁵⁶¹ See *id.*

⁵⁶² See Crypto Asset Market Value Chart; see also Treasury Crypto Report.

III. General Request for Comment

In addition to the specific requests for comment above, the Commission is requesting comments from all members of the public on all aspects of the proposed rule and amendments. Commenters are requested to provide empirical data in support of any arguments or analyses. With respect to any comments, the Commission notes that they are of the greatest assistance to this rulemaking initiative if accompanied by supporting data and analysis of the issues addressed in those comments and by alternatives to the Commission's proposals where appropriate.

IV. Economic Analysis

A. Introduction

The Commission is mindful of the economic effects, including the costs and benefits, of: (1) proposed Rule 10; (2) Parts I and II of proposed Form SCIR; (3) the proposed amendments to Rules 17a-4, 17ad-7, and 18a-6; (4) the proposed amendments to existing orders that exempt certain clearing agencies from registering with the Commission; and (5) the proposed amendments to paragraph (d)(1) of Rule 3a71-6 to add proposed Rule 10 and Form SCIR to the list of Commission requirements eligible for a substituted compliance determination. Section 3(f) of the Exchange Act provides that when engaging in rulemaking that requires the Commission to consider or determine whether an action is necessary or appropriate in the public interest, to also consider, in addition to the protection of investors, whether the action will promote efficiency, competition, and capital formation.⁵⁶³ Section 23(a)(2) of the Exchange Act also requires the Commission to consider the effect that the rules and rule amendments would have on competition, and it prohibits the Commission from adopting any rule that would impose a burden on competition not necessary or appropriate in furtherance of the Exchange Act.⁵⁶⁴ The analysis below addresses the likely economic effects of the proposed rule and form, the proposed rule amendments, and the proposed amendments to the exemptive orders, including the anticipated and estimated benefits and costs of these proposals and their likely effects on efficiency, competition, and capital formation. The Commission also discusses the potential economic effects of certain alternatives

⁵⁵⁵ See Microsoft 365 Defender Research Team, 'Ice Phishing' on the Blockchain (Feb. 16, 2022), available at <https://www.microsoft.com/security/blog/2022/02/16/ice-phishing-on-the-blockchain/>.

⁵⁵⁶ See CipherTrace June 2022 Report. Delegating authority to another user reportedly is a common transaction on decentralized finance ("DeFi") platforms, as the user may need to provide the DeFi platform with approval to conduct transactions with the user's tokens. In an "ice phishing" attack, the attacker modifies the spender address to the attacker's address. Once the approval transaction has been signed, submitted, and mined, the spender can access the funds. The attacker can accumulate approvals over a period of time and then drain the victim's wallets quickly.

⁵⁵⁷ Key logging can involve a threat actor deploying a software program designed to record which keys are pressed on a computer keyboard to obtain passwords or other encryption keys, therefore bypassing certain security measures. See NIST Glossary (defining "key logger"). Key logging software can be installed, for example, when the victim clicks a link or downloads an attachment in a phishing email, downloads a Trojan virus that is

⁵⁶³ See 15 U.S.C. 78c(f).

⁵⁶⁴ See 15 U.S.C. 78w(a)(2).

to the approaches taken with respect to these proposals.

As discussed above, Market Entities rely on information systems to perform functions that support the fair, orderly, and efficient operation of the U.S. securities markets.⁵⁶⁵ This exposes them and the U.S. securities markets to cybersecurity risk. According to the Bank for International Settlements, the financial sector has the second-largest share of COVID-19-related cybersecurity events between the end of February and June 2020.⁵⁶⁶ As is the case with other risks (e.g., market, credit, or liquidity risk), cybersecurity risk can be addressed through policies and procedures that are reasonably designed to manage the risk. A second means to address cybersecurity risk to the U.S. securities markets is through the Commission gathering and sharing information about significant cybersecurity incidents. This risk also can be addressed through greater transparency.⁵⁶⁷ For these reasons (and the reasons discussed throughout the release), the Commission is proposing Rule 10 and Form SCIR to require that Market Entities address cybersecurity risks, to improve the Commission's ability to obtain information about significant cybersecurity incidents impacting Covered Entities and to require Covered Entities to disclose publicly summary descriptions of their cybersecurity risks and significant cybersecurity incidents (if applicable).

It is important to note that the Market Entities serve different functions in the U.S. securities markets and are subject to different regulatory regimes. As a result, Market Entities today have varying approaches to cybersecurity protections and would have different costs and benefits associated with complying with proposed Rule 10 and for Covered Entities to file Parts I and II of proposed Form SCIR. In addition, Market Entities may have different costs and benefits depending on the size and complexity of their businesses. For example, because Non-Covered Broker-Dealers likely are materially smaller in size than Covered Entities, use fewer and less complex information systems, and have less data stored on information systems, the obligations of Non-Covered Broker-Dealers under proposed Rule 10

are more limited, and likely would have lower compliance costs. This could be the case even though Non-Covered Broker-Dealers may still need to invest in hardware and software, employ legal and compliance personnel, or contract with a third party. Furthermore, in addition to the direct benefits and costs realized by Market Entities, other market participants, such as investors and third-party service providers would realize indirect benefits and costs from the adoption of the proposed rule. The direct and indirect benefits and costs realized by each type of Market Entity and market participants are discussed below.⁵⁶⁸

Many of the benefits and costs discussed below are difficult to quantify. For example, the effectiveness of cybersecurity strengthening measures taken as a result of proposed Rule 10 depends on the extent to which they reduce the likelihood of a cybersecurity incident and on the expected cost of such an incident, including remediation costs in the event that a cybersecurity incident causes harm. As a result, the effectiveness of cybersecurity strengthening is subject to numerous assumptions and unknowns, and thus is difficult to quantify. Effectively, because cybersecurity infrastructure as well as policies and procedures help to prevent successful cybersecurity intrusions, the benefit of cybersecurity protection can be measured as the expected loss from a cybersecurity incident. In 2020, the average loss in the financial services industry was \$18.3 million, per company per incident. The average cost of a financial services data breach was \$5.85 million.⁵⁶⁹ Thus, those values would represent the benefit of avoiding a cybersecurity incident.

The Commission has limited information on cybersecurity incidents impacting Market Entities. For example, as discussed above, certain Market Entities are SCI entities subject to the requirements of Regulation SCI.⁵⁷⁰ SCI entities must report SCI events to the Commission on Form SCI, which could include cybersecurity incidents.⁵⁷¹ However, only certain Market Entities are SCI entities and the reporting requirements of Regulation SCI are limited to SCI systems and indirect SCI

systems, which are a subset of the information systems used by SCI entities. To the extent that a cybersecurity incident at a Market Entity that is also a SCI entity is an SCI event, the Market Entity would be required to file Form SCI. However, only certain SCI events are also considered to be cybersecurity incidents. Consequently, the Commission currently has only partial knowledge of the cybersecurity incidents that occur at Market Entities. The Commission believes using the benefit and cost values related to SCI Entities as a basis to estimate the benefits and costs of the proposed rule for Covered Entities would be instructive but may be under inclusive.

Similarly, the Commission has access to information contained in confidential anti-money laundering (AML) suspicious activity reports ("SARs") that broker-dealers file with the Department of the Treasury's Financial Crime Enforcement Network ("FinCEN"), which includes known or suspected cybersecurity incidents.⁵⁷² However, the SARs filed by broker-dealers with FinCEN do not necessarily include all of the details associated with an incident, such as whether the incident was confirmed, the extent of the impact, and how the breach was remediated. Furthermore, the SAR filing may not be timely, as a broker-dealer has up to 30 days to file the SAR if a suspect is identified, or up to 60 days if a suspect is not identified. Issues that require immediate attention—such as terrorist financing or ongoing money laundering schemes—must be reported to law enforcement.⁵⁷³ If reporting is not otherwise required by the Commission or an SRO, a broker-dealer "may also, but is not required to" contact the Commission.⁵⁷⁴ Broker-dealers must make the supporting documentation available to the Commission and registered SROs (as well as to FinCEN, law enforcement agencies, and Federal regulatory authorities that examine for Bank Secrecy Act compliance) upon request.⁵⁷⁵ The benefits and costs of filing SARs with FinCEN can serve as a basis to approximate the cost of filing Part I of proposed Form SCIR. However, the proposed rule would require a

⁵⁶⁵ See section I.A. of this release (discussing cybersecurity risks and the use of information systems by Market Entities).

⁵⁶⁶ *Id.* The health sector is ranked first in term of the cyberattacks.

⁵⁶⁷ "The Council recommends that regulators and market participants continue to work together to improve the coverage, quality, and accessibility of financial data, as well as improve data sharing among relevant agencies." FSOC 2021 Annual Report, at 16.

⁵⁶⁸ See section IV.D. of this release (discussing these benefits and costs).

⁵⁶⁹ Jennifer Rose Hale, *The Soaring Risks of Financial Services Cybercrime: By the Numbers*, Diligent (Apr. 9, 2021), available at <https://www.diligent.com/insights/financial-services/cybersecurity/#>.

⁵⁷⁰ See section II.F.1.b. of this release (discussing the Covered Entities that are subject to Regulation SCI).

⁵⁷¹ See section II.F.1.d. of this release (discussing the reporting requirements of Regulation SCI).

⁵⁷² See, e.g., Fergus Shiel and Ben Hallman, International Consortium of Investigative Journalists, *Suspicious Activity Reports, Explained* (Sept. 20, 2020), available at <https://www.icij.org/investigations/fincen-files/suspicious-activity-reports-explained/> (stating that approximately 85% of SARs are filed by a few large banks to report money laundering).

⁵⁷³ See 31 CFR 1023.320(b)(3).

⁵⁷⁴ See 31 CFR 1023.320(a)(1), (b)(3).

⁵⁷⁵ See 31 CFR 1023.320(d).

quicker reporting timeline, more information to be provided, and multiple updates with regard to a given significant cybersecurity event. Thus, the costs related to complying with SAR filings serves as a floor for Covered Entities complying with the proposed rule.

While the Commission has attempted to quantify economic effects where possible, some of the discussion of economic effects is qualitative in nature. The Commission seeks comment on all aspects of the economic analysis, especially any data or information that would enable the Commission to quantify the proposal's economic effects more accurately.

B. Broad Economic Considerations

Market Entities generally have financial incentives to maintain some level of cybersecurity protection because failure to safeguard their operations from attacks on their information systems and protect information about their customers, counterparties, members, registrants, or users as well as their funds and assets could lead to losses of funds, assets, and customer information, as well as damage the Market Entity's reputation. As a result, Market Entities generally have an incentive to invest some amount of money to address cybersecurity risk.

Market Entities' reputational motives generally should encourage them to invest in measures to protect their information systems from cybersecurity risk.⁵⁷⁶ Moreover, the damage caused by a significant cybersecurity incident, including the associated remediation costs, may exceed that of implementing cybersecurity policies and procedures that may have prevented the incident and its harmful impacts. As a result, significant losses arising from a potential significant cybersecurity incident can encourage Market Entities to invest in cybersecurity protections today. However, such investments in cybersecurity protections may not be sufficient. The Investment Company Institute notes that the remediation costs of \$252 million associated with the 2013 data breach experienced by Target Brands, Inc. ("Target") far exceeded the cost of the cybersecurity insurance the company purchased (\$90 million), resulting in an out-of-pocket loss for Target of \$162 million.⁵⁷⁷ PCH

⁵⁷⁶ See Marc Dupuis and Karen Renaud, *Scoping the Ethical Principles of Cybersecurity Fear Appeals*, 23 Ethics and Info. Tech. 265 (2021), available at <https://doi.org/10.1007/s10676-020-09560-0>.

⁵⁷⁷ See National Law Review, *Target Data Breach Price Tag: \$252 Million and Counting* (Feb. 26,

Technologies states that in 2020, small companies (1–49 employees) lost an average of \$24,000 per cybersecurity incident. That loss increased to \$50,000 per incident for medium-sized companies (50–249 employees). Large companies (250–999 employees) and enterprise-level firms (1,000 employees or more) lost an average of \$133,000 and \$504,000 per cybersecurity incident, respectively.⁵⁷⁸

Having an annual penetration testing requirement can help Market Entities reduce the likelihood of costly data breaches. For instance, according to one industry source, RSI Security, a penetration test "can measure [the entity's] system's strengths and weaknesses in a controlled environment before [the entity has] to pay the cost of an extremely damaging data breach."⁵⁷⁹ For example, RSI Security explains that penetration testing "can cost anywhere from \$4,000–\$100,000," and "[o]n average, a high quality, professional [penetration testing] can cost from \$10,000–\$30,000."⁵⁸⁰ RSI Security, however, was clear that the magnitudes of these costs can vary with size, complexity, scope, methodology, types, experience, and remediation measures.⁵⁸¹ On the other hand, the same article cited IBM's 2019 Cost of a Data Breach Study, which reported that the average cost of a data breach is \$3.92 million with an average loss of 25,575 records,⁵⁸² which would more than justify "the average \$10,000–\$30,000 bill from a professional, rigorous [penetration testing]."⁵⁸³ Another

2015), available at <https://www.natlawreview.com/article/target-data-breach-price-tag-252-million-and-counting>.

⁵⁷⁸ Timothy Guim, *Cost of Cyber Attacks vs. Cost of Cyber Security in 2021*, PCH Technologies (July 7, 2021), available at <https://pchtechnologies.com/cost-of-cyber-attacks-vs-cost-of-cyber-security-in-2021/#:-:text=1%20Large%20businesses%3A%20Between%20%242%20million%20and%20%245,%24500%2C000%20or%20less%20spent%20on%20cybersecurity%20per%20year>.

⁵⁷⁹ RSI Security, *What is the Average Cost of Penetration Testing?*, RSI Security Blog (posted Mar. 5, 2020), available at <https://blog.rsisecurity.com/what-is-the-average-cost-of-penetration-testing/#:-:text=Penetration%20testing%20can%20cost%20anywhere,that%20of%20a%20large%20company>.

⁵⁸⁰ See RSI Security, *What is the Average Cost of Penetration Testing?*, RSI Security Blog (posted Mar. 5, 2020), available at <https://blog.rsisecurity.com/what-is-the-average-cost-of-penetration-testing/#:-:text=Penetration%20testing%20can%20cost%20anywhere,that%20of%20a%20large%20company>.

⁵⁸¹ See id.

⁵⁸² See IBM, *Cost of a Data Breach Report* (2019), available at <https://www.ibm.com/downloads/cas/RDEQK07R> ("2019 Cost of Data Breach Report").

⁵⁸³ See RSI Security, *What is the Average Cost of Penetration Testing?*, RSI Security Blog (posted Mar. 5, 2020), available at <https://>

source estimates a "high-quality, professional [penetration testing to cost] between \$15,000–\$30,000," while emphasizing that "cost varies quite a bit based on a set of variables."⁵⁸⁴ This is in line with a third source, which states that "[a] true penetration test will likely cost a minimum of \$25,000."⁵⁸⁵ It is the Commission's understanding that multi-cloud architecture could introduce more complexity and accordingly, cybersecurity risks into Market Entities back-up systems, to the extent they have them.⁵⁸⁶

Large Market Entities that have economies of scale are able to implement cybersecurity policies and procedures in a more cost-effective manner. Smaller Market Entities, on the other hand, generally do not enjoy the same economies of scale or scope. The marginal cost for smaller Market Entities when implementing cybersecurity policies and procedures that are just as robust as those that would be needed by large Market Entities likely would be relatively high for smaller Market Entities. As a result, investment costs in cybersecurity protection at small broker-dealers, for example, (most of which would be Non-Covered Broker-Dealers under proposed Rule 10) likely will account for a larger proportion of their revenue than at relatively large broker-dealers (which likely would be Covered Entities that realize economies of scale).

Having policies and procedures in place to address cybersecurity risk would benefit the customers, counterparties, members, registrants, or users with whom Market Entities interact. However, a cybersecurity budget likely is tempered, in part, such that the total sum spent to address cybersecurity risk provides some, but possibly not complete, protection against cyberattacks.⁵⁸⁷ Ultimately,

blog.rsisecurity.com/what-is-the-average-cost-of-penetration-testing/#:-:text=Penetration%20testing%20can%20cost%20anywhere,that%20of%20a%20large%20company.

⁵⁸⁴ Gary Glover, *How Much Does a Pentest Cost?*, Securitymetrics Blog (Nov. 15, 2022, 8:36 a.m.), available at <https://www.securitymetrics.com/blog/how-much-does-pentest-cost>.

⁵⁸⁵ Mitnick Security, *What Should You Budget for a Penetration Test? The True Cost*, Mitnick Security Blog, (posted Jan. 29, 2021, 5:13 a.m.), available at <https://www.mitnicksecurity.com/blog/what-should-you-budget-for-a-penetration-test-the-true-cost>.

⁵⁸⁶ For example, security breach possibilities could increase because of the interconnection of Market Entities through their multi cloud providers.

⁵⁸⁷ See Martijn Wessels, Puck van den Brink, Thijmen Verburgh, Beatrice Cadet, and Theo van Ruijven, *Understanding Incentives for Cybersecurity Investments: Development and Application of a Typology*, 1 Digit. Bus. 1–7 (Oct. 2021), available at <https://doi.org/10.1016/j.digbus.2021.100014>; Scott Dynes, Eric Goetz, and Michael Freeman, *Cyber*

Continued

those costs to address cybersecurity risks will be passed on, to the extent possible, to the persons with whom the Market Entities do business.⁵⁸⁸

The level of cybersecurity protection instituted by Market Entities may be inadequate from the perspective of overall economic efficiency.⁵⁸⁹ In other words, the chosen level of cybersecurity protection may, in fact, represent an underinvestment relative to the optimal level of cybersecurity protection that should be maintained by Market Entities from an overall economic perspective. Levels of cybersecurity protection that are not optimal may exacerbate the occurrence of harmful cybersecurity incidents. Cybersecurity events have grown in both number and sophistication.⁵⁹⁰ These developments in the market have significantly increased the negative externalities that may flow from systems failures.

Underinvestment in cybersecurity may occur because a Market Entity is aware that it would not bear the full cost of a cybersecurity incident (*i.e.*, some negative externalities may be borne by its customers, counterparties, members, registrants, or users). As a result, the Market Entity does not have to internalize the complete cost of cybersecurity protection when deciding upon its level of investment. This underinvestment by the Market Entity is considered to be a moral hazard problem, because other market participants are harmed by a significant cybersecurity incident and are forced to bear those costs that spill over to them.

Security: Are Economic Incentives Adequate? (Intern. Conf. on Critical Infrastructure Protection, Conference Paper, 2007), available at https://doi.org/10.1007/978-0-387-75462-8_2; Brent R. Rowe and Michael P. Gallaher, *Private Sector Cyber Security Investment Strategies: An Empirical Analysis*, The Fifth Workshop on the Economics of Information Security (Mar. 2006), available at <http://www.infoseccon.net/workshop/downloads/2006/pdf/18.pdf> (“Private Sector Cyber Security Investment Strategies Analysis”); Nicole van der Meulen, RAND Europe, *Investing in Cybersecurity* (Aug. 2015), available at https://repository.wodc.nl/bitstream/handle/20.500.12832/2173/2551-full-text_tcm28-73946.pdf?sequence=4&isAllowed=y.

⁵⁸⁸ See Derek Mohammed, *Cybersecurity Compliance in the Financial Sector*, J. Internet Banking and Com. (2015), available at <https://www.icommercecentral.com/open-access/cybersecurity-compliance-in-the-financial-sector.php?aid=50498>.

⁵⁸⁹ Low levels of investment in cybersecurity protection, which are different from underinvestment in cybersecurity protection, can be a function of a number of issues, such as firm budget, available solutions, knowledge of the threat actors’ capabilities, and the performance of in-house or contracted information technology teams.

⁵⁹⁰ See, e.g., Chuck Brooks, *Alarming Cyber Statistics For Mid-Year 2022 That You Need To Know* (June 3, 2022), available at <https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=2429c57e7864>.

At the same time, even though Market Entities may not bear the full cost of a cybersecurity failure (*e.g.*, loss of the personal information or the assets of their customers, members, registrants, or users), they likely would incur some costs themselves and therefore have incentives to avoid cybersecurity failures. These incentives could cause them to implement policies and procedures to address cybersecurity risk, which would likely result in benefits that accrue in large part to their customers, counterparties, members, registrants, or users. Market Entities could do this in order to avoid the harms that could be caused by a significant cybersecurity incident (*e.g.*, loss of funds, assets, or personal, confidential, or proprietary information; damage to or the holding hostage of their information systems; or reputational damage). As a result, Market Entities have a potential incentive to rely overly on reactive solutions to cybersecurity threats and attacks instead of proactive ones.⁵⁹¹

1. In the context of cybersecurity, negative externalities arising from the moral hazard problem can have significant negative repercussions on the financial system more broadly, particularly due to the interconnectedness of Market Entities.⁵⁹² Borg notes that the level of interconnectedness and complexity can have an influence on the degree of damage that cybersecurity incidents impose on Market Entities as well as their customers, counterparties, members, registrants, and users.⁵⁹³ As for the availability of substitutes the negative effect of a cybersecurity incident could be lessened to the extent that there is one or more competing firms that can complete the task, such as another broker-dealer or national securities exchange. On the flip side, significant cybersecurity incidents may be the most damaging when there are no substitutes available to execute the required task.

In addition to other firms being negatively affected by a cybersecurity incident, investors can be negatively affected. For example, a significant cybersecurity incident at a national securities exchange could affect its ability to execute trades, causing orders

⁵⁹¹ See Private Sector Cyber Security Investment Strategies Analysis.

⁵⁹² See Anil K. Kashyap and Anne Wetherilt, *Some Principles for Regulating Cyber Risk*, 109 Amer. Econ. Assoc. Papers and Proc. 482 (May 2019).

⁵⁹³ See Scott Borg, *Economically Complex Cyberattacks*, IEEE Computer Society (2005), available at <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1556539>.

to go unfilled. Depending on how long it takes the national securities exchange to resolve the issue, the prices of securities traded on the exchange may be different from when the orders were originally placed.⁵⁹⁴ A loss of confidence in an exchange due to a cybersecurity incident could result in a longer-term reallocation of trading volume to competing exchanges or other trading venues.⁵⁹⁵ A significant cybersecurity incident could produce negative effects that spill over and affect market participants outside of the national securities exchange itself. It also may adversely affect market confidence, and curtail economic activity through a reduction in securities trading among market participants.⁵⁹⁶

While the negative externalities that arise from the moral hazard problem are usually depicted as being absorbed by other market participants, the losses to other parties may be potentially covered in part or in full by insurance policies.⁵⁹⁷ An even stronger incentive to underinvest is the possibility that an outside party can make whole or at least mitigate some of the losses incurred by the various market participants. Market Entities may underinvest in their cybersecurity measures due to the moral hazard that results from expectations of government support.⁵⁹⁸ Most threat

⁵⁹⁴ National securities exchanges currently are subject to certain obligations under Regulation SCI.

⁵⁹⁵ National securities exchanges may be required to meet certain regulatory obligations in such circumstances.

⁵⁹⁶ See Electra Ferriello, *Prof. Robert Shiller's U.S. Crash Confidence Index*, Yale School of Management, Intern. Ctr. for Fin. (Nov. 3, 2020), available at <https://som.yale.edu/blog/prof-robert-shillers-us-crash-confidence-index>; Gregg E. Berman, Senior Advisor to the Director, Division of Trading and Markets, Commission, Speech by SEC Staff: Market Participants and the May 6 Flash Crash (Oct. 2010), available at <https://www.sec.gov/news/speech/2010/spch101310geb.htm>.

⁵⁹⁷ See Marsh, *Underinvestment in Cyber Insurance Can Leave Organizations Vulnerable* (2022), available at <https://www.marsh.com/pr/en/services/cyber-risk/insights/underinvestment-in-cyber-insurance.html>.

⁵⁹⁸ It has long been noted that it is difficult for governments to commit credibly to not providing support to entities that are seen as critical to the functioning of the financial system, resulting in problems of moral hazard. See, e.g., Walter Bagehot, *Lombard Street: A Description of the Money Market* (Henry S. King & Co., 1873). Historically, banking entities seen as “too big to fail” or “too interconnected to fail” have been the principal recipients of such government support. Since the financial crisis of 2007–2009, non-bank financial institutions (such as investment banks), money market funds, and insurance companies, as well as specific markets such as the repurchase market have also benefited. See, e.g., Gary B. Gorton, *Slapped by the Invisible Hand: The Panic of 2007*, Oxford Univ. Press (2010); see also Viral V. Acharya, Deniz Anginer, and A. Joseph Warburton, *The End of Market Discipline? Investor Expectations of Implicit Government Guarantees*,

actors primarily have a monetary incentive, and there is a large monetary incentive to breach cybersecurity protections in the financial sector. As a result, Covered Entities—such as clearing agencies, large national securities exchanges, and large carrying broker-dealers—may be attractive targets to sophisticated threat actors aiming to compromise or disrupt the U.S. financial system because of the services they perform to support the functioning of the U.S. securities markets; the protection of confidential, proprietary, or personal information they store; or the financial assets they hold. Protection against “advanced persistent threats”⁵⁹⁹ from sophisticated threat actors, whatever their motives, is costly.⁶⁰⁰ The belief—no matter how misplaced—that a widespread and crippling cybersecurity attack would be met with government support, such as direct payments for recovery and immediate cybersecurity investments, could lead to moral hazard where certain Covered Entities underinvest in defenses aimed at countering that threat.⁶⁰¹

Suboptimal spending on cybersecurity also can be the result of asymmetric information among Market Entities and market participants. A Market Entity may not know what its optimal cybersecurity expenditures should be because the nature and scope of future attacks are unknown. In addition, a Market Entity may not know what its competitors do in terms of cybersecurity planning, whether they have been subject to unsuccessful cyberattacks, or have been a victim of one or more significant cybersecurity incidents. Market Entities also may not be able to signal credibly to their customers, counterparties, members, registrants, or users that they are better at addressing cybersecurity risks than their peers, thus reducing their incentive to bear such cybersecurity

investment costs.⁶⁰² Lastly, Market Entities’ customers, counterparties, members, registrants, or users typically do not have information about the Market Entities’ cybersecurity spending, the efficacy of the cybersecurity investments made, or their policies and procedures. Therefore, those market participants cannot make judgments about Market Entities’ cybersecurity preparedness. Because of this information asymmetry, Market Entities may not have as strong of an incentive to have robust cybersecurity measures compared to a scenario in which customers, counterparties, members, registrants, or users had perfect information about the Market Entities’ cybersecurity practices and the risks that they face.

Underinvestment in cybersecurity also may stem from the principal-agent problem of divergent goals in economic theory. The relationship between a Market Entity (*i.e.*, the agent) and the principals (*i.e.*, its customers, counterparties, members, registrants, or users) can be affected if the principal relies on the agent to perform services on the principal’s behalf.⁶⁰³ Because principals and their agents may not have perfectly aligned preferences and goals, agents may take actions that increase their well-being at the expense of principals, thereby imposing “agency costs” on the principals.⁶⁰⁴ Although private contracts between principals and agents may aim to minimize such costs, they are limited in their ability to do so in that agents can decide not to enter into such agreements and ultimately not provide the particular services to the principals. Furthermore, agents can charge much higher fees that the principals choose not to bear. These limitations provides one rationale for regulatory intervention.⁶⁰⁵ Market-based incentives alone are unlikely to result in optimal provision of cybersecurity protection. In this context, having plans

and procedures in place to prepare for and respond to cybersecurity incidents,⁶⁰⁶ and the rule would help ensure that the infrastructure of the U.S. securities markets remains robust, resilient, and secure. A well-functioning financial system is a public good.

Beyond reputational damage to the affected agent (Market Entity), the principals (the Market Entity’s customers, counterparties, members, registrants, or users) can be negatively affected by a cybersecurity breach as a result of loss in personal information and/or funds and assets. Thus the principals and the agents may have different reasons for needing cybersecurity protocols. Furthermore, the negative effects of a cybersecurity incident also can spread among Market Entities due to their interconnectedness.⁶⁰⁷ Those other Market Entities prefer that the principals employ strong cybersecurity practices that reduce the chances of a successful breach and its negative cascading effects throughout the financial sector. All of the preceding negative externalities are arguments for proposed Rule 10.

In the production of cybersecurity defenses and controls, the main input is information. In particular, information about prior attacks and their degree of success, as well as prior human errors and their degree of harm, is valuable in mounting effective countermeasures and controls.⁶⁰⁸ However, Market Entities may be naturally reluctant to share such information, as doing so could assist future attackers as well as lead to loss of customers, reputational harm, litigation, or regulatory scrutiny, which would be costs associated with public disclosure.⁶⁰⁹ On the other hand, disclosure of such information creates a positive information externality—the benefits of which accrue to society at large and are not fully captured by the Market Entity making the disclosure.

SSRN Scholarly Paper, Rochester, NY: Social Science Research Network (May 1, 2016).

⁵⁹⁹ “Advanced persistent threat” refers to sophisticated cyberattacks by hostile organizations with the goal of: gaining access to defense, financial, and other targeted information from governments, corporations and individuals; maintaining a foothold in these environments to enable future use and control; and modifying data to disrupt performance in their targets. See Michael K. Daly, *The Advanced Persistent Threat (or Informationized Force Operations)*, Raytheon (Nov. 4, 2009), available at <https://www.usenix.org/legacy/event/lisa09/tech/slides/daly.pdf>.

⁶⁰⁰ See Nikos Virvilis and Dimitris Gritzalis, *The Big Four—What We Did Wrong in Advanced Persistent Threat Detection?*, 2013 Int’l Conf. on Availability, Reliability and Security 248 (2013).

⁶⁰¹ See Lawrence A. Gordon, Martin P. Loeb, and William Lucyshyn, *Cybersecurity Investments in the Private Sector: The Role of Governments*, 15 Geo. J. Int’l Aff. 79 (2014).

⁶⁰² See Sanford J. Grossman, *The Informational Role of Warranties and Private Disclosure about Product Quality*, 24 J. L. Econ. 461 (Dec. 1981); see also Michael Spence, *Competitive and Optimal Responses to Signals: An Analysis of Efficiency and Distribution*, 7 J. Econ. Theory 296 (Mar. 1, 1974); George A. Akerlof, *The Market for “Lemons” : Quality Uncertainty and the Market Mechanism*, 84 Q. J. Econ. 488 (Aug. 1970).

⁶⁰³ See Michael C. Jensen and William H. Meckling, *Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure*, 3 J. Fin. Econ. 305 (1976).

⁶⁰⁴ *Id.*

⁶⁰⁵ Such limitations can arise from unobservability or un-verifiability of actions, transactions costs associated with including numerous contingencies in contracts, or bounded rationality in the design of contracts. See, e.g., Jean Tirole, *Cognition and Incomplete Contracts*, 99 a.m. Econ. Rev. 265 (Mar. 2009) (discussing a relatively modern treatment of these issues).

⁶⁰⁶ For example, according to an IBM report, in the context of system issues arising from cybersecurity events, having an incident response plan and “testing that plan regularly can help [each firm] proactively identify weaknesses in [its] cybersecurity and shore up [its] defenses” and “save millions in data breach costs.” See 2019 Cost of Data Breach Report; see also Alex Asen et al., *Are You Spending Enough on Cybersecurity* (Feb. 19, 2020), available at <https://www.bcg.com/publications/2019/are-you-spending-enough-cybersecurity> (noting “[a]s the world becomes ever more reliant on technology, and as cybercriminals refine and intensify their attacks, organizations will need to spend more on cybersecurity”).

⁶⁰⁷ See sections I.A.1. and I.A.2. of this release (discussing how the interconnectedness of Market Entities creates cybersecurity risk).

⁶⁰⁸ See Peter W. Singer and Allan Friedman, *Cybersecurity: What Everyone Needs to Know 222* (Oxford Univ. Press, 2014).

⁶⁰⁹ See, e.g., FTC Equifax Civil Action.

This situation can occur because the disclosure informs the Market Entity's customers, counterparties, members, registrants, or users—as well as the Market Entity's competitors—about the cybersecurity incidents experienced by the Market Entity. As a result, information disclosures intended to close the information asymmetry gap can have both positive and negative consequences.

As discussed earlier, sources of market failure in cybersecurity come from information asymmetries at two different levels: (1) between Market Entities and their customers, counterparties, members, registrants, or users; and (2) between Market Entities and threat actors. These two failures, in turn, create distinct consequences for each of these stakeholders.

At the first level, a Market Entity's customers, counterparties, members, registrants, or users have incomplete information about their own cybersecurity risks due to incomplete information about the Market Entity's actual cybersecurity policies and procedures. To exacerbate the first level of information asymmetry, Market Entities typically interact with other market participants. For example, investors do business with broker-dealers, introducing broker-dealers work with carrying broker-dealers, FINRA supervises broker-dealers, broker-dealers interact with national securities exchanges, and national securities exchanges work with clearing agencies.

When utilizing the services of a Market Entity, other market participants may not have full information regarding the Market Entity's exposure to material harm as a result of a cybersecurity incident. A cybersecurity incident that harms a Market Entity can harm its customers, counterparties, members, registrants, or users. Disclosure of information regarding significant cybersecurity incidents by Market Entities could be used by their customers, counterparties, members, registrants, or users to manage their own cybersecurity risk by investing in additional cybersecurity protection, and, to the extent they have a choice, selecting a different Market Entity with satisfactory cybersecurity protection with whom to transact or otherwise conduct business.⁶¹⁰ That is, a Market Entity with strong cybersecurity policies and procedures and a clean record in

⁶¹⁰ As discussed earlier, the public disclosure requirements of proposed Rule 10 would apply to Market Entities that meet the proposed rule's definition of "covered entity." See paragraph (d) of proposed Rule 10; section II.B.3. of this release (discussing the public disclosure requirements of proposed Rule 10).

terms of past significant cybersecurity incidents may be perceived by these market participants as more desirable to interact with, or obtain services from, than Market Entities of the same type that do not fit that profile. Even general details about the cybersecurity incidents, as well as the number of significant cybersecurity incidents during the current or previous calendar year, could allow customers, counterparties, members, registrants, and users to compare Market Entities.

As a result, information from the disclosure may permit customers, counterparties, members, registrants, and users to gauge the riskiness of doing business with a certain Market Entity when they would not have been able to without that knowledge, and the disclosures may encourage those market participants to move their business to competing Market Entities that would have to disclose information under proposed Rule 10 and are perceived to be more prepared for cybersecurity attacks.⁶¹¹ The information disclosed by competitors also can incentivize Market Entities to increase their investment in cybersecurity protections and allow them to adjust their defenses when they would not have done so otherwise, thus increasing overall market stability by further limiting harmful cybersecurity incidents.

At the second level, there are differences in the capabilities of threat actors that are external to Market Entities and the assumed level of cybersecurity preparations needed by Market Entities to protect against significant cybersecurity incidents. Specifically, Market Entities cannot fully anticipate the type, method, and complexity of all types of cyberattacks that may materialize. Moreover, cyberattacks evolve over time, becoming more complex and using new avenues to circumvent Market Entities' cybersecurity protections.⁶¹² Furthermore, Market Entities cannot predict the timing or the target of a given cyberattack. Though this information asymmetry is impossible to eradicate fully given the inherent secretive nature of threat actors, regulation may help to prevent an expansion of information asymmetry by requiring Market Entities to gather and assess information about cybersecurity risks and vulnerabilities more often. Doing so would not only help to contain the negative effects of successful

⁶¹¹ The firms making the disclosure may be incentivized to invest more in cybersecurity protection, potentially to the point of overinvestment in order not to lose customers, counterparties, members, registrants, and users.

⁶¹² See, e.g., Verizon DBIR.

cybersecurity attacks on any one Market Entity going forward, but it also would aid in minimizing the growth in negative externalities as the effects of successful cyberattacks spillover to other Market Entities as well as to their customers, counterparties, members, registrants, or users.

Cybersecurity defenses must constantly evolve in order to keep up with the threat actors who are exogenous to the Market Entity, and its ability to anticipate specific attacks on itself is difficult at best. Within the reasonable scenario of an interconnected market with multiple points of entry for a potential threat actor, it may be more costly for Market Entities that are the victims of cascading cybersecurity breaches than for the initial target itself, as the other Market Entities within the network ultimately would need to prepare for a multitude of attacks originating from many different initial targets.⁶¹³ A strong cybersecurity program can also help Market Entities to protect themselves from cybersecurity attacks that could possibly come from one of multiple entry points. Having comprehensive cybersecurity policies and procedures will aid Market Entities identifying the source of a breach, which can result in lower detection costs and the identification of the threat actor in a more expeditious manner.

C. Baseline

Each type of Market Entity that would be subject to proposed Rule 10 has a distinct business model and role in the U.S. financial markets. As a result, the risks and practices, regulation, and market structure for each Market Entity will form the baseline for the economic analysis.

1. Cybersecurity Risks and Current Relevant Regulations

a. Cybersecurity Risks

With the widespread adoption of internet-based products and services over the last two decades, all businesses have had to address cybersecurity issues.⁶¹⁴ For financial services firms, the stakes are particularly high because they transact, hold custody of, and maintain ownership records of wealth in the form of cash, securities, or other liquid assets that cyber threat actors might strive to obtain illegally. Such entities also represent attack vectors for threat actors. In addition, Market Entities have linkages with each other as

⁶¹³ See Cybersecurity and its Cascading Effect on Societal Systems.

⁶¹⁴ See section I.A.1. of this release (discussing cybersecurity risks to the U.S. securities markets).

a result of the business they conduct together. A breach at one Market Entity may be exploited and serve as a means of compromising other Market Entities. Cybersecurity threat intelligence surveys consistently find the financial sector to be one of the most—if not the most—attacked industries,⁶¹⁵ and remediation costs for an incident can be substantial.⁶¹⁶ As a result, firms in the financial sector need to invest in cybersecurity to protect their business operations along with the accompanying assets and data stored on information systems.

Further, as discussed earlier, the custody and transfer of crypto assets depends almost exclusively on the operations of information systems.⁶¹⁷ Crypto assets, therefore, are exposed to cybersecurity risks and they are attractive targets for threat actors. Information systems that involve crypto assets may be subject to heightened cybersecurity risks. To the extent that Market Entities engage in business activities involving crypto assets, they could be exposed to these heightened cybersecurity risks.

The ubiquity and rising costs of cybercrime,⁶¹⁸ along with financial services firms' increasingly costly efforts to prevent it,⁶¹⁹ have been the motivation behind the growth in the cybersecurity industry.⁶²⁰ Many Market Entities cite the NIST Framework as the main standard for implementing strong cybersecurity measures.⁶²¹ The focus that has been placed on cybersecurity also has led to the development of numerous technologies and standards by private sector firms aimed at mitigating cybersecurity threats. Many of these developments, such as multi-factor authentication, secure hypertext

transfer protocol,⁶²² and user-access control, are now commonplace. Practitioners—chief technology officers (“CTOs”), chief compliance officers (“CCOs”), chief information officers (“CIOs”), chief information security officers (“CISOs”), and their staffs—frequently utilize industry standard frameworks⁶²³ and similar offerings from cybersecurity consultants and product vendors to assess and address institutional cybersecurity preparedness. Such frameworks include information technology asset management, controls, change management, vulnerability management, incident management, continuity of operations, risk management, dependencies on third parties, training, and information sharing. In recent years, companies' boards of directors and executive management teams have focused on these areas.

Unaddressed cybersecurity risks, particularly at Market Entities, impose negative externalities on the broader financial system. Actions taken to implement, maintain, and upgrade cybersecurity protections likely reduce overall risk in the economy. In addition, due to the potential for large-scale losses with respect to funds, securities, and customer information, Market Entities have a vested interest in installing, maintaining, and upgrading cybersecurity-related software and hardware. Based on staff discussions with market participants, cybersecurity-related activities can be performed in-house or contracted out to third parties with expertise in those areas. Financial services firms may employ a mix of in-house and outsourced staff and resources to meet their cybersecurity needs and goals.

b. Current Relevant Regulations

i. Broker-Dealers

Broker-dealers are subject to Regulation S–P⁶²⁴ and Regulation S–ID.⁶²⁵ In addition, ATSs that trade certain stocks exceeding specific volume thresholds are subject to Regulation SCI.⁶²⁶ Further, an ATS is subject to Regulation ATS.⁶²⁷ As discussed earlier, Regulation SCI,

Regulation S–P, Regulation ATS, and Regulation S–ID have provisions requiring policies and procedures to address certain types of cybersecurity risks.⁶²⁸ Regulation SCI also requires immediate written or telephonic notice and subsequent reporting to the Commission on Form SCI of certain types of incidents.⁶²⁹ Finally, Regulation SCI has provisions requiring disclosures to persons affected by certain incidents.⁶³⁰

Broker-dealers are also subject to the Commission's financial responsibility rules. Rule 15c3–1 requires broker-dealers to maintain minimum amounts of net capital, ensuring that the broker-dealer at all times has enough liquid assets to promptly satisfy all creditor claims if the broker-dealer were to go out of business.⁶³¹ Rule 15c3–3 under the Exchange Act imposes requirements relating to safeguarding customer funds and securities.⁶³² These rules provide protections for broker-dealer counterparties and customers and can help to mitigate the risks to, and impact on, customers and other market participants by protecting them from the consequences of financial failure that may occur because of a systems issue at a broker-dealer.

Under Exchange Act Rule 15c3–4, OTC derivatives dealers must establish, document, and maintain a system of internal risk management controls to assist it in managing the risks associated with its business activities, including market, credit, leverage, liquidity, legal, and operational risks.⁶³³ The required risk management system must include, among other things: a risk control unit that reports directly to senior management, periodic reviews which may be performed by internal audit staff, and annual reviews which must be conducted by independent certified public accountants.⁶³⁴ Management must periodically review the entity's business activities for consistency with risk management guidelines, including that the data necessary to conduct the risk monitoring and risk management function as well as the valuation process

⁶¹⁵ See, e.g., IBM, *X-Force Threat Intelligence Index 2022* (2022), available at <https://www.ibm.com/security/data-breach/threat-intelligence>.

⁶¹⁶ See, e.g., 2019 Cost of Data Breach Report (noting the average cost of a data breach in the financial industry in the United States is \$5.97 million).

⁶¹⁷ See section II.G. of this release (discussing cybersecurity risks related to crypto assets).

⁶¹⁸ See FBI internet Crime Report (noting that cybercrime victims lost approximately \$6.9 billion in 2021).

⁶¹⁹ See Office of Financial Research, *Annual Report to Congress 2021*, available at <https://www.financialresearch.gov/annual-reports/files/OFR-Annual-Report-2021.pdf>.

⁶²⁰ Sage Lazzaro, *The Cybersecurity Industry Is Burning—But VCs Don't Care*, *VentureBeat* (Sept. 2, 2021), available at <https://venturebeat.com/2021/09/02/the-cybersecurity-industry-is-burning-and-vc-dont-care/> (“VentureBeat”).

⁶²¹ FCI, *Top 5 Ways the Financial Services Industry Can Leverage NIST for Cybersecurity Compliance*, available at <https://fcicyber.com/top-5-ways-the-financial-services-industry-can-leverage-nist-for-cybersecurity-compliance/>.

⁶²² Hypertext transfer protocol, HTTP, is the primary set of rules that allow a web browser to communicate with (i.e., send data to) a website.

⁶²³ CISA, *Cyber Resilience Review (CRR): Method Description and Self-Assessment User Guide* (Apr. 2020), available at https://www.cisa.gov/sites/default/files/publications/2_CRR%204.0_Self-Assessment_User_Guide_April_2020.pdf.

⁶²⁴ See 17 CFR 248.1 through 248.30.

⁶²⁵ See 17 CFR 248.201 and 202.

⁶²⁶ See 17 CFR 242.1000 through 1007.

⁶²⁷ See 17 CFR 242.301 through 304.

⁶²⁸ See section II.F.1.c. of this release (discussing in more detail the existing requirements of Regulation SCI, Regulation S–P, Regulation ATS, and Regulation S–ID to have policies and procedures to address certain cybersecurity risks).

⁶²⁹ See section II.F.1.d. of this release (discussing in more detail the existing immediate notification and subsequent reporting requirements of Regulation SCI).

⁶³⁰ See section II.F.1.e. of this release (discussing in more detail the existing disclosure requirements of Regulation SCI).

⁶³¹ See 17 CFR 240.15c3–1.

⁶³² See 17 CFR 240.15c3–3.

⁶³³ See 17 CFR 240.15c3–4(a).

⁶³⁴ See 17 CFR 240.15c3–4(c).

over the entity's portfolio of products is accessible on a timely basis and information systems are available to capture, monitor, analyze, and report relevant data.⁶³⁵

Exchange Act Rules 17a-3 and 17a-4 require broker-dealers to make and keep current records detailing, among other things, securities transactions, money balances, and securities positions.⁶³⁶ Further, a broker-dealer that fails to make and keep current the records required by Rule 17a-3 must give notice to the Commission of this fact on the same day and, thereafter, within 48 hours transmit a report to the Commission stating what the broker-dealer has done or is doing to correct the situation.⁶³⁷

Moreover, with certain exceptions, broker-dealers must file confidential SARs with FinCEN to report any suspicious transaction relevant to a possible violation of law or regulation.⁶³⁸ The SARs include information regarding who is conducting the suspicious activity, what instruments or mechanisms are being used, when and where the suspicious activity took place, and why the filer thinks the activity is suspicious. Broker-dealers must make the records available to FinCEN as well as to other appropriate law enforcement agencies, federal or state securities regulators, and SROs registered with the Commission.

Broker-dealers are generally required to register with the Commission and join a national securities association or national securities exchange.⁶³⁹ As SROs, national securities associations and national securities exchanges are required to enforce their members' compliance with the Exchange Act, the rules and regulations thereunder, and the SRO's own rules. The vast majority of brokers and dealers join FINRA. Broker-dealers that are members of FINRA are subject FINRA Rules 3110, 3120, and 4530(b) (among other FINRA rules).⁶⁴⁰ FINRA Rule 3110 requires broker-dealer members to have in place a system to supervise its activities so that they are in compliance with applicable rules and regulations. FINRA Rule 3120 requires broker-dealer members to test and verify that the

supervisory procedures are reasonably designed with respect to the activities of the member and its associated persons, as well as to achieve compliance with applicable securities laws and regulations and with applicable FINRA rules. In addition, broker-dealer members must create additional or amended supervisory procedures where a need is identified by such testing and verification. The designated individual(s) must submit to the broker-dealer member's senior management no less than annually a report detailing each member's system of supervisory controls, the summary of the test results and significant identified exceptions, and any additional or amended supervisory procedures created in response to the test results. FINRA Rule 4530(b) states that each broker-dealer member shall promptly report to FINRA, but not later than 30 calendar days after the member has concluded or reasonably should have concluded, that an associated person of the member or the member itself has violated any securities-, insurance-, commodities-, financial- or investment-related laws, rules, regulations, or standards of conduct of any domestic regulatory body, foreign regulatory body, or SRO. Furthermore, Commission staff has issued statements⁶⁴¹ and FINRA has

issued guidance⁶⁴² in the area of cybersecurity.⁶⁴³ The statements and FINRA guidance with respect to these rules identify common elements of reasonably designed cybersecurity policies and procedures including risk assessment, user security and access, information protection, incident response,⁶⁴⁴ and training.⁶⁴⁵

Consistent with these rules, nearly all broker-dealers that participated in two Commission exam sweeps in 2015 and 2017 reported⁶⁴⁶ maintaining some

⁶⁴² See FINRA, *Core Cybersecurity Threats and Effective Controls for Small Firms* (May 2022), available at https://www.finra.org/sites/default/files/2022-05/Core_Cybersecurity_Threats_and_Effective_Controls-Small_Firms.pdf; FINRA, *Cloud Computing in the Securities Industry* (Aug. 16, 2021), available at <https://www.finra.org/sites/default/files/2021-08/2021-cloud-computing-in-the-securities-industry.pdf>; FINRA, *2021 Report on FINRA's Examination and Risk Monitoring Program* (Feb. 1, 2021), available at <https://www.finra.org/sites/default/files/2021-02/2021-report-finras-examination-risk-monitoring-program.pdf> ("FINRA 2021 Report on Examination and Risk Monitoring Program"); FINRA, *2019 Report on FINRA Examination Findings and Observations* (Oct. 16, 2019), available at <https://www.finra.org/sites/default/files/2019-10/2019-exam-findings-and-observations.pdf>; FINRA Common Cybersecurity Threats; FINRA, *Report on Selected Cybersecurity Practices—2018* (Dec. 1, 2018), available at https://www.finra.org/sites/default/files/Cybersecurity_Report_2018.pdf ("FINRA Report on Selected Cybersecurity Practices"); FINRA, *Report on FINRA Examination Findings* (Dec. 6, 2017), available at <https://www.finra.org/sites/default/files/2017-Report-FINRA-Examination-Findings.pdf>; FINRA, *Small Firm Cybersecurity Checklist* (May 23, 2016), available at <https://www.finra.org/compliance-tools/small-firm-cybersecurity-checklist>.

⁶⁴³ Cybersecurity has also been a regular theme of FINRA's Regulatory and Examination Priorities Letter since 2008 often with reference to Regulation S-P. Similarly, while risks related to data compromises were highlighted in the Commission staff's exam priorities, an official focus on "cyber" began in 2014 after the SEC sponsored a Cybersecurity Roundtable and the Division of Examination conducted cybersecurity initiative I and II to assess industry practices and legal and compliance issues associated with broker-dealer and investment adviser cybersecurity preparedness. Cybersecurity initiatives I and II were each separate series of examinations of cybersecurity practices conducted by EXAMS, concluding in 2014 and 2017. The examinations covered broker-dealers, investment advisers, and funds. EXAMS released a summary report for each initiative.

⁶⁴⁴ See FINRA 2021 Report on Examination and Risk Monitoring Program (noting that FINRA recommended among effective practices with respect to incident response: (1) establishing and regularly testing—often using tabletop exercises—a written formal incident response plan that outlines procedures for responding to cybersecurity and information security incidents; and (2) developing frameworks to identify, classify, prioritize, track and close cybersecurity-related incidents).

⁶⁴⁵ These categories vary somewhat in terms of nomenclature and the specific categories themselves across different Commission and FINRA publications.

⁶⁴⁶ See Cybersecurity Examination Sweep Summary (noting that of 57 examined broker-dealers, the vast majority adopted written information security policies, conducted periodic audits to determine compliance with these information security policies and procedures,

⁶³⁵ *Id.*

⁶³⁶ See 17 CFR 240.17a-3; 17 CFR 240.17a-4.

⁶³⁷ See 17 CFR 240.17a-11.

⁶³⁸ See 31 CFR 1023.320; section IV.A. of this release (discussing the requirements to file SARs in more detail).

⁶³⁹ See 15 U.S.C. 78o(a)(1) and 15 U.S.C. 78o(b)(8).

⁶⁴⁰ Broker-dealers that are members of national securities exchanges are also subject to the rules of the national securities exchanges regarding membership, registration, operation, and business conduct, among other exchange regulations.

⁶⁴¹ See, e.g. EXAMS, Risk Alert, *Safeguarding Client Accounts*; EXAMS, Risk Alert, *Select COVID-19 Compliance Risks and Considerations for Broker-Dealers and Investment Advisers* (Aug. 12, 2020), available at <https://www.sec.gov/files/Risk%20Alert%20-%20COVID-19%20Compliance.pdf>; EXAMS, Risk Alert, *Ransomware*; EXAMS, *Report on OCIE Cybersecurity and Resiliency Observations* (Jan. 27, 2020), available at <https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf> ("EXAMS Cybersecurity and Resiliency Observations"); EXAMS, *Safeguarding Customer Records and Information in Network Storage—Use of Third Party Security Features* (May 23, 2019), available at <https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Network%20Storage.pdf>; EXAMS, *Investment Adviser and Broker-Dealer Compliance Issues Related to Regulation S-P—Privacy Notices and Safeguard Policies* (Apr. 16, 2019), available at <https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Regulation%20S-P.pdf>; EXAMS, *Observations from Cybersecurity Examinations* (Aug. 7, 2017), available at <https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf> ("EXAMS Observations from Cybersecurity Examinations"); EXAMS, *Cybersecurity: Ransomware Alert* (May 17, 2017), available at <https://www.sec.gov/files/risk-alert-cybersecurity-ransomware-alert.pdf>; EXAMS, *OCIE's 2015 Cybersecurity Examination Initiative* (Sept. 15, 2015), available at <https://www.sec.gov/files/ocie-2015-cybersecurity-examination-initiative.pdf>; EXAMS, *Cybersecurity Examination Sweep Summary* (Feb. 3, 2015), available at <https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf> ("Cybersecurity Examination Sweep Summary"); EXAMS, *OCIE's 2014 Cybersecurity Initiative* (Apr. 15, 2014), available at <https://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert-Appendix-4.15.14.pdf>.

cybersecurity policies and procedures; conducting some periodic risk assessments to identify threats and vulnerabilities,⁶⁴⁷ conducting firm-wide systems inventorying or cataloguing, ensuring regular system maintenance including the installation of software patches to address security vulnerabilities, performing some penetration testing.⁶⁴⁸ A separate staff statement observed that at least some firms implemented capabilities that are able to control, monitor, and inspect all incoming and outgoing network traffic to prevent unauthorized or harmful traffic and implemented capabilities that are able to detect threats on endpoints.⁶⁴⁹ In the two Commission exam sweeps, many firms indicated that policies and procedures were vetted and approved by senior management and that firms provided annual cybersecurity reports to the board while some also provided ad hoc reports in the event of major cybersecurity events.⁶⁵⁰ Broadly, many broker-dealers reported relying on industry standards with respect to cybersecurity⁶⁵¹ typically by adhering to a specific industry standard or combination of industry standards or by using industry

standards as guidance in designing policies and procedures.

With respect to broker-dealer reporting to their boards regarding cybersecurity policies and procedures and cybersecurity incidents, the board reporting frequency ranged from quarterly to ad-hoc among the firms FINRA reviewed.⁶⁵² Approximately two-thirds of the broker-dealers (68%) examined in a 2015 survey had an individual explicitly assigned as the firm's CISO which might suggest extensive executive leadership engagement.

There are no current Commission or FINRA requirements for broker-dealers to disseminate notifications of breaches to members or clients although many firms do so⁶⁵³ pursuant to various state data breach laws.⁶⁵⁴ Broker-dealers are subject to state laws known as "Blue Sky Laws," which generally are regulations established as safeguards for investors against securities fraud.⁶⁵⁵ All 50 states have enacted laws in recent years requiring firms to notify individuals of data breaches. These laws differ by state, with some states imposing heightened notification requirements relative to other states.⁶⁵⁶

conducted risk assessments and reported considering such risk assessments in establishing their cybersecurity policies and procedures, and that with respect to vendors, the majority of the broker-dealers required cybersecurity risk assessments of vendors with access to their firms' networks and had at least some specific policies and procedures relating to vendors). *See also* EXAMS Observations from Cybersecurity Examinations (noting that nearly all firms surveyed had incident response plans).

⁶⁴⁷ *See* FINRA Report on Selected Cybersecurity Practices. This report noted that FINRA has conducted a voluntary Risk Control Assessment ("RCA") Survey with all active member firms for a number of years. According to the 2018 RCA, 94% of higher revenue firms and 70% of mid-level revenue firms use a risk assessment as part of their cybersecurity program.

⁶⁴⁸ *Id.* According to FINRA's 2018 RCA, 100% of higher revenue firms include penetration testing as a component in their overall cybersecurity program.

⁶⁴⁹ *See* EXAMS Cybersecurity and Resiliency Observations.

⁶⁵⁰ *See* FINRA, *Report on Cybersecurity Practices* (Feb. 2015), available at <https://www.finra.org/sites/default/files/2020-07/2015-report-on-cybersecurity-practices.pdf> ("FINRA Report on Cybersecurity Practices").

⁶⁵¹ *Id.* Among the firms that were part of the sweep, nearly 90% used one or more of the NIST, International Organization for Standardization ("ISO") or Information Systems Audit and Control Association ("ISACA") frameworks or standards. More specifically, 65% of the respondents reported that they use the ISO 27001/27002 standard while 25% use the Control Objectives for Information and Related Technologies ("COBIT") framework created by ISACA. Some firms use combinations of these standards for various parts of their cybersecurity programs. While the report focused on firm utilization of cybersecurity frameworks specifically, in many cases, the referenced frameworks were broader IT frameworks.

⁶⁵² *See* FINRA Report on Cybersecurity Practices. At a number of firms, the board received annual cybersecurity-related reporting while other firms report on a quarterly basis. A number of firms also provide ad hoc reporting to the board in the event of major cybersecurity events.

⁶⁵³ *See* Cybersecurity Examination Sweep Summary. Based on a small sample of firms, the vast majority of broker-dealers maintained plans for data breach incidents and most had plans for notifying customers of material events.

⁶⁵⁴ *See* Digital Guardian, *The Definitive Guide to U.S. State Data Breach Laws* (Nov. 15, 2022), available at <https://info.digitalguardian.com/rs/768-OQW-145/images/the-definitive-guide-to-us-state-data-breach-laws.pdf>.

⁶⁵⁵ *See, e.g.,* Office of Investor Education and Advocacy, Commission, *Blue Sky Laws*, available at <https://www.investor.gov/introduction-investing/investing-basics/glossary/blue-sky-laws>.

⁶⁵⁶ For example, some states may require a firm to notify individuals when a data breach includes biometric information, while others do not.

Compare Cal. Civil Code § 1798.29 (stating that notice to California residents of a data breach is generally required when a resident's personal information was or is reasonably believed to have been acquired by an unauthorized person and that "personal information" is defined to mean an individual's first or last name in combination with one of a list of specified elements, which includes certain unique biometric data), *with* Ala. Stat. §§ 8-38-2, 8-38-4, 8-38-5 (stating that notice of a data breach to Alabama residents is generally required when sensitive personally identifying information has been acquired by an unauthorized person and is reasonably likely to cause substantial harm to the resident to whom the information relates and that "sensitive personally identifying information" is defined as the resident's first or last name in combination with one of a list of specified elements, which does not include biometric information).

ii. SROs

National securities exchanges, registered clearing agencies, FINRA, and the MSRB are all SROs and are all considered to be SCI Entities, which requires them to comply with Regulation SCI.⁶⁵⁷ As discussed earlier, Regulation SCI has provisions requiring policies and procedures to address certain types of cybersecurity risks.⁶⁵⁸ Regulation SCI also requires immediate written or telephonic notice and subsequent reporting to the Commission on Form SCI of certain types of incidents.⁶⁵⁹ Finally, Regulation SCI has provisions requiring disclosures to persons affected by certain incidents.⁶⁶⁰

In addition, as described above, Rule 613 of Regulation NMS requires the Participants to jointly develop and submit to the Commission a CAT NMS Plan.⁶⁶¹ The Participants conduct the activities of the CAT through a jointly owned limited liability company, Consolidated Audit Trail, LLC. The CAT is intended to function as a modernized audit trail system that provides regulators with more timely access to a comprehensive set of trading data, thus enabling regulators to more efficiently and effectively reconstruct market events, monitor market behavior, and investigate misconduct. The CAT System accepts data that are submitted by the Participants and broker-dealers, as well as data from certain market data feeds like SIP and OPRA.⁶⁶²

FINRA CAT, LLC—a wholly-owned subsidiary of FINRA—has entered into an agreement with the Company to act as the Plan Processor and, as such, is responsible for building, operating and maintaining the CAT. However, because the CAT System is owned and operated by FINRA CAT, LLC on behalf of the national securities exchanges and FINRA, the Participants remain ultimately responsible for the performance of the CAT and its compliance with statutes, rules, and regulations.

⁶⁵⁷ *See* 17 CFR 242.1000 through 1007.

⁶⁵⁸ *See* section II.F.1.c. of this release (discussing in more detail the existing requirements of Regulation SCI to have policies and procedures to address certain cybersecurity risks).

⁶⁵⁹ *See* section II.F.1.d. of this release (discussing in more detail the existing immediate notification and subsequent reporting requirements of Regulation SCI).

⁶⁶⁰ *See* section II.F.1.e. of this release (discussing in more detail the existing disclosure requirements of Regulation SCI).

⁶⁶¹ *See* 17 CFR 242.613; *see also* section II.F.1.c. of this release (discussing the CAT NMS Plan in general and describing the roles of the Participants and Plan Processor).

⁶⁶² CAT data is not public, although some information in the CAT may be available through public sources (*e.g.*, market data feeds like the SIP or proprietary exchange feeds).

Under the Commission approved CAT NMS Plan, the Plan Processor must develop various policies and procedures related to data security, including a comprehensive information security program that includes, among other things, requirements related to: (1) connectivity and data transfer, (2) data encryption, (3) data storage, (4) data access, (5) breach management, including requirements related to the development of a cyber incident response plan and documentation of all information relevant to breaches, and (6) personally identifiable information data management.⁶⁶³ As part of this requirement, the Plan Processor is required to create and enforce policies, procedures, and control structures to monitor and address CAT data security, including reviews of industry standards⁶⁶⁴ and periodic penetration testing.⁶⁶⁵ Under the CAT NMS Plan the comprehensive information security program must be updated by the Plan Processor at least annually.⁶⁶⁶ Furthermore, both the Participants and the Plan Processor must also implement various data confidentiality measures that include safeguards to secure access and use of the CAT.⁶⁶⁷ The Plan Processor must also review Participant information security policies and procedures related to the CAT to ensure that such policies and procedures are comparable to those of the CAT System.⁶⁶⁸ In addition to these policies and procedures requirements,⁶⁶⁹ the

⁶⁶³ See CAT NMS Plan, appendix D, sections 4 and 6.12.

⁶⁶⁴ The Company is subject to certain industry standards with respect to its comprehensive information security program, including but not limited to: NIST 800–23 (Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Test/Evaluated Products), NIST 800–53 (Security and Privacy Controls for Federal Information Systems and Organizations), NIST 800–115 (Technical Guide to Information Security Testing and Assessment), and, to the extent not otherwise specified, all other provisions of the NIST cyber security framework. See CAT NMS Plan, Appendix D, section 4.2.

⁶⁶⁵ *Id.* at section 6.2(b)(v); Appendix D, sections 4 and 6.12.

⁶⁶⁶ See CAT NMS Plan at Appendix D, section 4.1.

⁶⁶⁷ Specifically, the measures implemented by the Plan Processor must include, among other things: (1) restrictions on the acceptable uses of CAT Data; (2) role-based access controls; (3) authentication of individual users; (4) MFA and password controls; (5) implementation of information barriers to prevent unauthorized staff from accessing CAT Data; (6) separate storage of sensitive personal information and controls on transmission of data; (7) security-driven monitoring and logging; (8) escalation of non-compliance events or security monitoring; and (9) remote access controls. *Id.* at Appendix D, sections 4.1, 5.3, 8.1.1, and 8.2.2; section 6.2(a)(v)(J)–(L); and section 6.2(b)(vii); section 6.5(c)(i); section 6.5(f).

⁶⁶⁸ CAT NMS Plan at section 6.2(b)(vii).

⁶⁶⁹ In August 2020, the Commission proposed certain amendments to the CAT NMS Plan that are

CAT NMS Plan requires several forms of periodic review of CAT, including an annual written assessment,⁶⁷⁰ regular reports,⁶⁷¹ and an annual audit.⁶⁷²

iii. SBS Entities

Section 15F(j)(2) of the Exchange Act, among other things, requires each SBS Entity to establish robust and professional risk management systems adequate for managing its day-to-day business.⁶⁷³ Additionally, certain SBS Entities must comply with specified provisions of Rule 15c3–4 and, therefore, establish, document, and maintain a system of internal risk management controls to assist in managing the risks associated with their business activities.⁶⁷⁴ Further, SBS Entities could be subject to Regulation

designed to enhance the security of the CAT. See <https://www.sec.gov/rules/proposed/2020/34-89632.pdf>.

⁶⁷⁰ The Participants are required to provide the Commission with an annual written assessment of the Plan Processor's performance, which must include, among other things, an evaluation of potential technology upgrades and an evaluation of the CAT information security program. *Id.* at section 6.6(b); section 6.2(a)(v)(G).

⁶⁷¹ The Plan Processor is required to provide the operating committee with regular reports on various topics, including data security issues and the Plan Processor. *Id.* at section 6.1(o); section 6.2(b)(vi); section 6.2(a)(v)(E); and section 4.12(b)(i).

⁶⁷² The Plan Processor is required to create and implement an annual audit plan that includes a review of all Plan Processor policies, procedures, control structures, and tools that monitor and address data security, in addition to other types of auditing practices. *Id.* at section 6.2(a)(v)(B)–(C); Appendix D, section 4.1.3; Appendix D, section 5.3.

⁶⁷³ 15 U.S.C. 78o–10(j). The Commission also requires that specified SBS Entity trading relationship documentation include the process for determining the value of each security-based swap for purposes of complying with, among other things, the risk management requirements of section 15F(j) of the Exchange Act and paragraph (h)(2)(iii)(I) of Rule 15Fh–3, and any subsequent regulations promulgated pursuant to section 15F(j). See 17 CFR 140.15Fi–5(b)(4). The documentation must include *either*: (1) alternative methods for determining the value of the security-based swap in the event of the unavailability or other failure of any input required to value the security-based swap for such purposes; or (2) a valuation dispute resolution process by which the value of the security-based swap shall be determined for the purposes of complying with the rule. See 17 CFR 140.15Fi–5(b)(4)(ii). Further, SBS Entities must engage in portfolio reconciliation to resolve discrepancies, among other things. See 17 CFR 240.15Fi–3(a) and (b). Such discrepancies include those resulting from a cybersecurity incident.

⁶⁷⁴ See 17 CFR 240.15c3–1(a)(7)(iii) (applies to broker-dealers authorized to use models, including broker-dealers dually registered as an SBSID); 17 CFR 240.15c3–1(a)(10)(ii) (applies to broker-dealers not authorized to use models that are dually registered as an SBSID); 17 CFR 240.18a–1(f) (applies to SBSIDs that are not registered as a broker-dealer, other than an OTC derivatives dealer, and that do not have a prudential regulator); 17 CFR 240.18a–2(c) (applies to MSBSPs); see also 17 CFR 240.15c3–4; see section IV.C.1.b.i. of this section (discussing requirements of Rule 15c3–4).

S–ID if they are “financial institutions” or “creditors.”⁶⁷⁵

SBS Entities are subject to additional Commission rules to have risk management policies and procedures, to review policies and procedures, to report information about compliance to the Commission, and to disclose certain risks to their counterparties. For example, paragraph (h) of Rule 15Fh–3 requires, among other things, that an SBSID or MSBSP establish, maintain, and enforce written policies and procedures regarding the supervision of the types of security-based swap business in which it is engaged and the activities of its associated persons that are reasonably designed to prevent violations of applicable federal securities laws and the rules and regulations thereunder.⁶⁷⁶ The policies and procedures must include, among other things: (1) procedures for a periodic review, at least annually, of the security-based swap business in which the SBS Entity engages and (2) procedures reasonably designed to comply with duties set forth in section 15F(j) of the Exchange Act, such as risk management duties set forth in section 15F(j)(2).⁶⁷⁷

Paragraph (b) of Rule 15Fk–1 requires each SBS Entity's CCO to, among other things, report directly to the board of directors or to the senior officer of the SBS Entity and to take reasonable steps to ensure that the SBS Entity establishes, maintains, and reviews written policies and procedures reasonably designed to achieve compliance with the Exchange Act and the rules and regulations thereunder relating to its business as an SBS Entity by: (1) reviewing its compliance with respect to the requirements described in section 15F of the Act and the rules and regulations thereunder, where the review involves preparing the an annual assessment of its written policies and procedures reasonably designed to achieve compliance with section 15F of

⁶⁷⁵ See 17 CFR 248.201 and 202. The scope of Regulation S–ID includes any financial institution or creditor, as defined in the Fair Credit Reporting Act (15 U.S.C. 1681) that is required to be “registered under the Securities Act of 1934.” See 17 CFR 248.201(a). Because SBS Entities are required to be so registered, an SBS Entity that is a “financial institution” or “creditor” as defined in the Fair Credit Reporting Act is within the scope of Regulation S–ID.

⁶⁷⁶ See 17 CFR 240.15Fh–3(h). An SBS Entity must amend its written supervisory procedures, as appropriate, when material changes occur in its business or supervisory system. Material amendments to the SBS Entity's supervisory procedures must be communicated to all associated persons to whom such amendments are relevant based on their activities and responsibilities. See 17 CFR 240.15Fh–3(h)(4).

⁶⁷⁷ See 17 CFR 240.15Fh–3(h)(2)(iii).

the Act and the rules and regulations thereunder; (2) taking reasonable steps to ensure that the SBS Entity establishes, maintains, and reviews policies and procedures reasonably designed to remediate non-compliance issues identified by the chief compliance officer through any means; and (3) taking reasonable steps to ensure that the SBS Entity establishes and follows procedures reasonably designed for the handling, management response, remediation, retesting, and resolution of non-compliance issues.⁶⁷⁸

Paragraph (c) of Rule 15Fk-1 requires an SBS Entity to submit an annual compliance report containing, among other things, a description of: (1) its assessment of the effectiveness of its policies and procedures relating to its business as an SBS Entity; (2) any material changes to the SBS Entity's policies and procedures since the date of the preceding compliance report; (3) any areas for improvement, and recommended potential or prospective changes or improvements to its compliance program and resources devoted to compliance; (4) any material non-compliance matters identified; and (5) the financial, managerial, operational, and staffing resources set aside for compliance with the Exchange Act and the rules and regulations thereunder relating to its business as a SBS or MSBSP, including any material deficiencies in such resources.⁶⁷⁹ The compliance report must be submitted to the Commission within 30 days following the deadline for filing the SBS Entity's annual financial report.⁶⁸⁰

SBS Entities' operations also are governed, in part, by paragraph (b) of Rule 15Fh-3 in that they must, at a reasonably sufficient time prior to entering into a security-based swap, disclose to a counterparty (other than a SBS, MSBSP, swap dealer, or major swap participant) material information concerning the security-based swap in a manner reasonably designed to allow the counterparty to assess material risks and characteristics as well as material incentives or conflicts of interest.⁶⁸¹ Relevant risks may include market, credit, liquidity, foreign currency, legal, operational, and any other applicable risks.⁶⁸² Further, SBSs must establish, maintain, and enforce written policies and procedures reasonably designed to

obtain and retain a record of the essential facts concerning each counterparty whose identity is known to the SBS that are necessary for conducting business with such counterparty.⁶⁸³ Among other things, the essential facts regarding the counterparty are facts required to implement the SBS's operational risk management policies in connection with transactions entered into with such counterparty.⁶⁸⁴

iv. SBSDRs

Section 13(n) of the Exchange Act specifies the requirements and core principles with which SBSDRs are required to comply. The Commission adopted rules that cover the receiving and maintenance of security-based swap data, how entities can access such information, and the maintaining the continued privacy of confidential information. Security-based swap data repositories must have written policies and procedures reasonably designed to review any prohibition or limitation of any person with respect to access to services offered, directly or indirectly, or data maintained by the SBSDR.⁶⁸⁵

The SBSDRs must enforce written policies and procedures reasonably designed to protect the privacy of security-based swap transaction information.⁶⁸⁶ As a result, they must establish and maintain safeguards, policies, and procedures reasonably designed to prevent the misappropriation or misuse, directly or indirectly, of confidential information, including, but not limited to, trade data; position data; and any nonpublic personal information about a market participant or any of its customers, material, nonpublic information, and/or intellectual property, such as trading strategies or portfolio positions, by the SBSDR or any person associated with the SBSDR for personal benefit or for the benefit of others. Such safeguards, policies, and procedures must address, without limitation: (1) limiting access to such confidential information, material, nonpublic information, and intellectual property; (2) standards pertaining to trading by persons associated with the SBSDR for their personal benefit or for the benefit of others; and (3) adequate oversight to ensure compliance with these safeguards. These rules cover potential unauthorized access from within or outside of the SBSDR, which could include a cybersecurity breach.⁶⁸⁷

Additionally, a SBSDR must furnish to a market participant, prior to accepting its securities-based swap data, a disclosure document that contains information from which the market participant can identify and evaluate accurately the risks and costs associated with using the services of the SBSDR.⁶⁸⁸ Key points include, among other things, the criteria for providing others with access to services offered and data maintained by the SBSDR; criteria for those seeking to connect to or link with the SBSDR; policies and procedures regarding the SBSDR's safeguarding of data and operational reliability, as described in Rule 13n-6; policies and procedures reasonably designed to protect the privacy of any and all security-based swap transaction information that the SBSDR receives from a SBS, counterparty, or any registered entity, as described in Rule 13n-9(b)(1); policies and procedures regarding its non-commercial and/or commercial use of the security-based swap transaction information that it receives from a market participant, any registered entity, or any other person; dispute resolution procedures involving market participants, as described in Rule 13n-5(b)(6); and governance arrangements of the swap-based security data repository.⁶⁸⁹

v. Transfer Agents

Transfer agents registered with the Commission (but not transfer agents registered with another appropriate regulatory agency) are subject to the Regulation S-P Disposal Rule.⁶⁹⁰ Transfer agents also may be subject to Regulation S-ID if they are "financial institutions" or "creditors."⁶⁹¹ As discussed earlier, the Regulation S-P Disposal Rule and Regulation S-ID have provisions requiring policies and procedures to address certain types of cybersecurity risks.⁶⁹²

Rule 17Ad-12 requires transfer agents to ensure that all securities are held in safekeeping and are handled, in light of all facts and circumstances, in a manner that is reasonably free from risk of theft, loss, or destruction. In addition, the transfer agent must ensure that funds

⁶⁸⁸ See 17 CFR 240.13n-10.

⁶⁸⁹ See 17 CFR 240.13n-10(b).

⁶⁹⁰ See 17 CFR 248.30(b)(2).

⁶⁹¹ See 17 CFR 248.201 and 202. The scope of Regulation S-ID includes any financial institution or creditor, as defined in the Fair Credit Reporting Act (15 U.S.C. 1681) that is required to be "registered under the Securities Exchange Act of 1934." See 17 CFR 248.201(a).

⁶⁹² See section II.F.1.c. of this release (discussing in more detail the existing requirements of the Regulation S-P Disposal Rule and Regulation S-ID to have policies and procedures to address certain cybersecurity risks).

⁶⁷⁸ See 17 CFR 240.15Fk-1(b)(2). The CCO also must administer each policy and procedure that is required to be established pursuant to section 15F of the Exchange Act and the rules and regulations thereunder. See 17 CFR 240.15Fk-1(b)(4).

⁶⁷⁹ See 17 CFR 240.15Fk-1(c)(2).

⁶⁸⁰ *Id.*

⁶⁸¹ See 17 CFR 240.15Fh-3(b).

⁶⁸² See 17 CFR 240.15Fh-3(b)(1).

⁶⁸³ See 17 CFR 240.15Fh-3(e).

⁶⁸⁴ See 17 CFR 240.15Fh-3(e)(2).

⁶⁸⁵ 17 CFR 240.13n-4(c)(1)(iv).

⁶⁸⁶ 17 CFR 240.13n-9(b)(1).

⁶⁸⁷ 17 CFR 240.13n-9(b)(2).

are protected, in light of all facts and circumstances, against misuse. In evaluating which particular safeguards and procedures must be employed, the cost of the various safeguards and procedures as well as the nature and degree of potential financial exposure are two relevant factors.⁶⁹³

Transfer agents are subject indirectly to state corporation law when acting as agents of corporate issuers, and they are directly subject to state commercial law, principal-agent law, and other laws, many of which are focused on corporate governance and the rights and obligations of issuers and securityholders.⁶⁹⁴ The transfer of investment securities is primarily governed by UCC Article 8, which has been adopted by the legislatures of all 50 states,⁶⁹⁵ the District of Columbia, Puerto Rico, and the Virgin Islands. Transfer agents may also be subject to the laws of the states of incorporation for both issuers and their securityholders that apply to specific services provided by the transfer agent, such as data privacy.⁶⁹⁶

c. Market Entities Subject to CFTC Regulations

Certain types of Market Entities are dually registered with the Commission and the CFTC. For example, some clearing agencies are registered with the CFTC as derivative clearing organizations (“DCOs”) and some SBSDRs are registered with the CFTC as swap data repositories (“SDRs”). In addition, some broker-dealers are registered with the CFTC as futures commission merchants (“FCMs”) or swap dealers. Most currently registered SBSDRs are also registered with the CFTC as swap dealers. As CFTC registrants, these Market Entities are subject to requirements that pertain to cybersecurity or are otherwise relevant to the proposals in this release.

i. Requirements for DCOs

DCOs are subject to a CFTC systems safeguards rule.⁶⁹⁷ This rule requires

⁶⁹³ 17 CFR 240.17Ad-12(a).

⁶⁹⁴ See, e.g., Del. Code Ann. tit. 8 (Delaware General Corporation Law), Del. Code Ann. tit. 6, art. 8 (Investment Securities), Restatement (Third) of Agency (2006).

⁶⁹⁵ Louisiana has enacted the provisions of Article 8 into the body of its law, among others, but has not adopted the UCC as a whole.

⁶⁹⁶ For example, California’s privacy statute which became effective in 2003, was the first significant effort by a state to assert substantive regulation of privacy of customer data. See Cal. Civ. Code §§ 1798.80–1798.84. While state regulations vary across jurisdictions, other states have followed suit with similar regulatory initiatives. See, e.g., Minn. Stat. § 325E.61, Neb. Rev. Stat. §§ 87–801–807.

⁶⁹⁷ See 17 CFR 39.18.

them—among other things—to establish and maintain: (1) a program of risk analysis and oversight with respect to their operations and automated systems to identify and minimize sources of operational risk; and (2) a business continuity and disaster recovery plan, emergency procedures, and physical, technological, and personnel resources sufficient to enable the timely recovery and resumption of operations and the fulfillment of each obligation and responsibility of the DCO, including, but not limited to, the daily processing, clearing, and settlement of transactions, following any disruption of its operations.⁶⁹⁸ The safeguards rule also requires vulnerability and penetration testing (among other things).⁶⁹⁹ Further, it requires notice to the CFTC staff if the DCO experiences certain exceptional events.⁷⁰⁰

ii. Requirements for SDRs

SDRs are subject to a CFTC systems safeguards rule.⁷⁰¹ This rule requires them—among other things—to: (1) establish and maintain a program of risk analysis and oversight to identify and minimize sources of operational risk through the development of appropriate controls and procedures and the development of automated systems that are reliable, secure, and have adequate scalable capacity; (2) establish and maintain emergency procedures, backup facilities, and a business continuity-disaster recovery plan that allow for the timely recovery and resumption of operations and the fulfillment of their duties and obligations as an SDR; and (3) periodically conduct tests to verify that backup resources are sufficient to ensure continued fulfillment of all their duties under the Commodity Exchange Act and the CFTC’s regulations.⁷⁰² The program of risk analysis and oversight required by the SDR safeguards rule—among other things—must address: (1)

⁶⁹⁸ See 17 CFR 39.18(b) and (c). The program of risk analysis and oversight must include—among other elements—information security, including, but not limited to, controls relating to: access to systems and data (including, least privilege, separation of duties, account monitoring and control); user and device identification and authentication; security awareness training; audit log maintenance, monitoring, and analysis; media protection; personnel security and screening; automated system and communications protection (including, network port control, boundary defenses, encryption); system and information integrity (including, malware defenses, software integrity monitoring); vulnerability management; penetration testing; security incident response and management; and any other elements of information security included in generally accepted best practices. See 17 CFR 39.18(b)(2)(i).

⁶⁹⁹ See 17 CFR 39.18(e).

⁷⁰⁰ See 17 CFR 39.18(g).

⁷⁰¹ See 17 CFR 49.24.

⁷⁰² See 17 CFR 49.24(a).

information security; and (2) business continuity-disaster recovery planning and resources.⁷⁰³ The safeguards rule also requires the SDR to notify the CFTC promptly of—among other events—all cyber security incidents or targeted threats that actually or potentially jeopardize automated systems operation, reliability, security, or capacity.⁷⁰⁴

iii. Requirements for FCMs and Swap Dealers

The CFTC does not have a cybersecurity regime for FCMs and swap dealers comparable to that being proposed in this release.⁷⁰⁵ However, FCMs and swap dealers are currently subject to information security requirements by virtue of their membership with the National Futures Association (NFA).⁷⁰⁶ Specifically, NFA

⁷⁰³ See 17 CFR 49.24(b)(2) and (3). For the purposes of the SDR safeguards rule, information security includes, but is not limited to, controls relating to: access to systems and data (including least privilege, separation of duties, account monitoring and control); user and device identification and authentication; security awareness training; audit log maintenance, monitoring, and analysis; media protection; personnel security and screening; automated system and communications protection (including network port control, boundary defenses, encryption); system and information integrity (including malware defenses, software integrity monitoring); vulnerability management; penetration testing; security incident response and management; and any other elements of information security included in generally accepted best practices. See 17 CFR 49.24(b)(2).

⁷⁰⁴ See 17 CFR 49.24(g)(2).

⁷⁰⁵ Current CFTC requirements relating to information security for FCMs and swap dealers are more general in nature or limited in application. See, e.g., 17 CFR 23.600(c)(4)(vi) (providing that swap dealer’s risk management program policies and procedures shall take into account, among other things, secure and reliable operating and information systems with adequate, scalable capacity, and independence from the business trading unit; safeguards to detect, identify, and promptly correct deficiencies in operating and information systems; and reconciliation of all data and information in operating and information systems); 162.21, 160.30 (requiring FCMs and swap dealers to adopt written policies and procedures addressing administrative, technical, and physical safeguards with respect to the information of consumers). The current CFTC Chairman has, however, announced support for developing cybersecurity requirements for FCMs and swap dealers. See CFTC, Address of Chairman Rostin Behnam at the ABA Business Law Section Derivatives & Futures Law Committee Winter Meeting (Feb. 3, 2023), available at <https://www.cftc.gov/PressRoom/SpeechesTestimony/opabehnam31>.

⁷⁰⁶ See NFA, *Interpretive Notice 9070—NFA Compliance Rules 2–9, 2–36 and 2–49: Information Systems Security Programs* (Sept. 30, 2019), available at <https://www.nfa.futures.org/rulebooks/sql/rules.aspx?RuleID=9070&Section=9>. NFA has also issued guidance relating to the oversight of third-party service providers. See NFA, *Interpretive Notice 9079—NFA Compliance Rules 2–9 and 2–36: Members’ Use of Third-Party Service Providers* (Sept. 30, 2021), available at <https://>

examines swap dealers and FCMs for compliance with NFA Interpretive Notice 9070, which establishes general requirements for NFA members relating to their information systems security programs (ISSPs).⁷⁰⁷ The notice requires members to adopt and enforce a written ISSP reasonably designed to provide safeguards to protect against security threats or hazards to their technology systems. The safeguards must be appropriate to the member's size, complexity of operations, type of customers and counterparties, the sensitivity of the data accessible within its systems, and its electronic interconnectivity with other entities. The notice further provides guidance on how to meet this requirement, including that members should document and describe the safeguards in the ISSP, identify significant internal and external threats and vulnerabilities, create an incident response plan, and monitor and regularly review their ISSPs for effectiveness, among other things. Members should also have procedures to promptly notify NFA in the form and manner required of a cybersecurity incident related to the member's commodity interest business and that results in: (1) any loss of customer or counterparty funds; (2) any loss of a member's own capital; or (3) in the member providing notice to customers or counterparties under state or federal law.

The CFTC does require swap dealers to establish and maintain a business continuity and disaster recovery plan that outlines the procedures to be followed in the event of an emergency or other disruption of their normal business activities.⁷⁰⁸ The business

www.nfa.futures.org/rulebooksqll/rules.aspx?Section=9&RuleID=9079.

⁷⁰⁷ *Id.*

⁷⁰⁸ See 17 CFR 23.603. The business continuity and disaster recovery plan must include: (1) the identification of the documents, data, facilities, infrastructure, personnel and competencies essential to the continued operations of the swap dealer and to fulfill its obligations; (2) the identification of the supervisory personnel responsible for implementing each aspect of the business continuity and disaster recovery plan and the emergency contacts required to be provided; (3) a plan to communicate with specific persons in the event of an emergency or other disruption, to the extent applicable to the operations of the swap dealer; (4) procedures for, and the maintenance of, back-up facilities, systems, infrastructure, alternative staffing and other resources to achieve the timely recovery of data and documentation and to resume operations as soon as reasonably possible and generally within the next business day; (5) maintenance of back-up facilities, systems, infrastructure and alternative staffing arrangements in one or more areas that are geographically separate from the swap dealer's primary facilities, systems, infrastructure and personnel (which may include contractual arrangements for the use of facilities, systems and infrastructure provided by

continuity and disaster recovery plan must be designed to enable the swap dealer to continue or to resume any operations by the next business day with minimal disturbance to its counterparties and the market, and to recover all documentation and data required to be maintained by applicable law and regulation.⁷⁰⁹ The business continuity and disaster recovery plan must—among other requirements—be tested annually by qualified, independent internal personnel or a qualified third party service.⁷¹⁰ The date the testing was performed must be documented, together with the nature and scope of the testing, any deficiencies found, any corrective action taken, and the date that corrective action was taken.⁷¹¹

d. Market Entities Subject to Federal Banking Regulations

Broker-dealers affiliated with a banking organization⁷¹² and some SBS Entities and transfer agents that are banking organizations are subject to the requirements of prudential regulators such as the FDIC, Federal Reserve Board, and the OCC. These prudential regulators have rules requiring banking organizations to notify them no later than 36 hours after learning of a “computer-security incident,” which is defined “as an occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits.”

The rule also requires a bank service provider to notify at least one bank-designated point of contact at each affected customer bank as soon as possible when it determines it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to disrupt or degrade, covered services provided to the bank for four or more hours. If the bank has not previously provided a designated point of contact, the notification must be made to the

third parties); (6) back-up or copying, with sufficient frequency, of documents and data essential to the operations of the swap dealer or to fulfill the regulatory obligations of the swap dealer and storing the information off-site in either hard-copy or electronic format; and (7) the identification of potential business interruptions encountered by third parties that are necessary to the continued operations of the swap dealer and a plan to minimize the impact of such disruptions. See 17 CFR 23.603(b).

⁷⁰⁹ See 17 CFR 23.603(a).

⁷¹⁰ See 17 CFR 23.603(g).

⁷¹¹ *Id.*

⁷¹² In the simplification of the Volcker Rule, effective Jan. 21, 2020, Commission staff estimated that there were 202 broker-dealers that were affiliated with banking organizations.

bank's chief executive officer (“CEO”) and CIO or to two individuals of comparable responsibilities.”⁷¹³ Prudential regulators have also published guidance for banking organizations relating to cybersecurity.⁷¹⁴

e. Information Sharing

Information sharing is an important part of cybersecurity. Alerts that are issued by the Commission or by the securities industry make Market Entities aware of trends in cybersecurity incidents and potential threats. This advanced warning can help Market Entities to prepare for future cybersecurity attacks by testing and upgrading their cybersecurity infrastructure.

The value of such information sharing has long been recognized. In 1998, Presidential Decision Directive 63 established industry-based information sharing and analysis centers (“ISACs”) to promote the disclosure and sharing of cybersecurity information among firms.⁷¹⁵ The FS-ISAC provides financial firms with such a forum.⁷¹⁶ However, observers have questioned the efficacy of these information-sharing partnerships.⁷¹⁷ Although the Commission does not have data on the extent of Market Entities' use of such forums or their efficacy, surveys of securities firms conducted by FINRA suggest that there is considerable variation in firms' willingness to share

⁷¹³ See 12 CFR 53.1 through 53.4 (OCC); 12 CFR 225.300 through 225.303 (Federal Reserve Board); 12 CFR 304.21 through 24 (FDIC).

⁷¹⁴ See, e.g., SR 21-14: *Authentication and Access to Financial Institution Services and Systems* (Aug. 11, 2021), available at <https://www.federalreserve.gov/supervisionreg/srletters/sr2114.htm>; SR 15-9: *FFIEC Cybersecurity Assessment Tool for Chief Executive Officers and Boards of Directors* (July 2, 2015), available at <https://www.federalreserve.gov/supervisionreg/srletters/sr1509.htm>; SR 05-23/CA 05-10: *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* (Dec. 1, 2005), available at <https://www.federalreserve.gov/boarddocs/srletters/2005/SR0523.htm>.

⁷¹⁵ See *President Decision Directive/NSC-63, Critical Infrastructure Protection* (May 22, 1998); *President Decision Directive 63, Critical Infrastructure Protection: Sector Coordinators*, 98 FR 41804 (Aug. 5, 1998) (notice and request for expressions of interest); see also National Council of ISACs, available at <https://www.nationalisacs.org>.

⁷¹⁶ Information about FS-ISAC is available at <https://www.fsisac.com>.

⁷¹⁷ See James A. Lewis and Denise E. Zheng, *Cyber Threat Information Sharing*, 2015 Cre. for Strategic and Int'l Stud. 62 (Mar. 2015) (stating that the “benefits of information sharing, when done correctly, are numerous” but that [p]rogrammatic, technical, and legal challenges, as well as lack of buy-in from the stakeholder community, are the key impediments” to effective information-sharing partnerships).

information about cybersecurity threats on a voluntary basis, with larger firms being more likely to do so.⁷¹⁸ Similarly, a recent survey of financial firms found that while recognition of the value of information-sharing arrangements is widespread, the majority of firms report hesitance to participate due to regulatory restrictions or privacy concerns.⁷¹⁹

Market surveillance and regulatory activities—such as enforcement by SROs—can result in information sharing with—and referrals to—the Commission and other federal agencies, particularly if the issues being investigated are cybersecurity related.

f. Adequacy of Current Cybersecurity Policies and Procedures

While spending on cybersecurity measures in the financial services industry is considerable, and the growing risk of cybersecurity events has led many corporate executives to significantly increase their cybersecurity budget,⁷²⁰ the budget levels themselves are not the most important facet of a cybersecurity program.⁷²¹ In a recent survey of 20 consumer/financial (non-banking) services firms, respondents ranked cybersecurity budget levels lower than other facets of cybersecurity maintenance.⁷²² For example, financial companies’ boards and management teams indicated that overall cybersecurity strategy, the identification threats and cybersecurity risks, the firm’s susceptibility to breaches when other financial institutions are successfully attacked, and the results of cybersecurity testing all ranked higher

than security budgets themselves.⁷²³ Surveys of financial services firms indicate that 10.5% of their information technology budgets are spent on cybersecurity, and the per-employee expenditure is approximately \$2,348 annually as of 2020.⁷²⁴ This per-employee value can be used to estimate the cybersecurity expenditures at each of the Market Entities that would be affected by the proposed rule.⁷²⁵

2. Market Structure

a. Broker-Dealers

The operations and functions of broker-dealers are discussed earlier in this release.⁷²⁶ The following broker-dealers would be Covered Entities: (1) broker-dealers that maintain custody of securities and cash for customers or other broker-dealers (*i.e.*, carrying broker-dealers); (2) broker-dealers that introduce their customer accounts to a carrying broker-dealer on a fully disclosed basis (*i.e.*, introducing broker-dealers); (3) broker-dealers with regulatory capital equal to or exceeding \$50 million; (4) broker-dealers with total assets equal to or exceeding \$1 billion; (5) broker-dealers that operate as market makers; and (6) broker-dealers that operate an ATS.⁷²⁷ Broker-dealers that do not fall into one of those six categories would not be Covered Entities (*i.e.*, they would be Non-Covered Broker-Dealers). As discussed above, broker-dealers that are Covered Entities would be subject to additional policies and procedures, reporting, and disclosure requirements under proposed Rule 10.⁷²⁸ These additional

requirements would not apply to broker-dealers that are not Covered Entities.⁷²⁹

Table 1 presents a breakdown of all broker-dealers registered with the Commission as of the third quarter of 2022. Based on 2022 FOCUS Part II/IIA data, there were 3,510 registered broker-dealers with average total assets of \$1.5 billion and average regulatory capital of \$144 million. Of those broker-dealers, 1,541 would be classified as Covered Entities with average total assets of \$3.5 billion and average regulatory capital of \$325 million. Meanwhile, the 1,969 brokers that would be classified as Non-Covered Broker-Dealers were generally much smaller than broker-dealers that would be classified as Covered Entities, having an average total asset level of \$4.7 million and regulatory capital of \$3 million. In other words, Non-Covered Broker-Dealers accounted for only about 0.2 percent of total asset value and only 0.1 percent of total regulatory capital in the third quarter of 2022.

The majority of small broker-dealers, as defined by Rule 0–10⁷³⁰ were classified as Non-Covered Broker-Dealers (74%) compared to a minority of small broker-dealers that were classified as Covered Entities (26%), which means that most small broker-dealers would be subject to the less stringent regulatory requirements under the proposed Rule 10 for Non-Covered Broker-Dealers. The small broker-dealers that qualified as Covered Entities and would be subject to additional requirements of proposed Rule 10 generally were broker-dealers that introduce their customer accounts to carrying broker-dealers on a fully disclosed basis.

TABLE 1—BROKER-DEALERS AS COVERED ENTITIES AS OF SEPTEMBER 2022
[Average broker-dealer total assets and regulatory equity]

Categories of covered BDs	Total number of BDs	Number of small BDs included	Number of retail BDs	Average total assets (millions)	Average regulatory equity (millions)
Carrying	162	0	145	\$28,250.9	\$2,528.7
Introducing	1219	195	1106	103.0	44.3
Market making	19	0	1	179.2	17.4

⁷¹⁸ See FINRA Report on Cybersecurity Practices. Survey respondents included large investment banks, clearing firms, online brokerages, high-frequency traders, and independent dealers.

⁷¹⁹ See Julie Bernard, Mark Nicholson, and Deborah Golden, *Reshaping the Cybersecurity Landscape*, Deloitte (Jul. 24, 2020), available at <https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html> (“Reshaping the Cybersecurity Landscape”). Survey respondents consisted of CISOs (or equivalent) of 53 members of the FS-ISAC. Of the respondents, 24 reported being in the retail/corporate banking sector, 20 reported being in the consumer/financial services (non-banking) sector, and 17 reported being in the insurance sector. Other respondents included IT service providers, financial utilities, trade

associations, and credit unions. Some respondents reported being in multiple sectors.

⁷²⁰ For example, according to one source, as of 2020, “55% of enterprise executives [were planning] to increase their cybersecurity budgets in 2021 and 51% are adding full-time cyber staff in 2021.” Louis Columbus, *The Best Cybersecurity Predictions for 2021 Roundup*, Forbes.com (Dec. 15, 2020), available at <https://www.forbes.com/sites/louiscolombus/2020/12/15/the-best-cybersecurity-predictions-for-2021-roundup/?sh=6d6db8b65e8c>.

⁷²¹ See *Reshaping the Cybersecurity Landscape*.

⁷²² *Id.*

⁷²³ *Id.*

⁷²⁴ *Id.*

⁷²⁵ The per-employee expenditure can be multiplied by the Market Entity’s employee head count on a full-time equivalent basis to estimate its spending on cybersecurity protection.

⁷²⁶ See section I.A.2.b. of this release.

⁷²⁷ See paragraphs (a)(1)(i)(A) through (F) of proposed Rule 10.

⁷²⁸ See paragraph (b) through (d) of proposed Rule 10 (setting forth the requirements for Market Entities that meet the definition of “covered entity”).

⁷²⁹ See paragraph (e) of proposed Rule 10 (setting forth the requirements for Market Entities that do not meet the definition of “covered entity”).

⁷³⁰ See 17 CFR 240.0–10 (“Rule 0–10”) for definition of small entities including small broker-dealers under the Exchange Act for purposes of the Regulatory Flexibility Act (“RFA”). This definition is for the economic analysis only. See also section VI of this release (setting forth the Commission’s RFA analysis).

TABLE 1—BROKER-DEALERS AS COVERED ENTITIES AS OF SEPTEMBER 2022—Continued
[Average broker-dealer total assets and regulatory equity]

Categories of covered BDs	Total number of BDs	Number of small BDs included	Number of retail BDs	Average total assets (millions)	Average regulatory equity (millions)
ATS	36	0	21	4.1	3.1
>\$50 Million Regulatory Equity and/or >\$1 billion total assets	105	0	44	6,891.6	351.5
Covered	1541	195	1317	3,523.3	325.1
Non-Covered	1969	569	1115	4.7	3.0
Total	3510	764	2432	1,549.9	144.4

Covered Broker-Dealers provide a broad spectrum of services to their clients, including, for example: trade execution, clearing, market making, margin and securities lending, sale of investment company shares, research services, underwriting and selling, retail sales of corporate securities, private placements, and government and Series

K securities sales and trading. In contrast, Non-Covered Broker-Dealers tend to offer a more focused and limited set of services.

In terms of specific services offered, as presented in Table 2 below, while the majority of broker-dealers that are Covered Entities have lines of business devoted to broker and dealer services

across a broad spectrum of financial instruments, Non-Covered Broker-Dealers as a whole focus on private placements. In addition, a significant minority of Non-Covered Broker-Dealers also engages in mutual fund sales and underwriting, variable contract sales, corporate securities underwriting, and direct investment offerings.

TABLE 2—LINES OF BUSINESS AT BROKER-DEALERS AS OF SEPTEMBER 2022 *
[Percent of covered entity and non-covered broker-dealers engaged in each line of business]

Line of business	Percent of covered broker-dealers (percent)	Percent of non-covered broker-dealers (percent)
Retailing Corporate Equity Securities Over The Counter	76.4	8.1
Corporate Debt Securities	69.6	7.9
Mutual Funds	62.2	19.5
Private Placements	58.1	72.1
Options	58.1	3.7
US Government Securities Broker	56.2	3.9
Municipal Debt/Bonds—Broker	53.1	6.4
Other Securities Business	52.0	65.1
Underwriter—Corporate Securities	45.0	11.5
Trading Via Floor Broker	43.4	5.7
Variable Contracts	42.4	16.3
Proprietary Trading	40.4	3.8
Investment Advisory Services	25.8	4.6
Municipal Debt/Bonds—Dealer	25.4	1.5
Direct investments—Primary	21.2	13.2
US Government Securities Dealer	20.7	0.9
Other Non-Securities Business	18.1	11.2
Time Deposits	16.5	1.2
Commodities	12.5	1.1
Market Making	12.3	0.6
Mortgage or Asset Backed Securities	11.9	1.3
Bank Networking/Kiosk Relationship	11.0	0.4
Internet/Online Trading Accounts	10.8	0.5
Exchange Non-Floor Activities	10.6	0.9
Direct investments—Secondary	8.2	2.0
Oil and Gas Interests	7.9	3.1
Underwriter—Mutual Funds	6.4	7.8
Exchange Floor Activities	5.9	1.2
Executing Broker	5.5	0.6
Day Trading Accounts	4.8	0.3
Insurance Networking/Kiosk Relationship	4.7	0.6
Non Profit Securities	4.2	0.4
Real Estate Syndication	2.8	2.8
Prime Broker	1.6	0.0
Issuer Affiliated Broker	1.2	1.1
Clearing Broker in a Prime Broker Arrangement	1.2	0.0
Crowdfunding FINRA Rule 4518 (a)	0.7	1.1
Funding Portal	0.2	0.3
Crowdfunding FINRA Rule 4518 (b)	0.1	0.3

TABLE 2—LINES OF BUSINESS AT BROKER-DEALERS AS OF SEPTEMBER 2022 *—Continued
 [Percent of covered entity and non-covered broker-dealers engaged in each line of business]

Line of business	Percent of covered broker-dealers (percent)	Percent of non-covered broker-dealers (percent)
Capital Acquisition Broker	0.1	1.2

* This information is derived from Form BD, Question 12.

As of November 2022, there were 33 NMS Stock ATSs with an effective Form ATS–N on file with the Commission⁷³¹ and 68 non-NMS Stock ATSs with a Form ATS on file with the Commission.⁷³² Most broker-dealer ATS operators operate a single ATS.

b. Clearing Agencies

The operations and functions of clearing agencies are discussed earlier in this release.⁷³³ A clearing agency (whether registered with the Commission or exempt) would be considered a Covered Entity under proposed Rule 10.⁷³⁴ There are a total of 16 clearing agencies that would meet the definition of a Covered Entity under proposed Rule 10. There are seven registered and active clearing agencies: DTC, FICC, NSCC, ICC, ICEEU, the Options Clearing Corp., and LCH SA. Two clearing agencies are registered with the Commission but are inactive and currently do not provide clearing and settlement activities. Those clearing agencies are the BSECC and SCCP.⁷³⁵ In addition, there are five clearing agencies that are exempt from registering with the Commission. Those exempt clearing agencies are DTCC ITP Matching U.S. LLC, Bloomberg STP LLC, and SS&C Technologies, Inc., which provide

matching services; and Clearstream Banking, S.A. and Euroclear Bank SA/NV, which provide clearing agency services with respect to transactions involving U.S. government and agency securities for U.S. participants.⁷³⁶

Of the seven operating registered clearing agencies, six provide CCP clearing services and one provides CSD services. In addition, NSCC, FICC, and DTC are all registered clearing agencies that are subsidiaries of the Depository Trust and Clearing Corporation. Together, this subset of registered clearing agencies offer clearing and settlement services for equities, corporate, and municipal bonds, government and mortgage-backed securities, derivatives, money market instruments, syndicated loans, mutual funds, and alternative investment products in the United States. ICC and ICEEU are both registered clearing agencies for credit default swaps (“CDS”) and are both subsidiaries of ICE. LCH SA, a France-based subsidiary of LCH Group Holdings Ltd, is a registered clearing agency that also offers clearing for CDS. The seventh registered clearing agency, the Options Clearing Corp., offers clearing services for exchange-traded U.S. equity options.

c. The MSRB

The operations and functions of the MSRB are discussed earlier in this release.⁷³⁷ The MSRB would be considered a Covered Entity under proposed Rule 10.⁷³⁸ As an SRO registered with the Commission, the MSRB protects municipal securities investors, municipal entities, obligated persons, and the public interest. While the MSRB used to only regulate the activities of broker-dealers and banks that buy, sell, and underwrite municipal securities, it regulates certain activities of municipal advisors.

⁷³⁶ In addition to the 14 clearing agencies discussed above, the Commission’s expects that two entities may apply to register or to seek an exemption from registration as a clearing agency in the next three years. As a result, they were included in the PRA in section V.

⁷³⁷ See section I.A.2.d. of this release.

⁷³⁸ See paragraph (a)(1)(iv) of proposed Rule 10.

d. National Securities Associations

The operations and functions of national securities association are discussed earlier in this release.⁷³⁹ A national securities association would be considered a Covered Entity under proposed Rule 10.⁷⁴⁰ FINRA currently is the only national securities association registered with the Commission and is a not-for-profit organization with 3,700 employees that oversees broker-dealers, including their branch offices, and registered representatives through examinations, enforcement, and surveillance.

FINRA, among other things, provides a forum for securities arbitration and mediation; conducts market regulation, including by contract for a majority of the national securities exchanges; regulates its broker-dealer members; administers testing and licensing of registered persons; collects and stores regulatory filings;⁷⁴¹ and operates industry utilities such as Trade Reporting Facilities.⁷⁴² Through the collection of regulatory filings submitted by broker-dealers as well as stock options and fixed-income quote, order, and trade data, FINRA maintains certain confidential information—not only its own but of other SROs.

e. National Securities Exchanges

The operations and functions of the national securities exchanges are discussed earlier in this release.⁷⁴³ A national securities exchange would be considered a Covered Entity under proposed Rule 10.⁷⁴⁴ There are 24

⁷³⁹ See section I.A.2.e. of this release.

⁷⁴⁰ See paragraph (a)(1)(i)(v) of proposed Rule 10.

⁷⁴¹ Some of the filings collected include FOCUS reports; Form OBS; Form SSOI; Form Custody; firm clearing arrangements filings; Blue Sheets; customer margin balance reporting; short interest reporting; Form PF; Form 211; public offering and private placement related filings; FINRA Rules 4311 and 4530 reporting; subordination agreements; and Regulations M, T, and NMS.

⁷⁴² These include Trade Reporting and Compliance Engine (TRACE), OTC ATS and Non-ATS data, Over-the-Counter Reporting Facility (ORF), Trade Reporting Facility (TRF), Alternative Display Facility (ADF), and Order Audit Trail System (OATS) (phased out as of 2021).

⁷⁴³ See section I.A.2.f. of this release.

⁷⁴⁴ See paragraph (a)(1)(vi) of proposed Rule 10.

⁷³¹ See Form ATS–N Filings and Information, available at <https://www.sec.gov/divisions/marketreg/form-ats-n-filings.htm>.

⁷³² See the current list of registered ATSs on the Commission’s website, available at <https://www.sec.gov/foia/docs/atstlist>.

⁷³³ See section I.A.2.c. of this release.

⁷³⁴ See paragraph (a)(1)(iii). of proposed Rule 10.

⁷³⁵ BSECC and SCCP have not provided clearing services in over a decade. See BSECC Notice (stating that BSECC “returned all clearing funds to its members by September 30, 2010, and [] no longer maintains clearing members or has any other clearing operations as of that date BSECC [] maintain[s] its registration as a clearing agency with the Commission for possible active operations in the future”); SCCP Notice (noting that SCCP “returned all clearing fund deposits by September 30, 2009; [and] as of that date SCCP no longer maintains clearing members or has any other clearing operations SCCP [] maintain[s] its registration as a clearing agency for possible active operations in the future.”). BSECC and SCCP are included in the economic baseline and must be considered in the benefits and costs analysis due to their registration with the Commission. They also are included in the PRA for purposes of the PRA estimate. See section V of this release (setting forth the Commission’s PRA analysis).

national securities exchanges⁷⁴⁵ currently registered with the Commission that would meet the definition of a Covered Entity under proposed Rule 10(a)(1): BOX Exchange LLC; Cboe BYX Exchange, Inc.; Cboe BZX Exchange, Inc.; Cboe C2 Exchange, Inc.; Cboe EDGA Exchange, Inc.; Cboe EDGX Exchange, Inc.; Cboe Exchange, Inc.; Investors Exchange LLC; Long-Term Stock Exchange, Inc.; MEMX, LLC; Miami International Securities Exchange; MIAX Emerald, LLC; MIAX PEARL, LLC; Nasdaq BX, Inc.; Nasdaq GEMX, LLC; Nasdaq ISE, LLC; Nasdaq MRX, LLC; Nasdaq PHLX LLC; The Nasdaq Stock Market; New York Stock Exchange LLC; NYSE Arca, Inc.; NYSE Chicago, Inc.; NYSE American, LLC; and NYSE National, Inc.⁷⁴⁶

f. SBS Entities and SBSDRs

Operations and functions of SBS Entities and SBSDRs are discussed earlier in this release.⁷⁴⁷ An SBS Entity and an SBSDR would be considered a Covered Entity under proposed Rule 10.⁷⁴⁸ As of January 4, 2023, there were 50 registered SBSs that would meet the definition of a Covered Entity under proposed Rule 10(a)(1).⁷⁴⁹ There were no MSBSPs as of January 4, 2023.

There are three SBSDRs that would meet the definition of a Covered Entity under proposed Rule 10(a)(1). The Commission has two registered security-based swap data repositories (ICE Trade Vault, LLC and DTCC Data Repository (U.S.), LLC). GTR North America provides transaction reporting services for derivatives in the United States through the legal entity DTCC Data Repository (U.S.) LLC. DTCC Data Repository (U.S.), LLC enables firms to meet their reporting obligations under the Dodd-Frank Act and accepts trade submissions directly from reporting firms as well as through third-party service providers.⁷⁵⁰ In addition to the two registered SBSDRs, the Commission expects that an additional entity may

apply to be a registered SBSDR in the next three years.

g. Transfer Agents

The operations and functions of transfer agents are discussed earlier in this release.⁷⁵¹ Transfer agents would be Covered Entities under proposed Rule 10.⁷⁵² Transfer agents generally work for issuers of securities. Among other functions, they may: (1) track, record, and maintain on behalf of issuers the official record of ownership of each issuer's securities; (2) cancel old certificates, issue new ones, and perform other processing and recordkeeping functions that facilitate the issuance, cancellation, and transfer of securities; (3) facilitate communications between issuers and registered securityholders; and (4) make dividend, principal, interest, and other distributions to securityholders.⁷⁵³ Transfer agents are required to be registered with the Commission, or if the transfer agent is a bank, then with a bank regulatory agency. As of December 31, 2022, there were 353 registered transfer agents.⁷⁵⁴

h. Service Providers

Many Market Entities utilize service providers to perform some or all of their cybersecurity functions. Market Entities that are large—relative to other Market Entities—in terms of their total assets, number of clients or members, or daily transactions processed are likely to have significant information technology, their own information technology departments and dedicated staff such that some functions are performed in-house. Other services may be contracted out to service providers that cater to Market Entities. Smaller Market Entities that do not have large technology budgets may rely more heavily (or completely) on third parties for their cybersecurity needs. According to a voluntary survey, financial services firms spend approximately 0.3 percent of revenue or 10% of their information technology budgets on cybersecurity, highlighting the fact that identifying vulnerabilities and having cybersecurity policies and procedures in place are more important than the actual cybersecurity budget itself, particularly with respect to expensive hardware and software.⁷⁵⁵

In performing their contracted duties, specialized service providers may receive, maintain, or process confidential information from Market Entities, or are otherwise permitted to access Market Entities' information systems and the information residing on those systems. Market Entities work with service providers that provide certain critical functions, such as process payment providers, regulatory services consultants, data providers, custodians, and valuation services. However, Market Entities also employ general service providers, such as email providers, relationship management systems, cloud applications, and other technology vendors.

Regardless of their size, Market Entities typically enter into contracts with service providers to perform a specific function for a given time frame at a set price. At the conclusion of a contract, it may be renewed if both parties are satisfied. Because prices typically increase over time, there may be some need to negotiate a new fee for continued service. Negotiations also occur if additional services are requested from a given third-party provider. In the instance where additional services are required mid-contract, for example, due to increased regulatory requirements, the service provider may be able to bill for the extra work that it must incur separately to provide the additional service, particularly if that party is in a highly concentrated market for that service and can wield market power. This may be the case because that condition is specified in the contract with the Market Entity.

Service providers that cater to the securities industry with specialized services are likely to have economies of scale that allow them to more easily handle requests from Market Entities for additional services.⁷⁵⁶ Some service providers, however, may not have the technical expertise to provide a requested additional service or may refuse to do so for other reasons. In this case, the Market Entity would need to find another service provider. The costs associated with service provider contracts, including those of renegotiating them or tacking on of supplemental fees, are passed on to the Market Entity's customers, counterparties, members, participants,

⁷⁴⁵ Exempt securities exchanges governed by section 5 of the Act are not considered to be national securities exchanges.

⁷⁴⁶ Two exchanges, The Island Futures Exchange, LLC, and NQLX LLC, were formerly registered with the Commission as national securities exchanges.

⁷⁴⁷ See sections I.A.2.g. and I.A.2.h. of this release.

⁷⁴⁸ See paragraphs (a)(1)(iii), (vii), and (viii) of proposed Rule 10 (defining, respectively, MSBSPs, SBSDRs, and SBSs as "covered entities").

⁷⁴⁹ See *List of Registered Security-Based Swap Dealers and Major Security-Based Swap Participants* (Jan. 4, 2023), available at <https://www.sec.gov/tm/List-of-SBS-Dealers-and-Major-SBS-Participants>.

⁷⁵⁰ See DTCC, *GTR North America*, available at <https://www.dtcc.com/repository-and-derivatives-services/repository-services/gtr-north-america>.

⁷⁵¹ See section I.A.2.i. of this release.

⁷⁵² See paragraph (a)(1)(ix) of proposed Rule 10.

⁷⁵³ See *Transfer Agent Regulations*, Exchange Act Release No. 76743 (Dec. 22, 2015), 80 FR 81948, 81949 (Dec. 31, 2015).

⁷⁵⁴ See Commission, *Transfer Agent Data Sets* (Dec. 31, 2022), available at <https://www.sec.gov/dera/data/transfer-agent-data-sets>.

⁷⁵⁵ See Reshaping the Cybersecurity Landscape.

⁷⁵⁶ See Bharath Aiyer et al., *New Survey Reveals \$2 Trillion Market Opportunity for Cybersecurity Technology and Service Providers* (2022), available at <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers>.

or users to the extent that the Market Entities are able to do so.

D. Benefits and Costs of Proposed Rule 10, Form SCIR, and Rule Amendments

In this section, the Commission considers the benefits and costs of the rule, form, and amendments being proposed in this release.⁷⁵⁷ As discussed earlier, proposed Rule 10 would require all Market Entities (Covered Entities and non-Covered Entities) to establish, maintain, and enforce written policies and procedures that are reasonably designed to address their cybersecurity risks.⁷⁵⁸ All Market Entities also, at least annually, would be required to review and assess the design and effectiveness of their cybersecurity policies and procedures, including whether the policies and procedures reflect changes in cybersecurity risk over the time period covered by the review.⁷⁵⁹ They also would be required to prepare a report (in the case of Covered Entities) or a record (in the case of non-Covered Entities) with respect to the annual review.⁷⁶⁰ Finally, all Market Entities would need to give the Commission immediate written electronic notice of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring.⁷⁶¹

Market Entities that meet the definition of “covered entity” would be subject to certain additional requirements under proposed Rule 10.⁷⁶² First, their cybersecurity risk management policies and procedures

would need to include the following elements:

- Periodic assessments of cybersecurity risks associated with the Covered Entity’s information systems and written documentation of the risk assessments;
- Controls designed to minimize user-related risks and prevent unauthorized access to the Covered Entity’s information systems;
- Measures designed to monitor the Covered Entity’s information systems and protect the Covered Entity’s information from unauthorized access or use, and oversight of service providers that receive, maintain, or process information, or are otherwise permitted to access the Covered Entity’s information systems;
- Measures to detect, mitigate, and remediate any cybersecurity threats and vulnerabilities with respect to the Covered Entity’s information systems; and
- Measures to detect, respond to, and recover from a cybersecurity incident and written documentation of any cybersecurity incident and the response to and recovery from the incident.⁷⁶³

Second, Covered Entities would need to make certain records pursuant to the policies and procedures required under proposed Rule 10. In particular, Covered Entities would be required to document in writing periodic assessments of cybersecurity risks associated with the Covered Entity’s information systems and information residing on those systems.⁷⁶⁴ Additionally, Covered Entities would be required to document in writing any cybersecurity incident, including the Covered Entity’s response to and recovery from the cybersecurity incident.⁷⁶⁵

Third, Covered Entities—in addition to providing the Commission with immediate written electronic notice upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring—would need to report and update information about the significant cybersecurity incident by filing Part I of proposed Form SCIR with the

Commission by filing it with the Commission through the EDGAR system.⁷⁶⁶ The form would elicit information about the significant cybersecurity incident and the Covered Entity’s efforts to respond to, and recover from, the incident. Covered Entities would be required to file updated versions of proposed Form SCIR when material information becomes available or previously reported information is deemed inaccurate. Lastly, a final proposed Form SCIR would need to be submitted after a significant cybersecurity incident is resolved.

Fourth, Covered Entities would need to disclose publicly summary descriptions of their cybersecurity risks and the significant cybersecurity incidents they experienced during the current or previous calendar year on Part II of proposed Form SCIR.⁷⁶⁷ The form would need to be filed with the Commission through the EDGAR system and posted on the Covered Entity’s public-facing business internet website and, in the case of Covered Entities that are carrying or introducing broker-dealers, provided to customers at account opening and annually thereafter.

Rules 17a–4, 17ad–7, and 18a–6—which apply to broker-dealers, transfer agents, and SBS Entities respectively—would be amended to establish preservation and maintenance requirements for the written policies and procedures, annual reports, Parts I and II of proposed Form SCIR, and records required to be made pursuant to proposed Rule 10 (*i.e.*, the Rule 10 Records).⁷⁶⁸ The proposed amendments would specify that the Rule 10 Records must be retained for three years. In the case of the written policies and procedures to address cybersecurity risks, the record would need to be maintained until three years after the termination of the use of the policies and procedures.⁷⁶⁹ In addition, orders exempting certain clearing agencies from registering with the Commission are proposed to be amended to establish preservation and maintenance

⁷⁵⁷ Throughout the following, the Commission also considers benefits and costs related to potential effects on economic efficiency, competition, and capital formation. The Commission summarizes these effects in section IV.E. of this release.

⁷⁵⁸ See paragraphs (b) through (d) of proposed Rule 10 (setting forth the requirements for Market Entities that meet the definition of “covered entity”); paragraph (e)(1) of proposed Rule 10; *see also* sections II.B.1. and II.C. of this release (discussing these proposed requirements in more detail).

⁷⁵⁹ See paragraph (b)(2) of proposed Rule 10; paragraph (e)(1) of proposed Rule 10; *see also* sections II.B.1.f. and II.C. of this release (discussing these proposed requirements in more detail).

⁷⁶⁰ See paragraph (b)(2) of proposed Rule 10; paragraph (e)(1) of proposed Rule 10; *see also* sections II.B.1.f. and II.C. of this release (discussing these proposed requirements in more detail).

⁷⁶¹ See paragraph (c)(1) of proposed Rule 10; paragraph (e)(2) of proposed Rule 10; *see also* sections II.B.2.a. and II.C. of this release (discussing these proposed requirements in more detail).

⁷⁶² See paragraph (b) through (d) of proposed Rule 10 (setting forth the requirements for Market Entities that meet the definition of “covered entity”); paragraph (e) of proposed Rule 10 (setting forth the requirements for Market Entities that do not meet the definition of “covered entity”).

⁷⁶³ See sections II.B.1.a. through II.B.1.e. of this release (discussing these proposed requirements in more detail). In the case of non-Covered Entities, as discussed in more detail below in Section II.C. of this release, the design of the cybersecurity risk management policies and procedures would need to take into account the size, business, and operations of the broker-dealer. *See* paragraph (e) of proposed Rule 10.

⁷⁶⁴ See paragraph (b)(1)(i)(B) of proposed Rule 10; *see also* section II.B.1.a. of this release (discussing this documentation requirement in more detail).

⁷⁶⁵ See paragraph (b)(1)(v)(B) of proposed Rule 10; *see also* section II.B.1.e. of this release (discussing this documentation requirement in more detail).

⁷⁶⁶ See sections II.B.2. and II.B.4. of this release (discussing these proposed requirements in more detail).

⁷⁶⁷ See sections II.B.3. and II.B.4. of this release (discussing these proposed requirements in more detail).

⁷⁶⁸ See sections II.B.5. and II.C. of this release (discussing these proposed amendments in more detail). Rule 17a–4 sets forth record preservation and maintenance requirements for broker-dealers, Rule 17ad–7 sets forth record preservation and maintenance requirements for transfer agents, and Rule 18a–6 sets forth record preservation and maintenance requirements for SBS Entities.

⁷⁶⁹ See proposed rule 17a–4(e).

requirements for the Rule 10 Records that would apply to the exempt clearing agencies subject to those orders.⁷⁷⁰ The amendments would provide that the records need to be retained for five years (consistent with Rules 13n-7 and 17a-1).⁷⁷¹ In the case of the written policies and procedures to address cybersecurity risks, the record would need to be maintained until three years after the termination of the use of the policies and procedures.

1. Benefits and Costs of the Proposal to the U.S. Securities Markets

The Commission is proposing rules to require *all* Market Entities, based on the reasons discussed throughout, to take steps to protect their information systems and the information residing on those systems from cybersecurity risk.⁷⁷² For example, as discussed above, Market Entities may not take the steps necessary to address adequately their cybersecurity risks.⁷⁷³ A Market Entity that fails to do so is more vulnerable to succumbing to a significant cybersecurity incident. As discussed earlier, a significant cybersecurity incident can cause serious harm not only to the Market Entity but also to its customers, counterparties, members, registrants, or users, as well as to any other market participants (including other Market Entities) that interact with the impacted Market Entity.⁷⁷⁴ Therefore, it is vital to the U.S. securities markets and the participants in those markets that all Market Entities address cybersecurity risk, which, as discussed above, is increasingly threatening the financial sector.⁷⁷⁵

a. Benefits

The Commission anticipates that an important economic benefit of the proposal would be to protect the fair, orderly, and efficient operations of the U.S. securities markets and the

soundness of Market Entities better by requiring all Market Entities to establish, maintain, and enforce written policies and procedures cybersecurity policies and procedures. As noted earlier, the average loss in the financial services industry was \$18.3 million, per company per cybersecurity incident. Adopting and enforcing cybersecurity policies and procedures could assist Market Entities from incurring such losses. Furthermore, the requirement to implement cybersecurity policies and procedures could protect potential negative downstream effects that could be incurred by other participants in the U.S. securities markets, such as the Market Entity's customers, counterparties, members, registrants, and users, in the event of a cybersecurity attack. By requiring each Market Entity to implement policies and procedures to address cybersecurity risk, the proposed rule would reduce the likelihood that one Market Entity's cybersecurity incident can adversely affect other Market Entities and market participants, as well as the U.S. securities markets at large.

In addition, FSOC has stated that “[m]aintaining and improving cybersecurity resilience of the financial sector requires continuous assessment of cyber vulnerabilities and close cooperation across firms and governments within the U.S. and internationally.”⁷⁷⁶ The information provided to the Commission under the proposed reporting requirements could help in assessing potential cybersecurity risks that affect the U.S. securities markets. The reporting of significant cybersecurity incidents also could be used to address future cyberattacks. For example, these reports could assist the Commission in identifying patterns and trends across Covered Entities, including widespread cybersecurity incidents affecting multiple Covered Entities at the same time. Further, the

reports could be used to evaluate the effectiveness of various approaches that are used to respond to and recover from significant cybersecurity incidents. Therefore, requiring Covered Entities to report significant cybersecurity incidents to the Commission could help assist the Commission in carrying out its mission of maintaining fair, orderly, and efficient operations of the U.S. securities markets.

Similarly, requiring Covered Entities to publicly disclose summary descriptions of their cybersecurity risks and significant cybersecurity incidents would provide enhanced transparency about cybersecurity threats that could impact the U.S. securities markets. Participants in these markets could use this additional information to enhance the management of their own cybersecurity risks, which also could serve to strengthen the resilience of the U.S. securities markets to future cybersecurity threats.

b. Costs

In general, the costs associated with the proposals include the costs of developing, implementing, documenting, and reviewing cybersecurity policies and procedures. For example, a Market Entity that has only the minimal cybersecurity protection needed to meet the current regulatory requirements may incur substantial costs when implementing the policies and procedures required by proposed Rule 10. These costs could be significantly lower for a Market Entity that currently has a well-developed and documented cybersecurity program. A Market Entity that incurs costs under the proposal may attempt to pass them on to other market participants and even other Market Entities to the extent that they are able to do that. This could increase costs for the Market Entity's customers, counterparties, members, registrants, or users participate in the U.S. securities markets.

In general, compliance costs with proposed Rule 10 would vary across the various types of Market Entities. As discussed above, one factor determining costs would be the extent to which a Market Entity's existing measures to address cybersecurity risk would comply with the proposal. Other factors would be the Market Entity's particular business model, size, and unique cybersecurity risks. While the compliance costs for smaller entities, such as Non-Covered Broker-Dealers, may be relatively smaller, those costs may not be inconsequential relative to their size. Further, Covered Entities may incur substantial compliance costs given their relatively large size.

⁷⁷⁰ See section II.B.5. of this release (discussing these proposed amendments in more detail).

⁷⁷¹ As discussed in section II.B.5.a. of this release, the existing requirements of Rule 13n-7 (which applies to SBSDRs) and Rule 17a-1 (which applies to registered clearing agencies, the MSRB, national securities associations, and national securities exchanges) will require these Market Entities to retain the Rule 10 Records for five years and, in the case of the written policies and procedures, for five years after the termination of the use of the policies and procedures.

⁷⁷² See section I.A.1. of this release (discussing the attractiveness of the U.S. securities market to threat actors).

⁷⁷³ See section IV.B. of this release (discussing broad economic considerations).

⁷⁷⁴ See section I.A.2. of this release (discussing how critical operations of Market Entities are exposed to cybersecurity risk).

⁷⁷⁵ See section I.A.1. of this release (discussing threats to the U.S. financial sector).

⁷⁷⁶ FSOC, *Annual Report (2022)*, at 70, available at <https://home.treasury.gov/system/files/261/FSOC2022AnnualReport.pdf> (“FSOC 2022 Annual Report”) (“By exchanging cyber threat information within a sharing community, organizations can leverage the collective knowledge, experience, and capabilities of that sharing community to gain a more complete understanding of the threats the organization may face.”) See also NIST, Special Pub. 800-150, *Guide to Cyber Threat Information Sharing* iii (2016), available at <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf>. The NIST Special Publication also notes that the use of structured data can facilitate information sharing. *Id.* at 7 (“Structured data that is expressed using open, machine-readable, standard formats can generally be more readily accessed, searched, and analyzed by a wider range of tools. Thus, the format of the information plays a significant role in determining the ease and efficiency of information use, analysis, and exchange.”).

2. Policies and Procedures and Annual Review Requirements for Covered Entities

The definition of a “covered entity” includes a wide range of Commission registrants. The different Covered Entities that would be subject to proposed Rule 10 vary based on the types of businesses they are involved in, their relative sizes, and the number of competitors they face. As a result, the benefits and costs associated with the requirements to establish, maintain, and enforce written cybersecurity policies and procedures and to review them at least annually likely will vary among the different types of Covered Entities. Because the benefits and costs are heterogeneous across the different types of Covered Entities, the costs and benefits that are common to all Covered Entities are discussed first. Next, the benefits and costs associated with each type of Covered Entity are examined separately to account for the different operations and functions they perform and the differences in how existing or proposed regulations apply to them. The estimated cost of compliance for a given Covered Entity and for all Covered Entities combined is provided in the common costs discussion.

a. Common Benefits and Costs for Covered Entities

i. Benefits

As discussed above, due to the interconnected nature of the U.S. securities market, strong policies and procedures to address cybersecurity risks are needed by Covered Entities to protect not only themselves, but also the Market Entities with whom they do business, as well as other market participants, such as the Covered Entity’s customers, counterparties, members, or users. The Commission anticipates that an important economic benefit of the cybersecurity policies and procedures and annual review requirements of proposed Rule 10 would be to reduce the cybersecurity vulnerabilities of each Market Entity and enhance the preparedness of each Market Entity against cybersecurity threats to its operations. This would reduce the likelihood that the Market Entity experiences the adverse consequences of a cybersecurity incident. With written cybersecurity policies and procedures that are maintained and enforced, as well as periodically reviewed and assessed, Market Entities can better protect themselves against cybersecurity threats; harden the security surrounding their information systems and the data, which includes the prevention of

unauthorized access; minimize the damage from successful cyberattacks; and recover more quickly from significant cybersecurity incidents when they do occur. For example, the Covered Entity’s risk assessment policies and procedures would need to require written documentation of these risk assessments.⁷⁷⁷

Relatedly, proposed Rule 10 would require that the incident response and recovery policies and procedures include written documentation of a cybersecurity incident, including the Covered Entity’s response to and recovery from the incident.⁷⁷⁸ These records could be used by the Covered Entity to assess the efficacy of, and adherence to, its incident response and recovery policies and procedures. The record of the cybersecurity incidents further could be used as a “lessons-learned” document to help the Covered Entity respond more effectively the next time it experiences a cybersecurity incident. The Commission staff also could use the records to review compliance with this aspect of proposed Rule 10.

The records discussed above generally could be used by the Covered Entity when it performs its review to analyze whether its current policies and procedures need to be updated, to inform the Covered Entity of the risks specific to it, and to support responses to cybersecurity risks by identifying cybersecurity threats to information systems that, if compromised, could result in significant cybersecurity incidents.⁷⁷⁹ The documentation also could be used by Commission staff and internal auditors of the Covered Entity to examine for adherence to the risk assessment policies and procedures.

Moreover, the annual review requirement is designed to require the Covered Entity to evaluate whether its cybersecurity policies and procedures continue to work as designed and whether changes are needed to ensure their continued effectiveness, including oversight of any delegated responsibilities. As discussed earlier, the sophistication of the tactics, techniques, and procedures employed by threat actors is increasing.⁷⁸⁰

⁷⁷⁷ See paragraph (b)(1)(i)(B) of proposed Rule 10.

⁷⁷⁸ See paragraph (b)(1)(v)(B) of proposed Rule 10.

⁷⁷⁹ See paragraph (b)(2) of proposed Rule 10 (which would require a Covered Entity to review and assess the design and effectiveness of the cybersecurity policies and procedures, including whether the policies and procedures reflect changes in cybersecurity risk over the time period covered by the review). See also section II.B.1.f. of this release (discussing the proposed requirements in more detail).

⁷⁸⁰ See section I.A.1. of this release (discussing, for example, how cybersecurity threats are

As discussed above, it is unlikely that Covered Entities do not currently have some minimum level of cybersecurity policies and procedures in place due to their own business decisions and certain existing regulations and oversight. However, as discussed above, current Commission regulations regarding cybersecurity policies and procedures are narrower in scope. Proposed Rule 10 aims to be comprehensive in terms of mandating that Covered Entities have cybersecurity policies and procedures that address all cybersecurity incidents that may affect their information systems and the funds and securities as well as personal, confidential, and proprietary information that may be stored on those systems. The benefits of the proposed Rule 10 would be lessened to the extent that a Covered Entity already has implemented cybersecurity policies and procedures that are generally consistent with the written policies and procedures and annual review requirements under proposed Rule 10.

If a Covered Entity has to supplement its existing cybersecurity policies and procedures, amend them, or institute annual reviews and document their assessments in a report, the benefit of proposed Rule 10 for that Covered Entity would be greater. The proposal will help ensure the Covered Entity has robust procedures in place to prevent cybersecurity incidents, may enable Covered Entities to detect cybersecurity incidents earlier, and help ensure that Covered Entities have a plan in place to remediate cybersecurity incidents quickly. Lastly, as a second-order effect, it could reduce the Covered Entities’ risk of exposure to other Covered Entities’ cybersecurity incidents stemming—for example—from the interconnectedness of Covered Entities’ information systems.

The Commission currently does not have reliable data on the extent to which each Covered Entity’s existing policies and procedures are consistent with the proposed Rule 10. Therefore, it is not possible to quantify the scale of the benefits arising from the proposed policies and procedures and annual review requirements. However, given the importance of the U.S. securities markets, the value of the funds and assets that are traded and held, and the current state of transactions where much of them are electronic, it seems likely that the Covered Entities that

evolving); see also Bank of England CBEST Report (stating that “[t]he threat actor community, once dominated by amateur hackers, has expanded to include a broad range of professional threat actors, all of whom are strongly motivated, organised and funded”).

transact business digitally have a strong incentive to implement cybersecurity policies and procedures in order to protect and maintain their operations. The proposed rule will require Covered Entities to implement stronger protections that go beyond what they do based on those market incentives.

Based on the extent that Covered Entities engage in business activities involving crypto assets (which depend almost exclusively on the operations of information systems), developing strong cybersecurity policies and procedures would result in large benefits for them and potentially for their customers, counterparties, members, registrants or users. For example, robust cybersecurity policies and procedures would help to ensure that Covered Entities are better shielded from the theft of crypto assets by threat actors, which may be difficult or impossible to recover, given the nature of the distributed ledger technology.⁷⁸¹ In addition, Covered Entities would avoid negative reputational damage associated with a successful cyberattack.

ii. Costs

The costs associated with the policies and procedures and annual review requirements of proposed Rule 10 would primarily result from compliance costs borne by Covered Entities in the design, implementation, review, written assessment, and updates of the cybersecurity policies and procedures. The proposed requirement will likely change a Covered Entity's behavior toward cybersecurity risk and necessitates a certain amount of investment in cybersecurity protection.⁷⁸² In addition to the aforementioned direct compliance costs faced by Covered Entities, those Covered Entities that utilize service providers would need to take steps to oversee them under proposed Rule 10.⁷⁸³ The costs of this oversight, including direct compliance costs, ultimately would likely be passed on to

the Covered Entities' customers, counterparties, members, participants, or users to the extent Covered Entities are able to do so. As indicated above, the compliance costs generally may be lessened to the extent that Covered Entities' existing policies and procedures would be consistent with the requirements of proposed Rule 10. Therefore, the marginal increase in compliance costs that arise likely would be due to the extent to which a Covered Entity needs to make modifications to its existing cybersecurity policies and procedures, implement annual reviews of those policies and procedures, and/or write assessments reports.

The compliance costs associated with developing, implementing, documenting, and reviewing the cybersecurity policies and procedures for Covered Entities' activities that involve crypto assets likely would be higher than those connected with traditional services and technologies offered and used, respectively, by Covered Entities. The cost difference primarily would be due to technological features of distributed ledger technologies as well as with the costs increasing as a Covered Entity engages in activities with additional crypto assets and blockchains.

iii. Service Providers

As indicated above, Covered Entities may use service providers to supply them with some or all of their necessary cybersecurity protection. In general, the cost of contracted cybersecurity services depends on the size of the entity, where larger firms may offer a wider range of services and thus needing more cybersecurity protection. According to a data security provider blog, "[a]mong mid-market organizations (250–999 employees), 46% spend under \$250,000 on security each year and 43% spend \$250,000 to \$999,999. Among enterprise organizations (1,000–9,999 employees), 57% spend between \$250,000 and \$999,999, 23% spend less than \$250,000, and 20% spend at least \$1 million. Half of large enterprises (more than 10,000 employees) spend \$1 million or more on security each year and 43% spend between \$250,000 and \$999,999."⁷⁸⁴

Under the proposal, Covered Entities need to identify their service providers that receive, maintain, or process information, or are otherwise permitted to access its information systems and the information residing on those

systems, and then assess the cybersecurity risks associated with their use by those service providers.⁷⁸⁵ The policies and procedures for protecting information would require oversight of the service providers that receive, maintain, or process the Covered Entities' information, or are otherwise permitted to access the Covered Entities' information systems and the data residing on those systems, through a written contractual agreement, as specified in paragraph (b)(iii)(B) of proposed Rule 10.⁷⁸⁶ Service providers would be required to implement and maintain, pursuant to a written contract with the Covered Entities, appropriate measures, including the practices described in paragraph (b) of proposed Rule 10.

The proposed requirements will likely impose additional costs, at least initially, on service providers catering to Covered Entities, as they would be asked to provide services not included in existing contracts. The Commission believes that most service providers providing business-critical services would likely face pressure to enhance their cybersecurity practices to satisfy demand from Covered Entities due to new regulatory requirements placed on those Covered Entities.⁷⁸⁷ Service providers may be willing to bear additional costs in order to continue their business relationships with the Covered Entities, particularly if the parties are operating under an ongoing contract.⁷⁸⁸ Such situations are more likely to arise with services that are considered general information technology, such as email, relationship management, website hosting, cloud applications, and other common technologies, given that the service provider does not have market power because it has many competitors offering these services. In contrast, providers of more specialized services—such as payment service providers, regulatory service providers, data providers, custodians, and providers of valuation services—may have significant market power and may be able to charge a Covered Entity separately for the additional services that would be required under proposed Rule 10. Whether passed on to Covered Entities immediately or reflected in

⁷⁸¹ See section II.G. of this release (noting that there is no centralized IT infrastructure that can dynamically detect and prevent cyberattacks on wallets or prevent the transfer of illegitimately obtained crypto assets by bad actors).

⁷⁸² While the existing policies and procedures of Covered Entities largely could be consistent with the requirements of proposed Rule 10, without a requirement to do so, they may not conduct annual reviews and draft assessment reports. The annual review and report costs are estimated to be around \$1,500 and \$20,000 based on the costs of obtaining a cybersecurity audit. See *How Much Does a Security Audit Cost?*, Cyber Security Advisor (Jan. 29, 2019), available at <https://cybersecadvisor.org/blog/how-much-does-a-security-audit-cost> ("Cost of Security Audit").

⁷⁸³ See paragraphs (b)(1)(i)(A)(2), (b)(1)(iii)(B), and (b)(2) of proposed Rule 10.

⁷⁸⁴ See Desdemona Bandini, *New Security Report: The Security Bottom Line, How Much Security Is Enough?*, (Nov. 19, 2019), available at <https://duo.com/blog/new-security-report-the-security-bottom-line-how-much-security-is-enough>.

⁷⁸⁵ See paragraph (b)(1)(i)(A)(2) of proposed Rule 10.

⁷⁸⁶ See paragraph (b)(1)(iii)(B) of proposed Rule 10.

⁷⁸⁷ A service provider involved in any business-critical function would likely need to receive, maintain, or process information from the Covered Entities as well as the Covered Entities' customers, counterparties, members, registrants, or users.

⁷⁸⁸ See, e.g., *Cost of Security Audit*.

subsequent contract renewals, the costs associated the additional services—including the associated negotiation process—would likely be passed on to the Covered Entities' customers, counterparties, members, participants, or users to the extent that they are able to do so.

In terms of the cost of additional services received from service providers, those providers that offer a specialized service and have market power may not be willing to give any price concessions in the negotiation process. The same may be true for service providers where Covered Entities make up a small proportion of their overall business. Other service providers in a more competitive environment—such as those that offer general information technology services—may be more willing to provide a discount to keep the Covered Entity as a customer.⁷⁸⁹ Moreover, the compliance costs for service providers of common technologies may be generally larger than those realized by firms that offer specialized services because they cater to a wider variety of customers, which makes contracts with different parties more idiosyncratic.

Some Covered Entities may find that one or several of their existing service providers may not be technically able to—or may not wish to make the investment to—support the Covered Entities' compliance with the proposed rule. Similarly, some Covered Entities may find that one or several of their existing service providers may not be able to—or wish to because of significant market power—enter into written contracts where the costs are not mutually agreeable. Also, some service providers may not want to amend their contracts and take on the particular obligations even if they already have the technical abilities. In those cases, the Covered Entities would need to change service providers and bear the associated switching costs, while the service providers would suffer loss of their customer base.⁷⁹⁰

For service providers that do business with Covered Entities, the proposed rule may impose additional costs related to revising the service provider's cybersecurity practices to satisfy the requirements that would be imposed on

the Covered Entities. Moreover, if a service provider is already providing services to a Covered Entity that are largely compliant with proposed Rule 10, then the resulting increase in compliance costs likely would be minor.

Even if satisfying additional client requirements would not represent a significant expense for service providers, the processes and procedures that are necessary to implement an infrequently utilized service may prevent some service providers from continuing to work with the Covered Entity.⁷⁹¹ That is, the provision of the service may be viewed as more burdensome than the revenue received from the Covered Entity. This consequence would serve as a disincentive to the service provider. In such cases, Covered Entities would bear costs related to finding alternative service providers while existing service providers would suffer lost revenue once the Covered Entities switch service providers.⁷⁹²

To estimate the costs associated with the proposed policies and procedures requirements and annual review requirements, the Commission considered the initial and ongoing compliance costs.⁷⁹³ The internal annual costs for these requirements (which include an initial burden estimate annualized over a three year period) are estimated to be \$14,631.54 per Covered Entity, and \$29,102,133.06 in total. These costs include a blended rate of \$462 for a compliance attorney and assistant general counsel for a total of 31.67 hours. The annual external costs for adopting and implementing the policies and procedures, as well as the annual review of the policies and procedures are estimated to be \$3,472 per Covered Entity, and \$6,905,808 in total. This includes the cost of using outside legal counsel at a rate of \$496 per hour for a total of seven hours.

b. Broker-Dealers

i. Benefits

The benefits of the policies and procedures requirements of proposed Rule 10 for Covered Broker-Dealers likely will not be consistent across these entities, as their services vary. Covered Broker-Dealers that are larger, more interconnected with other market

participants, and offer more services have a higher potential for greater losses for themselves and others in the event of a cybersecurity incident. Thus, the benefits arising from robust cybersecurity practices increases with the size and number of services offered by Covered Broker-Dealers. For example, a cybersecurity incident at a large Covered Broker-Dealer that facilitates trade executions and/or provides carrying and clearing services carries greater risk due to the larger number of services it provides as well as its interconnections with other Market Entities. For example, carrying broker-dealers may provide services to multiple introducing brokers-dealers and their customers. Commission staff determined that, as of September 2022, carrying broker-dealers have an average of 44 introducing broker-dealers on behalf of which they carry funds and securities,⁷⁹⁴ with a median number of five broker-dealers. Furthermore, a carrying broker-dealer may intermediate the connection between one introducing broker-dealer and the final carrying broker-dealer.⁷⁹⁵ As a result, there are potentially many avenues for infiltration, from the introducing broker-dealers to the carrying broker-dealers. Such Covered Broker-Dealers will not only hold customers' personally identifiable information and records, but also typically have control over customers' funds and assets. This makes them attractive targets for threat actors. In addition, even a brief disruption of the services offered by a carrying broker-dealer (e.g., from a ransomware attack) could have large, negative downstream repercussions on the broker-dealer's customers and other Covered Entities (e.g., inability to submit orders during volatile market conditions or to access funds and securities). The persons negatively impacted could include not only individuals but also institutional customers, such as introducing broker-dealers, hedge funds, and family offices. In this scenario, the Covered Broker-Dealer could incur major losses if it experienced a significant cybersecurity incident. Thus, compliance with written cybersecurity policies and procedures, along with annual reviews and a written assessment report, likely would have substantial benefits for those Covered Broker-Dealers that hold customer information, funds, and assets.

Because Covered Broker-Dealers perform a number of functions in the U.S. securities markets and those functions are increasingly performed through the use of information systems,

⁷⁸⁹ See Jon Brodtkin, *IT Shops Renegotiate Contracts to Get Savings Out of Vendors*, Computer World (Nov. 6, 2008), available at <https://www.computerworld.com/article/2781173/it-shops-renegotiate-contracts-to-get-savings-out-of-vendors.html>.

⁷⁹⁰ For example, the Covered Entity has insufficient market power to affect changes in the service provider's business practices and the suite of cybersecurity technologies it currently offers to that Covered Entity.

⁷⁹¹ For example, the costs associated with legal review of alterations to standard contracts may not be worth bearing by the service provider if Covered Entities represent a small segment of the service provider's business.

⁷⁹² At the same time, these frictions would benefit service providers that cater to customers in regulated industries.

⁷⁹³ See section V of this release (discussing these costs in more detail).

⁷⁹⁴ Based on Form Custody, Item 4, as of 2021.

⁷⁹⁵ *Id.*

it is important that those information systems be secure against cyberattacks. Covered Broker-Dealers use networks to connect their information systems to those of national securities exchanges, clearing agencies, and to communicate and transact with other Covered Broker-Dealers. Written policies and procedures would strengthen a Covered Broker-Dealer's cybersecurity protocols so that it would be more difficult for threat actors to disrupt market-making activities in securities or otherwise compromise the liquidity of the securities markets, an occurrence that could negatively impact the ability of investors to liquidate or purchase certain securities at favorable or predictable prices or in a timely manner.

ATSs are trading systems that meet the definition of "exchange" under federal securities laws but are not required to register as national securities exchanges if they comply with the conditions of the Regulation ATS exemption, which includes registering as a broker-dealer. ATSs have become significant venues for orders and non-firm trading interest in securities.⁷⁹⁶ ATSs use data feeds, algorithms, and connectivity to perform their functions. ATSs rely heavily on information systems to perform these functions, including to connect to other Market Entities, such as other Covered Broker-Dealers and national securities exchanges.

A significant cybersecurity incident that disrupts an ATS could negatively impact the ability of investors to liquidate or purchase certain securities at favorable or predictable prices or in a timely manner to the extent it provides liquidity to the market for those securities. Furthermore, the records stored by ATSs on their information systems consist of proprietary information about Market Entities that use their services, including confidential business information (e.g., information about their trading activities). A significant cybersecurity incident at an ATS could lead to the improper use of this information to harm the Market Entities (e.g., public exposure of confidential trading information) or provide the unauthorized user with an unfair advantage over other market participants (e.g., trading based on

confidential business information). Comprehensive cybersecurity policies and procedures, along with periodic assessments, would fortify broker-dealer ATS operations in their efforts to thwart cybersecurity attacks.

On the other hand, a small Covered Broker-Dealer could experience a cybersecurity incident that has significant negative impacts on the entity and its customers, such as a disruption to its services or the theft of a customer's personal information. These types of incidents would have profound negative effects for the small Covered Broker-Dealer and its customers, but the negative effects would likely be insignificant relative to the size of the entire U.S. securities markets. In this case, strong cybersecurity policies and procedures generally could provide substantial benefits to small Covered Broker-Dealers themselves and their customers, but likely not to other market participants.

As discussed in the baseline, Covered Broker-Dealers currently are subject to Regulations S-P, Regulation S-ID, FINRA rules, and SRO and Commission oversight, as well as Regulation ATS applying to broker-dealer operated ATSs.⁷⁹⁷ In addition, Covered Broker-Dealers that operate an ATS and trade certain stocks exceeding specific volume thresholds are subject to Regulation SCI.⁷⁹⁸ As discussed above, Regulation S-P, Regulation ATS, and Regulation S-ID have requirements to establish policies and procedures that address certain cybersecurity risks.⁷⁹⁹ Therefore, Covered Broker-Dealers subject to these other regulations have existing cybersecurity policies and procedures that address certain cybersecurity risks. However, proposed Rule 10 would require all Covered Broker-Dealers to establish, maintain, and enforce a set of cybersecurity policies and procedures that is broader and more comprehensive than is required under the existing requirements of Regulation S-P, Regulation S-ID, and Regulation ATS that pertain to cybersecurity risk. This could substantially benefit these Covered Broker-Dealers and their customers and counterparties as well as other Market Entities that provide

services to them or transact with them. In particular, the failure to protect a particular information system from cybersecurity risk can create a vulnerability that a threat actor could exploit to access other information systems of the Covered Broker-Dealer. Therefore, proposed Rule 10—because it would require all information systems to be protected by policies and procedures—would result in benefits to Covered Broker-Dealers (i.e., enhanced cybersecurity resiliency).

Covered Broker-Dealers that are registered as FCMs or swap dealers are subject to NFA requirements that relate to proposed Rule 10.⁸⁰⁰ These additional requirements may bring those dually-registered Covered Broker-Dealers more in line with the requirements of the proposed rule.⁸⁰¹ As a result, the marginal benefit of compliance for them may be smaller than those that are only registered with the Commission.

ii. Costs

The compliance costs of the policies and procedures requirements of proposed Rule 10 for Covered Broker-Dealers may generally be lower, to the extent their current policies and procedures are designed to comply with Regulation SCI, Regulation S-P, Regulation ATS (if they operate an ATS), Regulation S-ID, and FINRA rules and are consistent with certain of the requirements of the proposed Rule 10.⁸⁰² However, the requirements of proposed Rule 10 are designed to address all of the Covered Broker-Dealer's cybersecurity risks; whereas the requirements of these other regulations that relate to cybersecurity are more narrowly focused. Consequently, the marginal costs associated with implementing the cybersecurity policies and procedures required under the proposed Rule 10 would depend on the extent to which broker-dealers' existing cybersecurity protections address cybersecurity risks beyond those that are required to be addressed by these other regulations.

Covered Broker-Dealers that are dually registered with the CFTC as FCMs or swap dealers are subject to

⁷⁹⁶ Exchange Act Rule 3a1-1(a)(2) exempts an ATS from the definition of exchange under section 3(a)(1) of the Exchange Act on the condition that the ATS complies with Regulation ATS. See generally Regulation of NMS Stock Alternative Trading Systems Release, 83 FR 38768; Amendments Regarding the Definition of "Exchange" and ATSs Release, 87 FR 15496.

⁷⁹⁷ See section IV.C.1.b.i. of this release (discussing as part of the baseline the current relevant regulations applicable to broker-dealers); see also section II.F. of this release (discussing other relevant regulations applicable to Covered Broker-Dealers).

⁷⁹⁸ *Id.*

⁷⁹⁹ See section II.F.1.c. of this release (discussing in more detail the existing requirements of Regulation S-P, Regulation ATS, and Regulation S-ID to have policies and procedures to address certain cybersecurity risks).

⁸⁰⁰ See section IV.C.1.d.iii. of this release (discussing as part of the baseline current CFTC-related requirements applicable to FCMs and swap dealers).

⁸⁰¹ See section I.B. of this release (discussing the proposed requirements for Covered Entities, including Covered Broker-Dealers, with respect to cybersecurity policies and procedures).

⁸⁰² See section II.F.1.c. of this release (discussing the requirements of proposed Rule 10 and how they relate to Regulation S-P, Regulation ATS, and Regulation S-ID).

NFA requirements, as noted above.⁸⁰³ These additional requirements may make compliance with the proposed rule less burdensome and thus less costly, as those NFA requirements are already in place.

c. Clearing Agencies and National Securities Exchanges

i. Benefits

Strong cybersecurity protocols at national securities exchanges would help maintain their critical function of matching orders of buyers and sellers. A cybersecurity incident could prevent an exchange from executing trades, therefore preventing members and their customers from buying or selling securities at the exchange. Interruptions in order flow and execution timing could lead to inefficiencies in order matching, possibly resulting in a less desirable execution price. Moreover, customer information could be stolen and trading strategies could be revealed. Lastly, a cybersecurity breach could be problematic for market surveillance staff that monitors the market for illegal trading activity. Thus, the policies and procedures requirements of proposed Rule 10 could offer significant benefits to national securities exchanges and market participants that depend on their processing of order flow and the ability of regulators to surveil the market.

Clearing agencies serve an important role in the securities markets by ensuring that executed trades are cleared and that the funds and securities are transferred to and from the appropriate accounts. A cybersecurity incident at a clearing agency could result in delays in clearing as well as in the movement of funds and assets. Such an incident also could lead to the loss or misappropriation of customer information, funds, and assets. Threat actors could also gain access to and misappropriate the clearing agency's default fund by, for example, obtaining access to the clearing agency's account in which the fund is held. Strong cybersecurity policies and procedures would assist clearing agencies in protecting the funds and securities in their control. This would benefit the clearing agency, its members, and market participants that rely on the services of its members.

As discussed in the baseline, national securities exchanges, registered clearing agencies, and certain exempt clearing agencies are subject to Regulation

⁸⁰³ See section IV.C.1.d.iii. of this release (discussing as part of the baseline current CFTC-related requirements applicable to FCMs and swap dealers).

SCI.⁸⁰⁴ Regulation SCI has requirements for SCI entities to establish policies and procedures that address certain cybersecurity risks. The proposed requirements of proposed Rule 10, in contrast, apply to all of the Covered Entity's information systems. The benefits of the policies and procedures requirements of proposed Rule 10 would depend on the extent to which the national securities exchanges' and clearing agencies' current cybersecurity policies and procedures (which include those required by Regulation SCI) are consistent with those required under the proposed rule. Major changes in cybersecurity policies and procedures could yield large benefits. However, the marginal benefit of the proposed rule likely would decline the more closely a national securities exchange's or clearing agency's cybersecurity policies and procedures are consistent with the requirements of proposed Rule 10.

Clearing agencies that are registered as DCOs are subject to additional CFTC requirements that may be related to those of proposed Rule 10.⁸⁰⁵ As a result, the marginal benefit of proposed Rule 10 may be smaller than those that are only registered with the Commission.

ii. Costs

The incremental cost of compliance with the policies and procedures requirements of proposed Rule 10 for national exchanges and clearing agencies depends on how much their current cybersecurity policies and procedures go beyond what is required by Regulation SCI. This is because the requirements of proposed Rule 10 are designed to address all of the cybersecurity risks faced by a national securities exchange or clearing agency; in contrast, the requirements of Regulation SCI that relate to cybersecurity are more narrowly focused.⁸⁰⁶ Therefore, national securities exchanges and clearing agencies that have policies and procedures in place that only address the requirements of Regulation SCI will need to make potentially significant changes to their cybersecurity policies and procedures in order to comply with the requirements of proposed Rule 10. Alternatively, national securities

⁸⁰⁴ See section IV.C.1.b.ii. of this release (discussing as part of the baseline the relevant regulations applicable to national securities exchanges and clearing agencies).

⁸⁰⁵ See section IV.C.1.d.i. of this release (discussing as part of the baseline the current relevant CFTC regulations applicable to DCOs).

⁸⁰⁶ See section II.F.1.c. of this release (discussing the requirements of proposed Rule 10 and how they relate to the requirements of Regulation SCI).

exchanges and clearing agencies that currently have comprehensive cybersecurity policies and procedures may incur fewer costs to comply with proposed Rule 10. Nevertheless, assuming that they do not do so already, ensuring that those cybersecurity policies and procedures are documented and reviewed on an annual basis as required by the proposal, with an accompanying written assessment, would assist national securities exchanges and clearing agencies to withstand cybersecurity incidents and address them more effectively, thus minimizing the negative effects of such occurrences.

Clearing agencies that are dually registered with the CFTC as DCOs are subject to that agency's systems safeguards rule, as noted above.⁸⁰⁷ Complying with the CFTC requirements may make compliance with the proposed rule less burdensome and thus less costly, to the extent that the registered DCO implements the CFTC requirements on the registered clearing agency side of its operations.

Finally, national securities exchanges and clearing agencies that are registered with the Commission but currently are not active would incur substantially higher costs relative to their active peers if they needed to come into compliance with proposed Rule 10. If they resume clearing activities and operations, they may incur significant costs to develop, document, implement, maintain, and enforce policies and procedures, including cybersecurity policies and procedures, as well as establish protocols for written annual reviews with necessary modifications and updates.

d. FINRA and the MSRB

i. Benefits

FINRA is the only national securities association currently registered with the Commission. Similarly, the MSRB is the only entity (other than the Commission) established by Congress to, among other activities, propose and adopt rules with respect to transactions in municipal securities.

FINRA issues cybersecurity-related statements to members that discuss best practices for achieving adequate cybersecurity protection.⁸⁰⁸ FINRA and MSRB members are also subject to internal oversight and external audits. Nevertheless, both FINRA and the

⁸⁰⁷ See section IV.C.1.c.i. of this release (discussing as part of the baseline the current relevant CFTC regulations applicable to DCOs).

⁸⁰⁸ See FINRA, *Cybersecurity*, available at <https://www.finra.org/rules-guidance/key-topics/cybersecurity#overview>.

MSRB store proprietary information about their members, including confidential business information, on their respective information systems. FINRA stores information about broker-dealers and trades. Some information and systems under FINRA's control may belong to other organizations where FINRA is simply contracted to perform data processing duties. There also may be sensitive information related to FINRA's oversight practices that is not made public, such as regulatory assessments of various broker-dealers or internal analyses regarding its examinations and examination programs. Furthermore, FINRA may keep information on cyberattacks on itself and on broker-dealers that, if made public, could compromise existing cybersecurity systems. Therefore, FINRA and the MSRB themselves require their own cybersecurity policies and procedures.

As discussed in the baseline, FINRA and the MSRB are subject to Regulation SCI.⁸⁰⁹ Regulation SCI has requirements to establish policies and procedures that address certain cybersecurity risks.⁸¹⁰ Therefore, the benefits of the policies and procedures requirements of proposed Rule 10 would depend on the extent to which the FINRA's and the MSRB's current cybersecurity policies and procedures (which include those required by Regulation SCI) are consistent with those required under the proposed rule. This means the marginal benefit of the proposed rule may be limited depending on how closely FINRA's and the MSRB's cybersecurity policies and procedures are consistent with proposed Rule 10. Nevertheless, ensuring that those cybersecurity policies and procedures are documented and reviewed on an annual basis, with an accompanying written assessment, could assist the two entities in avoiding cybersecurity incidents and addressing them more effectively, thus minimizing the negative effects of such occurrences.

ii. Costs

As with national securities exchanges and clearing agencies, the Commission does not expect that FINRA and the MSRB will incur significant costs as a result of complying with the policies and procedures requirements of proposed Rule 10 because they are already subject to Regulation SCI and, due to their importance in the oversight and oversight of their members or

⁸⁰⁹ See section IV.C.1.b.ii. of this release (discussing as part of the baseline the current relevant regulations applicable to national securities associations and FINRA).

⁸¹⁰ See section II.F.1.c. of this release (discussing in more detail the requirements of Regulation SCI).

registrants, as well as the storage of trade information and data owned by other parties, there are strong incentives for FINRA and the MSRB to invest in comprehensive cybersecurity programs.

e. SBS Entities

i. Benefits

As discussed in the baseline, SBS Entities must comply with section 15F(j)(2) of the Exchange Act and various Commission rules. SBS Entities that are dually registered with the CFTC are subject to that agency's rules as well as the rules of the NFA.⁸¹¹ The benefits that would accrue to SBS Entities depend on the level of cybersecurity protection they currently have in place. Policies and procedures that are consistent with the policies and procedures requirements of proposed Rule 10 may only need moderate updating and adjustment. As a result the marginal benefits likely are small. There would be much greater benefits for SBS Entities that must significantly revise their current policies and procedures. Further, proposed Rule 10 would require that SBS Entities have policies and procedures to respond to and recover from cybersecurity incidents, which would assist the SBS Entities in minimizing the harm caused by the incident and enhancing their ability to recover from it. Annual reviews also would help them update their policies and procedures to address emerging threats.

SBS Entities that are registered as swap dealers are subject to additional requirements of the CFTC and NFA that may be related to those of proposed Rule 10.⁸¹² As a result, the marginal benefit of compliance for them may be smaller than those that are only registered with the Commission.

ii. Costs

Complying with the policies and procedures requirements of proposed Rule 10 may not be costly for SBS Entities. SBS Entities must comply with section 15F(j)(2) of the Exchange Act and various Commission rules. The costs that arise from compliance with proposed Rule 10 depend on how closely their current documented policies and procedures, as well as annual reviews and summary reports, are consistent with the proposed rule. SBS Entities that have very similar cybersecurity policies and procedures to

⁸¹¹ See section IV.C.1.c.iii. of this release (discussing as part of the baseline current relevant regulations applicable to SBS Entities).

⁸¹² See section IV.C.1.c.iii. of this release (discussing as part of the baseline the current relevant CFTC regulations applicable to swap dealers).

those that would be required under proposed Rule 10 would have small associated costs to come into compliance with the rule. SBS Entities that need to make more substantial changes to their cybersecurity policies and procedures to comply with the proposed rule would incur higher attendant costs. Ultimately, the ability of SBS Entities to bear those additional costs depends on the competitive landscape of the security-based swap market.

SBS Entities that are dually registered with the CFTC as swap dealers are subject to that agency's requirements, as noted above.⁸¹³ These additional requirements may make compliance with the proposed rule less burdensome and thus less costly, as the CFTC requirements are already in effect and dually registered SBS Entities must comply with those regulations.

f. SBSDRs

i. Benefits

SBSDRs collect and maintain security-based swap transaction data so that relevant authorities can access and analyze the data from secure, central locations, thereby allowing regulators to monitor for potential market abuse and risks to financial stability.⁸¹⁴ SBSDRs also reduce operational risk and enhance operational efficiency in the security-based swap market, such as by maintaining transaction records that help counterparties ensure that their records reconcile.⁸¹⁵

The Commission requires SBSDRs to have written documentation regarding how they keep such transaction information secure.⁸¹⁶ If the policies and procedures requirements of proposed Rule 10 requires an SBSDR to do additional development, documentation, implementation, and review of its cybersecurity policies and procedures, then the benefits that accrue

⁸¹³ See section IV.C.1.c.iii. of this release (discussing as part of the baseline the current relevant CFTC regulations applicable to swap dealers).

⁸¹⁴ See SBSDR Adopting Release, 80 FR at 14440 (“[SBSDRs] are required to collect and maintain accurate SBS transaction data so that relevant authorities can access and analyze the data from secure, central locations, thereby putting them in a better position to monitor for potential market abuse and risks to financial stability.”).

⁸¹⁵ See SBSDR Proposing Release at 77307 (stating that “[t]he enhanced transparency provided by an [SBSDR] is important to help regulators and others monitor the build-up and concentration of risk exposures in the [security-based swap] market In addition, [SBSDRs] have the potential to reduce operational risk and enhance operational efficiency in the [security-based swap] market”).

⁸¹⁶ See section IV.C.1.b.iv. of this release (discussing as part of the baseline the current relevant regulations applicable to SBSDRs).

from doing so will be large. In this circumstance, compliance with the policies and procedures requirements of proposed Rule 10 would bolster SBSDRs' cybersecurity resiliency. As a result, SBSDRs would be better prepared to identify cybersecurity vulnerabilities and prevent significant cybersecurity incidents, thereby safeguarding the security-based swap trade data that they receive and maintain. Further, proposed Rule 10 would require that SBSDRs have policies and procedures to respond to and recover from a significant cybersecurity incident, which would assist SBSDRs in minimizing the harm caused by the incident and enhancing their ability to recover from it. Annual reviews also would help them update their policies and procedures to address emerging threats.

SBSDRs that are dually registered with the CFTC as SDRs must comply with that agency's systems safeguards rule, applicable to information systems for data under the CFTC's jurisdiction.⁸¹⁷ These additional requirements may bring those dually-registered SBSDRs more in line with the requirements of the proposed rule, to the extent that the registered entity applies the CFTC's systems safeguard requirements to the SBSDR operations. As a result, the marginal benefit of compliance for them may be smaller than those that are only registered with the Commission.

ii. Costs

The costs that arise from compliance with the policies and procedures requirements of proposed Rule 10 depend on how closely the current documented policies and procedures of SBSDRs are consistent with the proposed rule. SBSDRs that have very similar cybersecurity policies and procedures to those that would be required under proposed Rule 10 would face small costs to amend their cybersecurity policies and procedures. SBSDRs that need to make more substantial changes to their cybersecurity policies and procedures to comply with the proposed rule would realize greater marginal benefits from attaining compliance, while incurring higher attendant costs.

SBSDRs that are dually registered with the CFTC as SDRs are subject to that agency's system safeguards rule, as noted above.⁸¹⁸ These additional

⁸¹⁷ See section IV.C.1.d.ii. of this release (discussing as part of the baseline the current relevant CFTC regulations applicable to SDRs).

⁸¹⁸ See section IV.C.1.d.iii. of this release (discussing as part of the baseline the current

requirements may make compliance with the proposed rule less burdensome and thus less costly, to the extent the registered entity applies the CFTC's system safeguard requirements to its SBSDR operations.

g. Transfer Agents

i. Benefits

The benefits of the policies and procedures requirements of proposed Rule 10 likely will differ across transfer agents, as their size and the level of their services may vary. Transfer agents, among other functions, may: (1) track, record, and maintain on behalf of issuers the official record of ownership of each issuer's securities; (2) cancel old certificates, issue new ones, and perform other processing and recordkeeping functions that facilitate the issuance, cancellation, and transfer of those securities; (3) facilitate communications between issuers and registered securityholders; and (4) make dividend, principal, interest, and other distributions to securityholders.⁸¹⁹ A cybersecurity incident at a transfer agent would have varying negative impacts depending on the range of services offered by the transfer agent. Nonetheless, for the issuer who depends on the transfer agent to maintain the official record of ownership, or for securityholders who depend on the transfer agent for distributions, an incident at even a small transfer agent with limited services could have profound negative implications.

In addition, some transfer agents may maintain records and information related to securityholders that could include names, addresses, phone numbers, email addresses, employers, employment history, bank and specific account information, credit card information, transaction histories, securities holdings, and other detailed and individualized information related to the transfer agents' recordkeeping and transaction processing on behalf of issuers. This information may make a transfer agent particularly attractive to threat actors. Compliance with written cybersecurity policies and procedures under proposed Rule 10, along with annual reviews and a written assessment report, would likely produce a large benefit for clients and investors of transfer agents.

Preventing successful cyberattacks would keep securities from being stolen by threat actors and would ensure that dividends are paid when promised. In

relevant CFTC regulations applicable to swap dealers).

⁸¹⁹ See section I.A.2.i. of this release (discussing critical operations and functions of transfer agents).

addition, because transfer agents have information on the securityholders' personal information, policies and procedures to protect that information from unauthorized access or use would benefit the transfer agent and the securityholders. Moreover, if a significant cybersecurity incident materializes, transfer agents would have a plan to resolve the issue, thus potentially reducing the timeframe and damage associated with the incident.

As discussed in the baseline, transfer agents registered with the Commission (but not transfer agents registered with another appropriate regulatory agency) are subject to the Regulation S-P Disposal Rule and may be subject to Regulation S-ID.⁸²⁰ The Regulation S-P Disposal Rule and Regulation S-ID require measures that implicate a certain cybersecurity risk.⁸²¹ Nonetheless, the policies and procedures requirements of proposed Rule 10 would still provide substantial benefits to transfer agents. This is because, as discussed above, proposed Rule 10 would require all transfer agents to establish, maintain, and enforce policies and procedures to address cybersecurity risks that are broader and more comprehensive than those policies and procedures required by the existing requirements of Regulation S-P or Regulation S-ID.

ii. Costs

Transfer agents likely would incur moderate costs in complying with the policies and procedures requirements of proposed Rule 10 if their current policies and procedures—including those to comply with the Regulation S-P Disposal Rule and Regulation S-ID (if either or both apply)—would need to be augmented to meet the requirements of proposed Rule 10. Transfer agents also would have to do annual reviews and write assessment reports. Such costs likely would be passed on to the entities that use transfer agent's services. Transfer agents that have made the business decision to implement robust cybersecurity policies, procedures, and practices would incur lower marginal compliance costs, to the degree those policies, procedures, and practices are consistent with the requirements of proposed Rule 10.

⁸²⁰ See section IV.C.1.b.v. of this release (discussing as part of the baseline the current relevant regulations applicable to transfer agents). Transfer agents that are subsidiaries of bank holding companies would incur minimal cost since they are already subject to federal banking cybersecurity regulations.

⁸²¹ See section II.F.1.c. of this release (discussing in more detail the existing requirements of the Regulation S-P Disposal Rule and Regulation S-ID).

h. Request for Comment

The Commission requests comment on all aspects of the foregoing analysis of the benefits and costs of the policies and procedures, review and assessment, and report requirements of proposed Rule 10. Commenters are requested to provide empirical data in support of any arguments or analyses. In addition, the Commission is requesting comment on the following matters:

1. Please discuss which types of Covered Entities have some level of cybersecurity in place and which may not? If not, explain why. Please describe the level of cybersecurity policies and procedures that have been implemented by Covered Entities and compare them to the requirements of proposed Rule 10.

2. Do the benefits and costs associated with Covered Entities having written cybersecurity policies and procedures, including provisions for written annual reviews and assessments, reports, and updates (if necessary) vary by the type of Covered Entity? If so, explain how. Are there benefits and costs of the proposals not described above? If so, please describe them.

3. Are the estimated compliance costs (both initially and on an ongoing basis) for Covered Entities to adopt cybersecurity policies and procedures, along with reviewing them annually and drafting a summary report, reasonable? If not, explain why and provide estimates of the compliance costs.

4. How costly would it be for a given type of Covered Entity to become compliant with proposed Rule 10? Please explain and provide estimates of the costs.

5. Do Covered Entities typically document their cybersecurity policies and procedures? If not, how costly would it be for them to be documented?

6. Please describe practices of Covered Entities with regard to the use of service providers in connection with their information systems and the information residing on those systems. How many Market Entities contract with service providers? What functions are contracted out versus completed in house? Are the cybersecurity policies and procedures implemented by these service providers comparable to the requirements of proposed Rule 10? Please explain. Would it be costly contractually to request that a service provider provide compliant services, including documented policies and procedures? What are the costs of finding a new service provider if one or more could not provide services that are compliant with the proposed rule?

7. How costly would it be to review and update, if necessary, cybersecurity

policies and procedures at least annually? Would it be preferable to conduct the reviews on either a more or less frequent basis? Explain why. Would it be less costly to have a third party conduct the review and update of a Covered Entities' cybersecurity policies and procedures? Please explain.

3. Regulatory Reporting of Cybersecurity Incidents by Covered Entities

Under proposed Rule 10, Covered Entities would need to provide the Commission with immediate written electronic notice of a significant cybersecurity incident affecting the Covered Entity and, thereafter, report and update information about the significant cybersecurity incident by filing Part I of proposed Form SCIR with the Commission through the EDGAR system.⁸²² The form would elicit information about the significant cybersecurity incident and the Covered Entity's efforts to respond to, and recover from, the incident. In the case of certain Covered Entities, the notice and subsequent reports would need to be provided to other regulators.

a. Benefits

The requirements of proposed Rule 10 that Covered Entities provide immediate written electronic notice and subsequent reporting about significant cybersecurity incidents to the Commission and would improve the Commission's ability to assess these incidents. These requirements also would allow the Commission to understand better the causes and impacts of significant cybersecurity incidents and how Covered Entities respond to and recover from them. Thus, the notification and reporting requirements—through the information they would provide the Commission—could be used to understand better how significant cybersecurity incidents materialize and, therefore, how Covered Entities can better protect themselves from them and, when they occur, how Covered Entities can better mitigate their impacts and recover more quickly from them. Over time, this database of information could provide useful insights into how to minimize the harm more broadly that is caused by significant cybersecurity incidents, which have the potential to cause broader disruptions to the U.S. securities markets and undermine financial stability.

A Covered Entity would be required to provide immediate written electronic

notice to the Commission of a significant cybersecurity incident upon having a reasonable basis to conclude that the incident has occurred or is occurring.⁸²³ This timeframe allows for quick notification to the Commission and, in some cases, other regulators about the significant cybersecurity incident, which—in turn—would allow for more timely assessment of the incidents. These incidents, if not addressed quickly, could have harmful spillover impacts to other Market Entities and participants in the U.S. securities markets.

The immediate written electronic notice would need to identify the Covered Entity, state that the notice is being given to alert the Commission of a significant cybersecurity incident impacting the Covered Entity, and provide the name and contact information of an employee of the Covered Entity who can provide further details about the significant cybersecurity incident.⁸²⁴ By not requiring detailed information about the significant cybersecurity incident, the Covered Entity would be able to provide the notice quickly while it continues to assess which information systems have been subject to the significant cybersecurity incident and the impact that the incident has had on those systems. This would facilitate the Covered Entity's ability to alert the Commission and other regulators (if applicable) at a very early stage after it has a reasonable basis to conclude that a significant cybersecurity incident has occurred or is occurring. This, in turn, would allow the Commission and other regulators (if applicable) to begin taking steps to assess the significant cybersecurity incident at that early stage.

This proposed immediate written electronic notification requirement is modelled on other notification requirements that apply to broker-dealers and SBSBs pursuant to other Exchange Act rules. Under these existing requirements, broker-dealers and certain SBSBs must provide the Commission with same-day written notification if they undergo certain adverse events, including falling below their minimum net capital requirements or failing to make and keep current required books and records.⁸²⁵ The objective of these requirements is to provide the Commission staff with the opportunity to respond when a broker-

⁸²³ See paragraph (c)(1) of proposed Rule 10.

⁸²⁴ *Id.*

⁸²² See sections II.B.2. and II.B.4. of this release (discussing these proposed requirements in more detail).

⁸²⁵ See 17 CFR 240.17a–11 (notification rule for broker-dealers); 17 CFR 240.18a–8 (notification rule for SBS Entities).

dealer or SBSB is in financial or operational difficulty.⁸²⁶ Similarly, the immediate written electronic notification requirement of proposed Rule 10 would provide the Commission staff with the opportunity to promptly begin to assess the situation when a Covered Entity is experiencing a significant cybersecurity incident.

Promptly thereafter (but no later than 48 hours), a Covered Entity would be required to report separately more detailed information about the significant cybersecurity incident by filing initial, amended and final versions of Part I of proposed Form SCIR with the Commission through the EDGAR.⁸²⁷ The Covered Entity also would be required to file updated reports and a final report.

The reporting requirements under proposed Rule 10 would provide the Commission and its staff with information to understand better the nature and extent of a particular significant cybersecurity incident and the efficacy of the Covered Entity's response to mitigate the disruption and harm caused by the incident.⁸²⁸ It also strengthens and expands the Commission's knowledge regarding cybersecurity incidents beyond what is already required by current Commission regulations. In addition, the reporting would provide the staff with a view into the Covered Entity's understanding of the scope and impact of the significant cybersecurity incident. All of this information would assist the Commission and its staff in assessing the significant cybersecurity incident impacting the Covered Entity. It also could benefit other Market Entities to the extent the confidential information provided by the impacted Covered Entity could be used to assist them (without divulging the identity of the impacted Covered Entity) in avoiding a similar significant cybersecurity incident or succumbing to an attack by the same threat actor that caused the significant cybersecurity incident.

The information provided to the Commission under the proposed reporting requirements also would be used to assess the potential

cybersecurity risks affecting U.S. securities markets more broadly. This information could be used to address future significant cybersecurity incidents or address cybersecurity vulnerabilities that may be present at other similar Covered Entities. For example, these reports could assist the Commission in identifying patterns and trends across Covered Entities, including widespread cybersecurity incidents affecting multiple Covered Entities at the same time. Further, the reports could be used to evaluate the effectiveness of various approaches to respond to and recover from a different types of significant cybersecurity incidents. This could benefit all Market Entities, other participants in the U.S. securities markets, and ultimately promote the fair, orderly, and efficient operation of the U.S. securities markets.

Requiring Covered Entities to file Part I of proposed Form SCIR in EDGAR in a custom XML would allow for more efficient processing of information about significant cybersecurity incidents. It would create a comprehensive set of data of all significant cybersecurity incidents impacting Covered Entities that is based on these entities responding to the same check boxes and questions on the form. This would facilitate analysis of the data, including analysis across different Covered Entities and significant cybersecurity incidents. Eventually, this set of data and the analysis of it by searching and sorting based on how different Covered Entities responded to the same questions on the form could be used to spot common trending risks and vulnerabilities as well as best practices employed by Covered Entities to respond to and recover from significant cybersecurity incidents.

As discussed above, Covered Entities have incentives to not disclose information about significant cybersecurity incidents. Such incentives constrain the information available about cybersecurity threats and thereby inhibit the efficacy of collective (*i.e.*, an industry's or a society's) cybersecurity measures.⁸²⁹ At the same time, complete transparency in this area likely runs the risk of facilitating future attacks.⁸³⁰ As

discussed above, the challenge of effective information sharing has long been recognized, and government efforts at encouraging such sharing on a voluntary basis have had only limited success.⁸³¹ The Commission would not publicly disclose and would keep them confidential to the extent permitted by law Part I of proposed Form SCIR. This would limit the risks associated with public disclosure of vulnerabilities as a result of successful cybersecurity incidents. The Commission also may share information with relevant law enforcement or national security agencies.

The aforementioned benefits arise from improved information sharing between the affected Covered Entity and the Commission. Delays in incident reporting may hinder the utility of Part I of proposed Form SCIR because the Commission would not be able to assess the situation close to the time of its occurrence or discovery. Thus, the utility of such reports, at least initially, may be more limited if they are not filed as quickly as proposed.

Requiring Covered Entities to identify themselves on Part I of proposed Form SCIR with a UIC⁸³² if they already have a UIC would be beneficial because the LEI—which is a Commission-approved UIC—is a globally-recognized standard identifier⁸³³ with reference data that is

Standards and Tech. (Dec. 2021), available at <https://doi.org/10.6028/NIST.SP.800-160v2r1>. See also Section IV.D.2.b (discussion of costs associated with disclosure).

⁸³¹ See section IV.C.1.e. of this release (discussing information sharing).

⁸³² As mentioned in section II.B.2.b. of this release, the instructions of proposed Form SCIR would define UIC to mean an identifier that has been issued by an IRS that has been recognized by the Commission pursuant to Rule 903(a) of Regulation SBSR (17 CFR 242.903(a)).

⁸³³ “The [LEI] is a reference code—like a bar code—used across markets and jurisdictions to uniquely identify a legally distinct entity[.]” Office of Financial Research, U.S. Treasury Dep't, *Legal Entity Identifier—Frequently Asked Questions*, available at <https://www.financialresearch.gov/data/legal-entity-identifier-faqs/>. “The financial crisis underscored the need for a global system to identify financial connections, so regulators and private sector firms could understand better the true nature of risk exposures across the financial system.” *Id.* Using the LEI as a UIC to facilitate tracking financial entity cybersecurity incidents and risks is feasible because “[t]he Global LEI System was established for a large range of potential uses.” The Legal Entity Identifier Regulatory Oversight Committee (“LEIROC”), *LEI Uses*, available at <https://www.leiroc.org/lei/uses.htm>. The functionality of the LEI is such that it could be used to identify and track entities for various purposes. For example, the LEI is one of three identifiers that firms can use under a December 2022 U.S. Customs & Border Protection Pilot for automation program for enhanced tracing in international supply chains. See U.S. Customs and Border Protection, *Announcement of the National Customs Automation Program Test Concerning the Submission Through the Automated Commercial*

⁸²⁶ See SBSB Entity Recordkeeping and Reporting Proposing Release, 79 FR at 25247.

⁸²⁷ See paragraphs (c)(2) of proposed Rule 10. As discussed below, Part II of proposed Form SCIR would be used by Covered Entities to make public disclosures about the cybersecurity risks they face and the significant cybersecurity incidents they experienced during the current or previous calendar year. See sections II.B.2. and II.B.4. of this release (discussing these proposed requirements).

⁸²⁸ See Line Items 2 through 14 of Part I of proposed Form SCIR (eliciting information about the significant cybersecurity incident and the Covered Entity's response to the incident).

⁸²⁹ See section IV.B. of this release (discussing broad economic considerations); see, e.g., Lewis and Zheng, *Cyber Threat Information Sharing* (recommending that regulators encourage information sharing).

⁸³⁰ Although “security through obscurity” as a cybersecurity philosophy has long been derided, “obscurity,” or more generally “deception,” has been recognized as an important cyber resilience technique. See Ron Ross, Victoria Pillitteri, Richard Graubart, Deborah Bodeau, and Rosalie McQuaid, *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*, 2 Nat. Inst. of

available free of charge.⁸³⁴ Unlike many identifiers that are specific to a particular regulatory authority or jurisdiction, the LEI is a permanent, unique global identifier that also contains “Level 2” parent and (direct/indirect) child entity information. Entity parent-child relationships are particularly relevant to assessing the risks of entities operating in the securities markets, where financial entities’ interconnectedness and complex group structures could otherwise make understanding the scope of potential widespread risks challenging.⁸³⁵ Additionally, unlike most company registries, all LEI data elements are validated annually and subject to a “quality program [that] scans the full [data] repository daily and publishes the results monthly in quality reports[,]” which helps to ensure the accuracy—and usefulness—of LEI data as compared to other types of entity identifiers that lack such features.⁸³⁶

Environment of Certain Unique Entity Identifiers for the Global Business Identifier Evaluative Proof of Concept, 87 FR 74157 (Dec. 2, 2022), available at <https://www.federalregister.gov/documents/2022/12/02/2022-26213/announcement-of-the-national-customs-automation-program-test-concerning-the-submission-through-the>.

⁸³⁴ Bank for Int’l Settlements, David Leung, et al., *Corporate Digital Identity: No Silver Bullet, but a Silver Lining*, BIS Paper No. 126, at 20 (June 2022), available at <https://www.bis.org/publ/bppdf/bispap126.pdf>. (“BIS Papers 126”) (stating that “LEI data [is] available free of charge to users in both the public and private sector”). The FSOc has stated the LEI “enables unique and transparent identification of legal entities.” FSOc, 2021 Annual Report, at 171 (stating that “[b]roader adoption of the LEI by financial market participants continues to be a Council priority”). The FSOc also has stated that the LEI “facilitate[s] many financial stability objectives, including improved risk management in firms [and] better assessment of microprudential and macroprudential risks[.]” FSOc, 2022 Annual Report 99 (2022), available at <https://home.treasury.gov/system/files/261/FSOC2022AnnualReport.pdf>. The same principles that make the LEI well-suited for allowing regulators to track entity exposures to financial market risks across jurisdictions and entities should apply in other contexts, such as cross-border payments. See FSB, *FSB Options to Improve Adoption of the LEI, in Particular for Use in Cross-Border Payments* (July 7, 2022), available at <https://www.fsb.org/wp-content/uploads/P070722.pdf>.

⁸³⁵ FSB Peer Review Report; see also European Systemic Risk Board, Francois Laurent, et al., *The Benefits of the Legal Entity Identifier for Monitoring Systemic Risk*, Occasional Paper Series No. 18, (Sept. 2021) (“The fact that the LEI enables full reporting of the group structure in the LEI database is also crucial for risk analysis. Indeed, the risk usually stems from the group and not from individual entities, and conducting a relevant risk analysis implies aggregating exposures at the level of the group.”). For a discussion of the cybersecurity implications of the interconnectedness of Market Entities’ information systems, see section I.A.1 of this release.

⁸³⁶ See BIS Papers 126, at 16 (noting that “[h]istorically, corporate identification has mainly come from company registries in individual jurisdictions[,]” with the registries connected to the filing of certain documents and the paying of

b. Costs

Covered Entities would incur costs complying with the requirements of proposed Rule 10 to provide immediate written electronic notice and subsequent reporting about significant cybersecurity incidents to the Commission and, in the case of certain Covered Entities, other regulators, on Part I of proposed Form SCIR. The immediate notification requirement would impose minimal costs given the limited nature of the information that would need to be included in the written notice and the fact that it would be filed electronically.

The costs of complying with the requirements to file Part I of proposed Form SCIR to report a significant cybersecurity incident would be significantly greater than the initial notice, given the amount of information that would need to be included in the filing. In addition, because Part I of proposed Form SCIR is a regulatory filing, Covered Entities likely would incur costs associated with a legal and compliance review prior to the form being filed on EDGAR.

In terms of the costs of filing Part I of Form SCIR on EDGAR, several categories of Covered Entities already file forms in EDGAR. Specifically, all transfer agents, SBSs, MSBSPs, and SBSDRs must file registration or reporting forms in EDGAR,⁸³⁷ and some broker-dealers choose to file certain reports on EDGAR rather than filing them in paper form. The applicable EDGAR forms for these entities are filed, at least in part, in a custom XML. Covered Entities that do not currently file registration or reporting forms on EDGAR would have to file a notarized Form ID to receive a CIK number and access codes to file on EDGAR.⁸³⁸

required fees necessary to create legal entities). Under company registry regimes, each company typically is identified by name and “a company registration number” that is not standardized across jurisdictions and is not part of a harmonized system of corporate identification. See *id.* (stating that “[w]ith greater globalization of business and finance, [the existing company registry system] has become a source of inefficiency and risks from the standpoint of financial stability, market integrity, and investor protection”). Further, “company registries typically do not offer similar types of quality programs for the corporate data they provide” and that such data generally is “declarative—provided by the registrant” without independent verification or validation. See *id.* at 20.

⁸³⁷ SBSDRs received temporary relief from filing through EDGAR. See *Cross-Border Application of Certain Security-Based Swap Requirements*, Exchange Act Release No. 87780 (Dec. 18, 2019) [85 FR 6270, 6348 (Feb. 2, 2020)].

⁸³⁸ See section V of this release (discussing of the number of Covered Entities who do not currently file forms in EDGAR and the costs that would be associated with an EDGAR-filing requirement in more detail).

Consequently, the requirement to file Part I of proposed Form SCIR in EDGAR using a form-specific XML may impose some compliance costs on certain Covered Entities. These Covered Entities would need to complete Form ID to obtain the EDGAR-system access codes that enable entities to file documents through the EDGAR system. They would have to pay a notary to notarize Form ID. The inclusion of a UIC on proposed Form SCIR would not impose any marginal costs because a Covered Entity would only be required to provide a UIC if they have already obtained one.

To estimate the costs for Market Entities to research the validity of a suspected significant cybersecurity incident and to provide immediate written electronic notification to the Commission regarding the significant cybersecurity incident that are real or reasonably determined to be true, the Commission considered the initial and ongoing compliance costs.⁸³⁹ The internal annual costs for these requirements (which include an initial burden estimate annualized over a three year period) are estimated to be \$1,648.51 per Market Entity, and \$6,524,802.58 in total. These costs include a blended rate of \$353 for an assistant general counsel, compliance manager, and systems analyst for a total of 4.67 hours. The annual external costs for these requirements are estimated to be \$1,488 per Market Entity, and \$5,889,504 in total. This includes the cost of using outside legal counsel at a rate of \$496 per hour for a total of three hours.

To estimate the costs for Covered Entities to fill out an initial Part I of proposed Form SCIR, and file an amended Part I of Form SCIR, the Commission considered the initial and ongoing compliance costs.⁸⁴⁰ The internal annual costs for these requirements (which include an initial burden estimate annualized over a three year period) are estimated to be \$1,077.50 per Covered Entity, and \$2,143,147.50 in total. These costs include a blended rate of \$431 for an assistant general counsel and compliance manager for a total of 2.5 hours. The annual external costs for these requirements are estimated to be \$992 per Covered Entity, and \$1,973,088 in total. This includes the cost of using outside legal counsel at a rate of \$496 per hour for a total of two hours.

⁸³⁹ See section V of this release (discussing these costs in more detail).

⁸⁴⁰ See section V of this release (discussing these costs in more detail).

c. Request for Comment

The Commission requests comment on all aspects of the foregoing analysis of the benefits and costs of the requirements to provide immediate notification and subsequent reporting of significant cybersecurity incidents. Commenters are requested to provide empirical data in support of any arguments or analyses. In addition, the Commission is requesting comment on the following matters:

8. Are the estimated compliance costs (both initially and on an ongoing basis) for Covered Entities to provide the notification and subsequent reports reasonable? If not, explain why and provide estimates of the compliance costs.

9. Are there any other benefits and costs that the confidential reporting would provide the Commission? If so, please describe them. Please provide views on the costs of reporting significant cybersecurity incidents to the Commission relative to the Commission's cost estimates.

10. What are the costs and benefits associated with requiring Covered Entities to file Part I of proposed Form SCIR using a structured data language? Should the Commission require Covered Entities to file Part I of proposed Form SCIR using a structured data language, such as a custom XML? Should the Commission require Covered Entities to file Part I of proposed Form SCIR using a different structured data language than a custom XML, such as Inline XBRL? Why or why not?

11. Are there any Covered Entities that should be exempted from the proposed structured data requirements for filing Part I of proposed Form SCIR? If so, what particular exemption threshold should the Commission use for the structured data requirements and why?

12. Should Covered Entities be required to file proposed Form SCIR with a CIK number? What are the costs and benefits associated with requiring Covered Entities to identify themselves on Part I of proposed Form SCIR with a CIK number?

13. Should Covered Entities be required to file Part I of proposed Form SCIR with a UIC (*i.e.*, such as an LEI), particularly when some Covered Entities do not have a UIC and would have to obtain one? What are the benefits associated with requiring Covered Entities with a UIC to identify themselves with that UIC?

14. Would requiring a UIC on Part I of proposed Form SCIR allow the Commission to better evaluate cybersecurity threats to Covered Entities

using data from other regulators and from law enforcement agencies? Please explain how.

15. Are there any Covered Entities for which the proposed structured data requirements for Part I of proposed Form SCIR should be exempted? If so, what particular exemption threshold or thresholds should the Commission use for the structured data requirements under the proposed rule amendments, and why?

4. Public Disclosure of Cybersecurity Risks and Significant Cybersecurity Incidents

Under proposed Rule 10, Covered Entities would need to publicly disclose summary descriptions of their cybersecurity risks and the significant cybersecurity incidents they experienced during the current or previous calendar year on Part II of proposed Form SCIR.⁸⁴¹ The form would need to be filed with the Commission through the EDGAR system and posted on the Covered Entity's business internet website and, in the case of Covered Entities that are carrying or introducing broker-dealers, provided to customers at account opening and at least annually thereafter.

a. Benefits

As discussed above, there exists an information asymmetry between Covered Entities and their customers, counterparties, members, registrants, or users.⁸⁴² This information asymmetry, together with limitations to private contracting, inhibits the ability of customers, counterparties, members, registrants, and users to screen and discipline the Covered Entities with whom they do business or obtain services from based on the effectiveness of the Covered Entity's cybersecurity policies. The public disclosure requirements of proposed Rule 10 would help alleviate this information asymmetry, and in so doing would enable customers, counterparties, members, registrants, or users to better assess the effectiveness of Covered Entities' cybersecurity preparations and the cybersecurity risks of doing business with any one of them. For example, customers, counterparties, members, registrants, or users could use the frequency or nature of significant cybersecurity incidents—as disclosed under the proposed public disclosure requirement—to infer a Covered Entity's effort toward preventing cybersecurity

incidents. Likewise customers, counterparties, members, registrants, or users could use the descriptions of cybersecurity risks to avoid certain Covered Entities with less well-developed cybersecurity procedures.

Public disclosures mitigate the information asymmetry. Customers, counterparties, members, registrants, or users can use the information to understand better the risks of doing business with certain Covered Entities. A Covered Entity disclosing that it addresses cybersecurity risks in a robust manner and that it has not experienced a significant cybersecurity incident or few such incidents could signal to customers, counterparties, members, registrants, or users that customer information, funds, and assets are safeguarded properly. In contrast, disclosures of sub-par cybersecurity practices or a history of significant cybersecurity incidents may convince customers, counterparties, members, registrants, or users to not do business with that Covered Entity.

In addition to mitigating information asymmetries with stakeholders in general, public disclosure would also mitigate a source of principal-agent problems in the customer-Covered Entity relationship. As discussed above, Covered Entities may have different incentives than customers in the area of cybersecurity prevention.⁸⁴³ Insofar as principals (customers) prefer a higher level of cybersecurity focus by agents (Covered Entities), public disclosure would act as an incentive for Covered Entities to increase their focus in this area and signal their commitment to protecting customers' funds and data.

The proposed requirement for Covered Entities to post the required disclosures on their websites would help inform, for example, retail customers about Covered Broker-Dealers because they are likely to look for information about their broker-dealers on the firm's websites. In addition, requiring the submission of Part II of proposed Form SCIR in a custom XML data language would likely facilitate more effective and thorough review, analysis, and comparison of cybersecurity risks and significant cybersecurity incidents by the Commission and by Covered Entities' existing and prospective customers, counterparties, members, registrants, or users.⁸⁴⁴ The public disclosure

⁸⁴³ See section IV.B. of this release (discussing broad economic considerations).

⁸⁴⁴ While the Commission would separately receive the information significant cybersecurity incidents impacting Covered Entities thought the filings of Part I of proposed Form SCIR, those filings would not include the Covered Entity's summary

⁸⁴¹ See sections II.B.3. and II.B.4. of this release (discussing these proposed requirements in more detail).

⁸⁴² See section IV.B. of this release (discussing broad economic considerations).

requirement of proposed Rule 10 expands Market Entities', other market participants', the public's, the Commission's, and other regulatory bodies' knowledge about the cybersecurity risks faced by Covered Entities as well as their past experiences regarding significant cybersecurity incidents that is beyond what is provided by current Commission regulations.

Requiring Covered Entities to file Part II of proposed Form SCIR through the EDGAR system would allow the Commission—as well as customers, counterparties, members, and users of Covered Entity services—to download the Part II disclosures directly from a central location, thus facilitating efficient access, organization, and evaluation of the reported disclosures about significant cybersecurity incidents. Likewise, because Part II of proposed Form SCIR would be structured in SCIR-specific XML, the public disclosures would be machine-readable and, therefore, more readily accessible to the public and the Commission for comparisons across Covered Entities and time periods. With centralized filing in EDGAR in a custom XML, Commission staff as well as Covered Entities' customers, counterparties, members, registrants, or users (and the Covered Entities themselves) would be better able to assemble, analyze, review, and compare a large collection of data about reported cybersecurity risks and significant cybersecurity incidents, which could facilitate the efficient identification of trends in cybersecurity risks and significant cybersecurity incidents in the U.S. securities markets.

Centralized filing of the summary descriptions of the Covered Entity's cybersecurity risks and significant cybersecurity incidents on Part II of proposed Form SCIR in a structured format on EDGAR would enable investors and others—such as other government agencies, standard-setting groups, analysts, market data aggregators, and financial firms—to more easily and efficiently compare how one Covered Entity compares with others in terms of cybersecurity risks and incidents. For example, banks assessing potential security-based swap counterparties could efficiently aggregate and compare disclosures of multiple security-based swap dealers. Similarly, public companies deciding which transfer agent to use could

description of the cybersecurity risks that could materially affect the Covered Entity's business and operations and how it assesses, prioritizes, and addresses those cybersecurity risks that would be disclosed on Part II of proposed Form SCIR.

efficiently aggregate and compare the disclosures of many transfer agents.

These market participants would also be able to discern broad trends in cybersecurity risks and incidents more efficiently due to the central filing location and machine-readability of the disclosures. The more efficient dissemination of information about trends regarding cybersecurity risks and significant cybersecurity incidents could, for example, enable Covered Entities to better and more efficiently determine if they need to modify, change, or upgrade their cybersecurity defense measures in light of those trends. Likewise, more efficient assimilation of information about trends in significant cybersecurity incidents could enable Covered Entities customers, counterparties, members, or users and their services to more efficiently understand and manage their cybersecurity risks. Accordingly, centralized EDGAR filing of public cybersecurity disclosures in a machine-readable data language could help reduce the number of Covered Entities or their customers, counterparties, members, or users that suffer harm from cybersecurity breaches, or reduce the extent of such harm in the market, thus helping prevent or mitigate cybersecurity-related disruptions to the orderly operations of the U.S. securities markets.

Lastly, Covered Entities rely on electronic information, communication, and computer systems to perform their functions.⁸⁴⁵ Because many Covered Entities play critical global financial system, a cyberattack against Covered Entities without strong cybersecurity protocols could lead to more widespread breaches. Therefore, the centralized, public, structured filing of cybersecurity disclosures with Part II of proposed Form SCIR, which would be updated promptly upon the occurrence of a new significant cybersecurity incident, would increase the efficiency with which new cybersecurity information would be assimilated into the market, thereby also likely increasing the speed with which Covered Entities could react to potential contagion. This increased agility on the part of Covered Entities could reduce potential contagion in the U.S. securities markets. Additionally, Covered Entities would know that the centralized, public filing of information about significant cybersecurity incidents would make comparison with their competitors easier, and this could motivate Covered Entities to take

⁸⁴⁵ See section I.A.2. of this release (discussing how Covered Entities use information systems).

cybersecurity preparedness and risk management more seriously than they might otherwise, either by devoting more resources to cybersecurity or by addressing cybersecurity risks in a more effective manner. Such an effect could help reduce the number and extent of cybersecurity incidents, particularly those that negatively impact the U.S. securities markets.

As with Part I of proposed Form SCIR, the Commission also is proposing to require Covered Entities to identify themselves on Part II of proposed Form SCIR with a UIC, such as an LEI, if they have obtained one, to help facilitate efficient collection and analysis of cybersecurity incidents in the financial markets. The addition of UICs could facilitate coordinated inter-governmental responses to cybersecurity incidents that affect U.S. firms.⁸⁴⁶ Existing identifiers that are not UICs are more limited in scope, such as CIK numbers, which are Commission-specific identifiers for companies and individuals that have filed reports with the Commission. This limits their utility in analyzing and comparing significant cybersecurity incidents among Covered Entities and non-Commission-regulated financial institutions.

The markets for different Covered Entities present customers, counterparties, members, registrants, or users with a complex, multi-dimensional, choice problem. In choosing a Covered Entity to work with, customers, counterparties, members, registrants, or users may consider cybersecurity risk exposure (*i.e.*, financial, operational, legal, etc.), past significant cybersecurity incidents, reputation, etc. While the Commission is not aware of any studies that examine the role perceptions of cybersecurity play in this choice problem, the extant academic literature suggests that investors focus on salient, headline-grabbing information, such as large losses of customer information, when

⁸⁴⁶ The Commission has recognized the benefits of LEIs in other contexts. See *Joint Industry Plan; Order Approving the National Market System Plan Governing the Consolidated Audit Trail*, Release No. 34-79318; File No. 4-698 (Nov. 15, 2016), 81 FR 84696, 84745 (Nov. 23, 2016) (“The Commission believes use of the LEI enhances the quality of identifying information for Customers by incorporating a global standard identifier increasingly used throughout the financial markets.”); *Investment Company Reporting Modernization*, Release Nos. 33-10231; 34-79095; IC-32314; File No. S7-08-15 (Oct. 13, 2016), 81 FR 81870, 81877 (Nov. 18, 2016) (“Uniform reporting of LEIs by funds [] will help provide a consistent means of identification that will facilitate the linkage of data reported on Form N-PORT with data from other filings and sources that is or will be reported elsewhere as LEIs become more widely used by regulators and the financial industry.”).

making such choices.⁸⁴⁷ Details regarding significant cybersecurity incidents may allow customers, counterparties, members, registrants, or users to assess the severity of one incident compared to that of another. However, the public disclosures will be generalized (*i.e.*, summary descriptions) to a degree such that threat actors cannot take advantage of known vulnerabilities. Therefore, to the extent that cybersecurity disclosures from Covered Entities are “boilerplate,” they may be less informative.⁸⁴⁸ Thus, it may be difficult to choose among Covered Entities that have experienced similar significant cybersecurity incidents.

Significant cybersecurity incidents—especially those that involve loss of data or assets of customers, counterparties, members, registrants, or users—are likely to garner attention. Thus, the Commission expects that the proposed requirement to disclose significant cybersecurity incidents would have a direct effect on the choices of customers, counterparties, members, registrants, or users. In addition, third parties such as industry analysts—who may be more capable of extracting useful information across Covered Entities’ disclosures—may incorporate it in assessment reports that are ultimately provided to customers, counterparties, members, registrants, or users. Whether directly or indirectly, Covered Entities with subpar cybersecurity policies and procedures—as revealed by a relatively large number of significant cybersecurity incidents—could face pressure to improve their policies and procedures to reduce such incidents.⁸⁴⁹

The disclosures of significant cybersecurity incidents also should benefit a Covered Entity’s current customers, counterparties, members, registrants, or users if the Covered Entity experiences a significant cybersecurity incident by providing notice that, for example, personal information, transaction data, securities, or funds may have been compromised. While the customers, counterparties, members, registrants, or users that are

⁸⁴⁷ See, *e.g.*, Brad M. Barber, Terrance Odean, and Lu Zheng, *Out of Sight, Out of Mind: The Effects of Expenses on Mutual Fund Flows*, 78 J. Bus. 2095 (2005) (“Out of Sight, Out of Mind”).

⁸⁴⁸ However, as discussed above, the process of adopting “boilerplate” language by Covered Entities may itself affect improvements in policies and procedures.

⁸⁴⁹ This assumes that customers, counterparties, members, registrants, or users evaluating the Covered Entities would favor those Covered Entities that include language that cites strong cybersecurity procedures in their disclosures. Further, the Commission assumes that customers, counterparties, members, registrants, and users would prefer to do business with Covered Entities that have “superior” cybersecurity procedures.

directly impacted may be individually notified of significant cybersecurity incidents based on individual state laws and Commission rules, thus initiating timely remedial actions, other parties may benefit from the disclosures. Specifically, customers, counterparties, members, registrants, or users that are not affected by a significant cybersecurity incident may take the time to change and strengthen passwords, monitor account activity on a more consistent basis, and audit their financial statements for discrepancies.

b. Costs

The requirements to have reasonably designed policies and procedures to address cybersecurity risk and to report significant cybersecurity incidents to the Commission by filing Part I of proposed Form SCIR on EDGAR would—in practice—require the collection of the information that also would be used in the proposed public disclosures required to be made on Part II of proposed Form SCIR. Therefore, the disclosure requirement itself would not impose significant compliance costs beyond those already discussed with respect to the requirements to have reasonably designed policies and procedures to address cybersecurity risk and to report significant cybersecurity incidents to the Commission by filing Part I of proposed Form SCIR on EDGAR.⁸⁵⁰ Generally, it is expected that a compliance analysis would be needed to summarize the cybersecurity risks faced by the Covered Entity and a summary of previous significant cybersecurity incidents. In addition, there may be internal legal review of the public disclosure and administrative costs would be incurred associated with posting the disclosure on the Covered Entity’s website.

However, if the action of disclosing summary descriptions of a Covered Entity’s cybersecurity risks and significant cybersecurity incidents encourages the Covered Entity and/or other Covered Entities to review their policies and procedures and potentially direct more resources to cybersecurity protection, that would be an additional cost. Moreover, the disclosures may impose costs due to market reactions and exploitable information they may reveal to adverse parties.

Depending on the Covered Entity, reports of many significant cybersecurity incidents and, to a lesser extent, reports of greater cybersecurity risks and exposure to financial, operational, legal, reputational, or other

⁸⁵⁰ See sections IV.D.2. and IV.D.3. of this release (discussing the costs of those requirements).

consequences that could materially affect its business and operations as a result of a cybersecurity incident adversely impacting its information systems may bear costs arising from reactions in the marketplace. That is, a Covered Entity may lose business or suffer harm to its reputation and brand value.⁸⁵¹ These costs would be borne by the affected Covered Entity even if it made reasonable efforts to prevent them. If customers, counterparties, members, registrants, or users “overreact”⁸⁵² to disclosures of significant cybersecurity incidents, Covered Entities may pursue a strategy of overinvesting in cybersecurity precautions (to avoid such overreactions), resulting in reduced efficiency. The extent of such costs likely depends on a number of factors, including the size of a Covered Entity relative to others in the same category (*e.g.*, Covered Broker-Dealers, national securities exchanges, and clearing agencies), the severity and scope of the cybersecurity incident, and the availability of substitutes for a given Covered Entity.⁸⁵³

The national securities exchanges and clearing agencies that are currently registered with the Commission but are not active would not incur any costs related to the proposed public disclosure requirement if they remain inactive. However, if their operations restart, they likely would incur

⁸⁵¹ Customers, counterparties, members, registrants, and users would be more likely to act in response to realized significant cybersecurity incidents than in response to Covered Entities’ descriptions of their cybersecurity risks and how they address those risks.

⁸⁵² Such overreactions can be the result of overconfidence about the precision of the signal. See, *e.g.*, Kent Daniel, David Hirshleifer and Avanihar Subrahmanyam, *Investor Psychology and Security Market Under- and Overreactions*, 53 J. Fin. 1839 (1998); see also *Out of Sight, Out of Mind*.

⁸⁵³ One can differentiate between the smallest and largest Covered Broker-Dealer. A large broker-dealer may be more able to absorb more costs associated with a cybersecurity incident and continue to stay in business than a small broker-dealer. In addition, a large broker-dealer could have a more prestigious reputation that may persuade customers to continue using it despite the cybersecurity event. Or a large broker-dealer could have more news about it in the public domain that dilutes bad news about cybersecurity incidents, whereas a smaller firm’s name may become inextricably associated with one significant cybersecurity incident. In addition, significant cybersecurity incidents that are crippling and affect all of a Covered Entity’s customers, counterparties, members, registrants, and users would be more costly its reputation than ones that are more localized. Lastly, the cost of lost business for a Covered Entity may be muted if there are fewer competitors to choose from. For example, there is only one national securities association (*i.e.*, FINRA) relative to 353 transfer agents. It therefore could be costly in terms of lost business for a transfer agent as its customers can transfer their business to one of the many others that perform the same services.

moderate costs associated with the disclosure because they may need to restart their websites and provide summary descriptions of their cybersecurity risks. No significant cybersecurity incidents would need to be disclosed initially since they have been dormant for so long. In addition, many transfer agents do not have websites. Therefore, those transfer agents that do not have websites would incur the cost of obtaining a domain name as well as establishing and maintaining a website (either by themselves or using a third party) before being able to post their public disclosures. Small, independent broker-dealers also may not have websites. In a 2015 survey of 13 broker-dealers, 80% of respondents stated that they have a web policy or program; however, 7.6% do not have a web policy or program and 13.3% of the respondents were not sure. Furthermore, 47% of respondents reported that less than half of their firm's advisors (*i.e.*, registered representatives) currently have a website. Interestingly, the survey participants noted the value of having a website to establish credibility (80%), generate leads (53%), get referrals (40%), qualify and engage prospects (40%) and maintain existing client relationships (47%).⁸⁵⁴ The remaining Market Entities likely have websites.

Website costs can be broken into several categories: (1) obtaining a domain name (\$12 to \$15 per year); (2) web hosting (\$100 per month for premium service); (3) website theme or template (one-time fee of \$20 to \$200 or more); and SSL certificate (\$10 to \$200 per year).⁸⁵⁵ Ongoing website costs could be as high as \$1,215 per year to maintain.

Mandating the disclosure of significant cybersecurity incidents entails a tradeoff. While disclosure can inform customers, counterparties, members, registrants, and users, disclosure can also inform cyber attackers that they have been detected. Also, disclosing too much (*e.g.*, the types of systems that were affected and how they were compromised) could be used by threat actors to better attack their targets, imposing subsequent

potential losses on Covered Entities. For example, announcing a significant cybersecurity incident naming a specific piece of malware and the degree of compromise can provide details about the structure of the target's computer systems, the security measures employed (or not employed), and potentially suggest promising attack vectors for future targets by other would-be attackers.

Under proposed Rule 10, to mitigate these costs and to promote compliance with the disclosure requirements, each Covered Entity would be required to disclose summary descriptions of their cybersecurity risks and significant cybersecurity incidents on Part II of proposed Form SCIR.⁸⁵⁶ In the summary description of the significant cybersecurity incident, the Covered Entity would need to identify: (1) the person or persons affected; (2) the date the incident was discovered and whether it is still ongoing; (3) whether any data were stolen, altered, or accessed or used for any other unauthorized purpose; (4) the effect of the incident on the Covered Entity's operations; and (5) whether the Covered Entity, or service provider, has remediated or is currently remediating the incident.⁸⁵⁷ Thus, Covered Entities generally would not be required to disclose technical details about significant cybersecurity incidents that could compromise their cybersecurity protections going forward. As before, the costs associated with conveying this information to attackers is impracticable to estimate.⁸⁵⁸

While registering with the EDGAR system is free, the requirement to centrally file Part II of proposed Form SCIR in EDGAR would impose incremental costs on Covered Entities that have not previously filed documents in EDGAR. More specifically, Covered Entities that have never made a filing with the Commission via EDGAR would need to file a notarized Form ID, which is used to request the assignment of access codes to file on EDGAR. Thus, first-time EDGAR filers would incur modest costs associated with filing Form ID.⁸⁵⁹ That

said, Covered Entities that already file documents in EDGAR would not incur the cost of having to register with EDGAR. As discussed earlier, the extent to which different categories of Covered Entities are already required to file documents in EDGAR varies. For example, SBSs, MSBSPs, SBSRs, and transfer agents are already required to file some forms in EDGAR.

Likewise, as mentioned earlier, the Commission approved a UIC—namely, the LEI—in a previous rulemaking. The Commission could approve another standard identifier as a UIC in the future, but currently the LEI is the only approved UIC. Covered Entities that already have an LEI would not bear any cost to including it on proposed Form SCIR, as they would have already paid to obtain and maintain an LEI for some other purpose. Covered Entities that do not already have an LEI are not required to obtain an LEI in order to file proposed Form SCIR, thus, there is no additional cost to those Covered Entities that do not have an LEI.

In addition, a Covered Broker-Dealer would be required to provide the written disclosure form to a customer as part of the account opening process. Thereafter, the Covered Broker-Dealer would need to provide the customer with the written disclosure form annually and when it is updated using the same means that the customer elects to receive account statements (*e.g.*, by email or through some type of postal service). The Commission anticipates that the cost of initial and annual reporting will be negligible because the report text can be incorporated into other initial disclosures and periodic statements. The cost of furnishing updated reports in response to significant cybersecurity incidents depends on the degree to which such incidents occur and are detected, which cannot reliably be predicted. The Commission assumes that the delivery costs are the same regardless of the delivery method.

To estimate the costs associated for a Covered Entity to file a Part II of proposed Form SCIR with the Commission through EDGAR, as well as post a copy of the form on its website, the Commission considered the initial and ongoing compliance costs.⁸⁶⁰ The internal annual costs for these requirements (which include an initial burden estimate annualized over a three year period) are estimated to be \$1,377.46 per Covered Entity, and \$2,739,767.94 in total. These costs include a blended rate of \$375.33 for an

⁸⁵⁴ See *Broker Dealers and Web Marketing: What You Should Know* (Dec. 9, 2015), available at <https://www.advisorwebsites.com/blog/blog/general/broker-dealers-and-web-marketing-what-you-should-know#:~:text=While%2080%25%20of%20Broker-Dealers%20reps%20we%20polled%20say,to%20build%20and%20maintain%20a%20strong%20web%20presence>.

⁸⁵⁵ See Jennifer Simonson, *website Hosting Cost Guide 2023*, *Forbes*, available at <https://www.forbes.com/advisor/business/website-hosting-cost/>.

⁸⁵⁶ See paragraph (d)(1) of proposed Rule 10.

⁸⁵⁷ See paragraph (d)(1)(ii) of proposed Rule 10.

⁸⁵⁸ As noted in section IV.B. of this release, firms are generally hesitant to provide information about cyberattacks. Similarly, cybercriminals are not generally forthcoming with data on attacks, their success, or factors that made the attacks possible. Consequently, data from which plausible estimates could be made is not available.

⁸⁵⁹ Any Covered Entity that has made at least one filing with the Commission via EDGAR since 2002 has been entered into the EDGAR system by the Commission and will not need to file Form ID to file electronically on EDGAR.

⁸⁶⁰ See section V of this release (discussing these costs in more detail).

assistant general counsel, senior compliance examiner, and compliance manager for a total of 3.67 hours. The annual external costs for these requirements are estimated to be \$1,488 per Covered Entity, and \$2,959,632 in total. This includes the cost of using outside legal counsel at a rate of \$496 per hour for a total of three hours.

To estimate the costs associated for a Covered Broker-Dealer to deliver its disclosures to new customers, as well as deliver disclosures to existing customers on an annual basis, the Commission considered the initial and ongoing compliance costs.⁸⁶¹ The internal annual costs for these requirements (which include an initial burden estimate annualized over a three year period) are estimated to be \$3,536.94 per Covered Broker-Dealer, and \$5,450,424.54 in total. These costs include a rate of \$69 per hour for a general clerk for a total of 51.26 hours. It is estimated that there will be \$0 annual external cost for this additional disclosure requirement for Covered Broker-Dealers. With respect to the additional disclosure fees for broker dealers, the cost covers the clerks employed by the broker-dealers for stuffing envelopes and mailing them out. The legal fees associated with drafting the disclosure is already tied to the burden of filing the disclosure in Part II of EDGAR and putting the disclosure on its website.

c. Request for Comment

The Commission requests comment on all aspects of the foregoing analysis of the benefits and costs of the requirements to provide immediate notification and subsequent reporting of significant cybersecurity incidents. Commenters are requested to provide empirical data in support of any arguments or analyses. In addition, the Commission is requesting comment on the following matters:

16. Please provide views on the benefits and costs associated with posting the public disclosures on Covered Entities' websites and submitting them to the Commission through EDGAR. Will the general nature of the public disclosure be useful to Market Entities as well as customers, counterparties, members, participants, and users? Should the Commission require Covered Entities to both post cybersecurity risk and incident histories on Covered Entity websites and file that information on Part II of proposed Form SCIR in EDGAR? Should the Commission exempt some subset(s) of

Covered Entities from the requirement to file Part II of proposed Form SCIR in EDGAR? If so, please explain. Should the Commission exempt some subset(s) of Covered Entities from the requirement to post cybersecurity risk and incident history information on their websites? Explain.

17. Are the cost estimates associated with posting the public disclosure on the Covered Entities' websites, submitting Part II of proposed Form SCIR to the Commission through EDGAR, and providing disclosures to new and existing customers reasonable? If not, explain why? Are there any other benefits and costs of these proposed requirements? If so, please describe them.

18. Are there any other costs and benefits associated with requiring Covered Entities to file Part II of proposed Form SCIR using a structured data language? If so, please describe them. Should the Commission require Covered Entities to file Part II of proposed Form SCIR using a structured data language, such as a custom XML? Should the Commission require Covered Entities to file Part II of proposed Form SCIR using a different structured data language than a custom XML, such as Inline XBRL? Why or why not?

19. Are there any Covered Entities for whom the proposed structured data requirements of Part II of proposed Form SCIR should be exempted? If so, what particular exemption threshold or thresholds should the Commission use for the structured data requirements under the proposed rule amendments, and why?

20. Please provide views on the benefits and costs associated with requiring Covered Entities to identify themselves on Part II of proposed Form SCIR with both a CIK number and a UIC (such as an LEI)? What would be the benefits and costs of requiring Covered Entities without a UIC to obtain one in order to file Part II of proposed Form SCIR? What, if any, standard identifiers should the Commission require Covered Entities to use to identify themselves on Part II of proposed Form SCIR?

21. What would be the benefits and costs of requiring Covered Entities to place the required cybersecurity risk and incident history disclosures on individual Covered Entity websites and in EDGAR with Part II of proposed Form SCIR relative to the alternatives discussed below in section IV.F. of this release? Should the Commission instead adopt one of the alternatives for the requirements around where Covered Entities must place the public cybersecurity disclosures? Specifically, the Commission is proposing to require

Covered Entities to publish the disclosures on their individual firm websites and to file the information in EDGAR using Part II of proposed Form SCIR. Should the Commission eliminate one, or both, of those requirements?

22. Are there any Covered Entities for whom the proposed structured data requirements for Part II of proposed Form SCIR should be exempted? If so, what particular exemption threshold or thresholds should the Commission use for the structured data requirements under the proposed rule amendments, and why?

5. Record Preservation and Maintenance by Covered Entities

As discussed above, proposed Rule 10 would require a Covered Entity to: (1) establish, maintain, and enforce written policies and procedures that are reasonably designed to address cybersecurity risks; (2) create written documentation of risk assessments; (3) create written documentation of any cybersecurity incident, including its response to and recovery from the incident; (4) prepare a written report each year describing its annual review of its policies and procedures to address cybersecurity risks; (5) provide immediate written notice of a significant cybersecurity incident; (6) report a significant cybersecurity incident on Part I of proposed Form SCIR; and (7) provide a written disclosure containing a summary description of its cybersecurity risk and significant cybersecurity incidents on Part II of proposed Form SCIR. Consequently, proposed Rule 10 would require a Covered Entity to create several different types of records, but it would not include its own record preservation and maintenance provisions. Instead, these requirements would be imposed through amendments, as necessary, to the existing record preservation and maintenance rules applicable to the Covered Entities. In particular, the Commission is proposing to amend the record preservation and maintenance rules for: (1) broker-dealers (*i.e.*, Rule 17a-4); (2) SBS Entities (*i.e.*, Rule 18a-6); and (3) transfer agents (*i.e.*, Rule 17ad-7). The proposed amendments would specify that the Rule 10 Records must be retained for three years. In the case of the written policies and procedures to address cybersecurity risks, the record would need to be maintained until three years after the termination of the use of the policies and procedures.

The existing record maintenance and preservation rule applicable to registered clearing agencies, the MSRB, national securities associations, and

⁸⁶¹ See section V of this release (discussing these costs in more detail).

national securities exchanges (*i.e.*, Rule 17a-1) requires these categories of Covered Entities keep and preserve at least one copy of all documents, including all correspondence, memoranda, papers, books, notices, accounts, and other such records as shall be made or received by the Covered Entity in the course of its business as such and in the conduct of its self-regulatory activity. Under the existing provisions of Rule 17a-1, registered clearing agencies, the MSRB, national securities associations, and national securities exchanges would be required to preserve at least one copy of the Rule 10 Records for at least five years, with the first two years in an easily accessible place. Similarly, the existing record maintenance and preservation rule applicable to SBSDRs (*i.e.*, Rule 13n-7) requires these Market Entities to preserve records. And with respect to exempt clearing agencies, the Commission is proposing to amend the clearing agency exemption orders to add a condition that each exempt clearing agency must retain the Rule 10 Records for a period of at least five years after the record is made or, in the case of the written policies and procedures to address cybersecurity risks, for at least five years after the termination of the use of the policies and procedures.

a. Benefits

There would be a number of benefits for Covered Entities to preserving and maintaining the Rule 10 records. With respect to cybersecurity policies and procedures and the written documentation concerning risk assessments and any cybersecurity incidents, the Covered Entity's records could be reviewed for compliance purposes as well as a reference in future self-conducted audits of the Covered Entity's cybersecurity system. In addition, the written report each year describing the Covered Entity's annual review of its policies and procedures could be used to determine if the Covered Entity's cybersecurity risk management program is working as expected and to see if any changes should be made. Lastly, maintaining records of compliance would assist the Commission in its oversight role, particularly when conducting examinations of Covered Entities. With respect to the immediate written notice of a significant cybersecurity incident, as well as any submitted Part I of proposed Form SCIR, the records would facilitate examination of Covered Entities for compliance with proposed Rule 10.

Finally, with respect to the public disclosures that Covered Entities would

make on Part II of proposed Form SCIR, keeping records of these forms and submissions would be beneficial to Covered Entities for compliance purposes as well as use as a reference when updating the public disclosure. For example, a Covered Entity would need to file an updated Part II of proposed Form SCIR if the information in the summary description of a significant cybersecurity incident included on the form is no longer within the look-back period (*i.e.*, the current or previous calendar year). However, the retention period for the records (*e.g.*, three years in the case of broker-dealers, SBS Entities, and transfer agents, or five years in the case of registered clearing agencies, the MSRB, national securities associations, national securities exchanges, SBSDRs, and certain exempt clearing agencies) would require the Covered Entity to maintain a record of that particular public disclosure for a longer period of time.

Benefits also arise due to the Commission's regulation and oversight of Covered Entities with respect to their books and records.⁸⁶²

b. Costs

The costs associated with preserving the Covered Entity's cybersecurity policies and procedures and annual review are likely to be small. The cost would result from the requirement to preserve the Rule 10 Records for either three or five years. Given that the incremental volume of records that each Covered Entity would be required to retain would be relatively small, the costs should be minimal. Moreover, Covered Entities subject to other record retention requirements likely already have a system in place to maintain those records. Therefore, adding the records associated with proposed Rule 10 likely would be a small burden.

To estimate the costs associated for a Covered Entity to comply with its recordkeeping maintenance and preservation requirement, the Commission considered the initial and ongoing compliance costs.⁸⁶³ The internal annual cost for this requirement is estimated to be \$441 per Covered Entity, and \$877,149 in total. These costs include a blended rate of \$73.50 for a general clerk and compliance clerk for a total of 6 hours. It is estimated that there will be \$0 annual external cost for

⁸⁶² The Commission also would retain copies of Parts I and II of proposed Form SCIR filed through EDGAR.

⁸⁶³ See section V of this release (discussing these costs in more detail).

the recordkeeping maintenance and preservation requirement.

c. Request for Comment

The Commission requests comment on all aspects of the foregoing analysis of the benefits and costs of the proposed record preservation and maintenance requirements. Commenters are requested to provide empirical data in support of any arguments or analyses. In addition, the Commission is requesting comment on the following matter:

23. Are there any other benefits and cost associated with the requirements to preserve the Rule 10 Records? If so, please describe them.

6. Policies and Procedures, Annual Review, Immediate Notification of Significant Cybersecurity Incidents, and Record Preservation Requirements for Non-Covered Broker-Dealers

As discussed earlier, proposed Rule 10 would require Non-Covered Broker-Dealers to establish, maintain, and enforce written policies and procedures that are reasonably designed to address their cybersecurity risks taking into account the size, business, and operations of the firm.⁸⁶⁴ The proposed rule also would require Non-Covered Broker-Dealers to review the design and effectiveness of their cybersecurity policies and procedures annually, including whether the policies and procedures reflect changes in cybersecurity risk over the time period covered by the review. Furthermore, Non-Covered Broker-Dealers would be required to provide the Commission and their examining authority with immediate written electronic notice of the occurrence of a significant cybersecurity incident.⁸⁶⁵ The Commission also is proposing to amend the record preservation and maintenance rule for broker-dealers (Rule 17a-4) to specifically require Non-Covered Broker-Dealers to preserve certain records in connection with Rule 10.

a. Benefits

The requirement under proposed Rule 10 for Non-Covered Broker-Dealers to establish, maintain, and enforce written policies and procedures that are reasonably designed to address their cybersecurity risks would generally

⁸⁶⁴ See section I.I.C.1. of this release (discussing in more detail the proposed policies and procedures, annual review, and record preservation requirements for Non-Covered Broker-Dealers).

⁸⁶⁵ The Commission is not proposing that Non-Covered Broker Dealers be subject to the requirements to file Parts I and II of proposed Form SCIR and post copies of the most recently filed Part II of proposed Form SCIR on their websites and provide copies of that filing to their customers.

improve cybersecurity preparedness of Non-Covered Broker-Dealers—and hence reduce their clients' exposure to cybersecurity incidents. This is because, in establishing and maintaining a set of cybersecurity policies and procedures in a written format, a Non-Covered Broker-Dealer can evaluate whether its cybersecurity policies and procedures continue to work as designed and whether changes are needed to assure their continued effectiveness. In addition, by permitting Non-Covered Broker-Dealers to take into account their size, business, and operations of the firm when designing their written policies and procedures, Non-Covered Broker-Dealers can more efficiently utilize their resources. Moreover, by requiring Non-Covered Broker-Dealers to establish reasonably designed cybersecurity policies and procedures, the Commission would be better able to understand the protections that these broker-dealers put in place to address cybersecurity risk. During an examination, the Commission can assess the adequacy and completeness of a Non-Covered Broker-Dealers cybersecurity policies and procedures. Documenting a Non-Covered Broker-Dealer's cybersecurity policies and procedures in a written format also would aid the Commission in its review and oversight.

Due to the varying sizes and operations of Non-Covered Broker-Dealers, the benefits that accrue from the cybersecurity policies and procedures requirement likely differ across entities. Because Non-Covered Broker-Dealers are generally smaller and have fewer assets and interconnections with other Market Entities than Covered Broker-Dealers, there is less of a risk that a significant cybersecurity incident at a Non-Covered Broker-Dealer could provide the threat actor with access to other Market Entities. However, even though a Non-Covered Broker-Dealer may not pose a significant overall risk to the U.S. securities markets, a significant cybersecurity event at a Non-Covered Broker-Dealer could have profound negative effects if a threat actor is able to misappropriate customers' confidential financial information. Consequently, greater cybersecurity investment by a Non-Covered Broker-Dealer likely would lead to significant benefits for itself and its customers.

Non-Covered Broker-Dealers may already have implemented cybersecurity policies and procedures. The marginal benefits of the proposed rule would be mitigated to the extent that these existing policies and procedures are consistent with the proposed rule's

requirements. However, existing policies and procedures that are already consistent with the proposed rule would facilitate Non-Covered Broker-Dealers in conducting annual reviews, assessing the design and effectiveness of their cybersecurity policies and procedures, and making necessary adjustments.

The primary benefit of reviewing a Non-Covered Broker-Dealer's cybersecurity policies and procedures on an annual basis would help to ensure that they are working as designed, that they accurately reflect the firm's cybersecurity practices, and that they reflect changes and developments in the firm's cybersecurity risk over the time period covered by the review. The documented policies and procedures would serve as a benchmark when conducting the annual review. The Non-Covered Broker-Dealer would be required, for compliance purposes and future reference, to make a written record that documents the steps taken in performing the annual review and the conclusions of the annual review.

Cybersecurity threats constantly evolve, and threat actors consistently identify new ways to infiltrate information systems. An annual review requirement would ensure that Non-Covered Broker-Dealers conduct a regular assessment and undertake updates to prevent policies and procedures from becoming stale or ineffective, in light of the dynamism of cybersecurity threats.

The primary benefit of requiring Non-Covered Broker-Dealers to retain their written cybersecurity policies and procedures as well as a record of the annual reviews, is to assist the Commission in its oversight function. In reviewing their records, Non-Covered Broker-Dealers may see trends in their own cybersecurity risks, which may serve as an impetus to make adjustments to their cybersecurity policies and procedures. Furthermore, Proposed Rule 10 would expand beyond current Commission regulations Non-Covered Broker-Dealers' cybersecurity policies and procedures that address all cybersecurity risks that may affect their information systems and the funds and securities as well as personal, confidential, and proprietary information that may be stored on those systems.

As noted above, Non-Covered Broker-Dealers would be required to give the Commission immediate written electronic notice of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring. Compared to the suite of proposed requirements for

Covered Entities, including filing Parts I and II of proposed Form SCIR and publicly disclosing Part II (which would contain summary descriptions of the Covered Entity's cybersecurity risks and significant cybersecurity incidents that occurred in current and previous calendar years), the proposed requirement to provide immediate written electronic notice of significant cybersecurity incidents is relatively small but can yield significant benefits. Most notably, such immediate notifications would make Commission staff aware of significant cybersecurity incidents across all broker-dealers and not just at Covered Broker-Dealers, thus significantly increasing its oversight powers in the broker-dealer space with respect to cybersecurity incidents. Trends that impact Non-Covered Broker-Dealers, such as through malware or a particular type of software, may be detected by staff, which can then inform other Market Entities of emerging risks. This is particularly important due to the interconnected nature of the U.S. securities industry. Breaches that occur at Non-Covered Broker-Dealers may spread to larger firms, such as Covered Entities, that could cause more widespread financial disruptions. Furthermore, we anticipate that the burden on Non-Covered broker dealers of furnishing immediate written notification of a significant cybersecurity incident will be minimal.⁸⁶⁶

b. Costs

The costs associated with proposed Rule 10 for Non-Covered Broker-Dealers with respect to the written cybersecurity policies and procedures requirements would primarily result from establishing written cybersecurity policies and procedures that are reasonably designed. Such costs may be passed on to the Non-Covered Broker-Dealers' customers, either in part or in full.

Many Non-Covered Broker-Dealers currently have cybersecurity policies and procedures in place; to the extent a Non-Covered Broker-Dealer's existing policies and procedures are consistent with the requirements of the proposed rule, those Non-Covered Broker-Dealers would have limited need to update those policies and procedures, thus mitigating the costs of the proposal. Non-Covered Broker-Dealers may be subject to Regulation S-P, Regulation S-ID, and state regulations. In those particular instances, they may have already implemented policies and procedures that are consistent with the requirements of the proposed Rule 10,

⁸⁶⁶ See section IV.D.6.b. of this release.

which would mitigate some of the compliance costs associated with the proposed policies and procedures requirements.

The cost of complying with the proposed annual review requirement along with the accompanying written review and conclusion would depend on the size, business, and operations of the Non-Covered Broker-Dealer. A Non-Covered Broker-Dealer with simpler operations likely would incur lower annual review and modification costs than firms with larger operations. Furthermore, a Non-Covered Broker-Dealer may choose to hire a third-party for assistance or consultation regarding the completion of a written annual review and conclusion. This cost, in those situations, would depend on the services requested and the fees that are charged by the third-parties and consultants. Such costs could be passed along to the Non-Covered Broker-Dealer's customers depending on the competitive nature of the Non-Covered Broker-Dealer's market and its business model.

In either case, Non-Covered Broker-Dealers could tailor the policies and procedures to its cybersecurity risks taking into account its size, business, and operations. This offers Non-Covered Broker-Dealers the flexibility to implement cybersecurity policies and procedures based on the sophistication and complexity of their information systems. Of course, the cost of cybersecurity systems and modifications to cybersecurity policies and procedures may be higher as the size, business, and operation of a Non-Covered Broker-Dealer increases and becomes more complex.

The costs associated with giving the Commission immediate written electronic notice of a significant cybersecurity incident are likely to be relatively similar to, or possibly somewhat larger, than those incurred by Covered Broker-Dealers. As noted previously, the cost of immediate notification consists of notifying the Commission of a significant cybersecurity incident upon having a reasonable basis to conclude it has occurred or is occurring as well as researching the detailing of the incident in question. Non-Covered Broker-Dealers may be able to make the same determination and notify the Commission in the same amount of time as their Covered Broker-Dealer counterparts. However, smaller broker-dealers may not have the staffing or information technology expertise to make a reasonable decision about a suspected significant cybersecurity event as quickly as a Covered Broker-

Dealer that may have in-house staff dedicated to this function, thus increasing the overall immediate notification cost. On the other hand, smaller broker-dealers could instead contract with third parties for cybersecurity functions that could identify plausible significant cybersecurity attacks in the same amount of time as Covered Broker-Dealers. Unlike Covered Broker-Dealers, Non-Covered Broker-Dealers do not have to provide more detail beyond the immediate written notification requirement. Additional information regarding significant cybersecurity incidents do not have to be provided to the Commission on a confidential basis through the filing of Part I of proposed Form SCIR. Moreover, a summary of past incidents do not have to be publicly disclosed on their websites and with the Commission.

To estimate the costs associated with the proposed policies and procedures requirements and annual review requirements, the Commission considered the initial and ongoing compliance costs.⁸⁶⁷ The internal annual costs for these requirements (which include an initial burden estimate annualized over a three year period) are estimated to be \$9,702 per Non-Covered Broker-Dealer, and \$19,103,238 in total. These costs include a blended rate of \$462 for a compliance attorney and assistant general counsel for a total of 21 hours. The annual external costs for adopting and implementing the policies and procedures, as well as the annual review of the policies and procedures are estimated to be \$2,480 per Non-Covered Broker-Dealer, and \$4,883,120 in total. This includes the cost of using outside legal counsel at a rate of \$496 per hour for a total of five hours.

The cost associated Non-Covered Broker Dealer to research a suspected cybersecurity incident and provide immediate written notification to the Commission were combined earlier with those costs for Covered Entities.⁸⁶⁸ Broken out solely for Non-Covered Broker-Dealers, the Commission considered the initial and ongoing compliance costs. The internal annual costs for these requirements (which include an initial burden estimate annualized over a three year period) are estimated to be \$1,648.51 per Non-Covered Broker-Dealer, and \$3,245,916 in total. These costs include a blended rate of \$353 for an assistant general

counsel, compliance manager, and systems analyst for a total of 4.67 hours. The annual external costs for these requirements are estimated to be \$1,488 per Non-Covered Broker-Dealer, and \$2,959,872 in total. This includes the cost of using outside legal counsel at a rate of \$496 per hour for a total of three hours.

Pursuant to proposed Rule 10, a Non-Covered Broker-Dealer would be required to: (1) establish, maintain, and enforce written policies and procedures that are reasonably designed to address the cybersecurity risks of the firm; (2) make a written record that documents its annual review; and (3) provide immediate electronic written notice to the Commission of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring. The additional cost of the proposed amendments to Rule 17a-4 of preserving and maintaining these documents for three years, whether in paper or digital form, is likely minimal.

To estimate the costs associated for a Non-Covered Broker-Dealer to comply with its recordkeeping maintenance and preservation requirement, the Commission considered the initial and ongoing compliance costs.⁸⁶⁹ The internal annual cost for this requirement is estimated to be \$220.50 per Non-Covered Broker-Dealer, and \$434,164.50 in total. These costs include a blended rate of \$73.50 for a general clerk and compliance clerk for a total of 2 hours. It is estimated that there will be \$0 annual external cost for the recordkeeping maintenance and preservation requirement.

c. Request for Comment

The Commission requests comment on all aspects of the foregoing analysis of the benefits and costs of the proposed requirements for Non-Covered Broker-Dealers. Commenters are requested to provide empirical data in support of any arguments or analyses. In addition, the Commission is requesting comment on the following matters:

24. What level of cybersecurity policies and procedures have Non-Covered Broker-Dealers implemented? For example, would they meet the cybersecurity policies and procedures requirements of the proposed rule, thus making the compliance cost relatively low? Are those policies and procedures documented?

25. Are there any other benefits and costs for a Non-Covered Broker-Dealer

⁸⁶⁷ See section V of this release (discussing these costs in more detail).

⁸⁶⁸ See section IV.D.3.b. of this release (discussing the cost of immediate notification).

⁸⁶⁹ See section V of this release (discussing these costs in more detail).

in establishing, maintaining, and enforcing written policies and procedures under proposed Rule 10? If so, please describe them.

26. Are the estimated costs of compliance for Non-Covered Broker-Dealers to establish, maintain, and enforce written policies and procedures cybersecurity policies and procedures that comply with the proposed rule reasonable? If not, why not?

27. Would Non-Covered Broker-Dealers consult with a third party or hire a consultant with cybersecurity expertise in order to establish the cybersecurity policies and procedures under proposed Rule 10?

28. Are there quantifiable benefits to complying with the cybersecurity policies and procedures requirements of the proposed rule? If so, please describe them. Are there quantifiable costs for Non-Covered Broker-Dealers to review their cybersecurity policies annually that are different than those discussed above? If so, describe them.

29. Are there any other benefits in reviewing and updating Non-Covered Broker-Dealers' cybersecurity policies and procedures on an annual basis? If so, please describe them.

30. Is the estimated cost to review Non-Covered Broker-Dealers cybersecurity policies and procedures reasonable? If not, explain why?

31. Would it be more or less costly to outsource the responsibility of an annual review of cybersecurity policies and procedures to a third party?

7. Substituted Compliance for Non-U.S. SBS Entities

Commission Rule 3a71-6 states that the Commission may, conditionally or unconditionally, by order, make a determination with respect to a foreign financial regulatory system that compliance with specified requirements under such foreign financial regulatory system by a registered SBS Entity or class thereof, may satisfy the certain requirements that would otherwise apply to such an SBS Entity (or class thereof). The Commission may make such substituted compliance determinations to permit SBS Entities that are not U.S. persons (as defined in 17 CFR 240.3a71-3(a)(4)), but not SBS Entities that are U.S. persons, to satisfy the eligible requirements by complying with comparable foreign requirements.⁸⁷⁰ The Commission is proposing to amend Rule 3a71-6 to permit eligible applicants⁸⁷¹ to seek a Commission determination with respect to the cybersecurity requirements of

proposed Rule 10 and Form SCIR as applicable to SBS Entities that are not U.S. persons.⁸⁷² Additionally, Rule 3a71-6 currently permits eligible applicants to seek a substituted compliance determination from the Commission with regard to the requirements of Rule 18a-6, including the proposed amendments to Rule 18a-6 if adopted.⁸⁷³

a. Benefits

The Commission is proposing amendments to Rule 3a71-6 to make substituted compliance available to eligible SBS Entities that are not U.S. persons, if the Commission determines that compliance with specified requirements under a foreign financial regulatory system by a registered SBS Entity, or class thereof, satisfies the corresponding requirements of proposed Rule 10 and Form SCIR. Other regulatory regimes may achieve regulatory outcomes that are comparable to the Commission's proposed cybersecurity risk management requirements. Allowing for the possibility of substituted compliance may avoid regulatory duplication and conflict that may increase entities' compliance burdens without an analogous increase in benefits. The availability of substituted compliance could decrease the compliance burden for non-U.S. SBS Entities, in particular as it pertains to the establishment, maintenance, and enforcement of cybersecurity policies and procedures, notification and reporting to regulators, disclosure of cybersecurity risks and incidents, and record preservation. Allowing for the possibility of substituted compliance may help achieve the benefits of proposed Rule 10, Form SCIR, and the proposed amendments to Rule 18a-6 in a manner that avoids the costs that SBS Entities that are not U.S. persons would have to bear due to regulatory duplication or conflict.

Further, substituted compliance may have broader market implications, namely greater foreign SBSs' activity in the U.S. market, expanded access by both U.S. and foreign SBS Entities to global liquidity, and reduced possibility of liquidity fragmentation along jurisdictional lines. The availability of substituted compliance for non-U.S. SBS Entities also could promote market efficiency, while enhancing competition in U.S. markets. Greater participation and access to liquidity is likely to improve efficiencies related to hedging and risk sharing while simultaneously

increasing competition between domestic and foreign SBS Entities.

b. Costs

The Commission believes that the availability of substituted compliance for proposed Rule 10, Form SCIR, and the proposed amendments to Rule 18a-6 will not substantially alter the benefits intended by those requirements. In particular, it is expected that the availability of substituted compliance will not detract from the risk management benefits that stem from implementing proposed Rule 10, Form SCIR, and the proposed amendments to Rule 18a-6.

To the extent that substituted compliance reduces duplicative compliance costs, non-U.S. SBS Entities may incur lower overall costs associated with cybersecurity preparedness than they would otherwise incur without the option of substituted compliance availability, either because a non-U.S. SBS Entity may have already implemented foreign regulatory requirements which have been deemed comparable by the Commission, or because security-based swap counterparties eligible for substituted compliance do not need to duplicate compliance with two sets of comparable requirements.

A substituted compliance request can be made either by a foreign regulatory jurisdiction on behalf of its market participants, or by the registered market participant itself.⁸⁷⁴ The decision to request substituted compliance is voluntary, and therefore, to the extent that requests are made by individual market participants, such participants would request substituted compliance only if compliance with foreign regulatory requirements was less costly, in their own assessment, than compliance with both the foreign regulatory regime and the relevant Title VII requirements, including the requirements of proposed Rule 10, Form SCIR, and the proposed amendments to Rule 18a-6. Even after a substituted compliance determination is made, market participants would only choose substituted compliance if the benefits that they expect to receive exceed the costs that they expect to bear for doing so.

E. Effects on Efficiency, Competition, and Capital Formation

As discussed in the foregoing sections, market imperfections could lead to underinvestment in cybersecurity by Market Entities, and information asymmetry could contribute

⁸⁷⁰ See 17 CFR 240.3a71-6(d).

⁸⁷¹ See 17 CFR 240.3a71-6(c).

⁸⁷² See section II.D.3.

⁸⁷³ See paragraph (d)(6) of Rule 3a71-6.

⁸⁷⁴ See 17 CFR 240.3a71-6(c).

to a market-wide inefficient provision of cybersecurity defenses. The proposed rule aims to mitigate the inefficiencies resulting from these imperfections by: (1) imposing mandates for cybersecurity policies and procedures that could reduce cybersecurity underinvestment; (2) creating a reporting framework that could improve information sharing and improved cybersecurity defense investment and protection; and (3) providing public disclosure to inform Covered Entities' customers, counterparties, members, registrants, or users about the Covered Entities' cybersecurity efforts and experiences, thus potentially reducing information asymmetry.⁸⁷⁵ While the proposed rule has the potential to mitigate inefficiencies resulting from market imperfections, the scale of the overall effect would depend on numerous factors, including the state of existing of cybersecurity preparations,⁸⁷⁶ the degree to which the proposed provisions induce increases to these preparations, the effectiveness of additional preparations at reducing cybersecurity risks,⁸⁷⁷ the degree to which customers, counterparties, members, registrants, and users value additional cybersecurity preparations,⁸⁷⁸ the degree of information asymmetry and bargaining power between customers, counterparties, members, registrants, and users vis-à-vis Market Entities,⁸⁷⁹ the bargaining power of Market Entities vis-à-vis service providers,⁸⁸⁰ service

providers' willingness to provide bespoke contractual provisions to affected Market Entities,⁸⁸¹ the informational utility of the proposed disclosures, the scale of the negative externalities on the broader financial system,⁸⁸² the effectiveness of existing information sharing arrangements, and the informational utility of the required regulatory reports (as well as the Commission's ability to make use of them).⁸⁸³

However, since the proposed cybersecurity policies and procedures and related annual assessment are intended to prevent cybersecurity incidents at Market Entities that would otherwise cause financial loss and operational failure, compliance with the proposed rule likely would result in a safer environment to engage in securities transactions that protects the efficiency with which markets operate. Specifically, the proposed requirements are intended to protect the efficiency of securities market through the prevention of cybersecurity incidents that can adversely impact Market Entities and that, in turn, can interrupt the normal operations of U.S. securities markets and disrupt the efficient flow of information and capital.

The additional requirements applicable to Covered Entities (namely, the specific elements of the cybersecurity policies and procedures, the reporting to the Commission of any significant cybersecurity incident through Part I of proposed Form SCIR, and the disclosure of cybersecurity risks and significant cybersecurity incidents) would also allow for greater information sharing and would reduce the risk of underinvestment in cybersecurity across the securities industry. For example, confidential reporting to the Commission through Part I of proposed Form SCIR would provide regulators with the opportunity to promptly begin to assess the situation when a Covered Entity is experiencing a significant cybersecurity incident and begin to evaluate potential impacts on the market. In addition, public disclosures by Covered Entities through Part II of proposed Form SCIR and website postings would allow their customers, counterparties, members, registrants, and users to manage risk and choose with whom to do business, potentially allocating their resources to Covered Entities with greater cybersecurity

preparedness. In addition, the sharing of information through public disclosures could assist in the development and implementation of cybersecurity policies and procedures, particularly by smaller and less sophisticated Market Entities which likely have fewer resources to develop robust cybersecurity protocols. Such information may be useful to them in choosing one option over another, potentially allowing those smaller and less sophisticated Market Entities to develop their cybersecurity protection in the most cost-effective way possible.

Because the proposed rule would likely have differential effects on Market Entities along a number of dimensions, its overall effect on competition among Market Entities may be difficult to predict in certain instances. For example, smaller Market Entities, such as Non-Covered Broker-Dealers and certain transfer agents are likely to face disproportionately higher costs relative to revenues resulting from the proposed rule.⁸⁸⁴ With respect to broker-dealers, the Commission has endeavored to provide Non-Covered Broker-Dealers with a more limited and flexible set of requirements that better suits their business models and would therefore be less onerous. Still, a number of small broker-dealers would be subject to the proposed rule as Covered Entities, which could tilt the competitive playing field in favor of their larger Covered Broker-Dealer counterparts.⁸⁸⁵ In addition, all transfer agents would be Covered Entities under the proposed rule, regardless of their size, so the same concern is present.

On the other hand, if customers, counterparties, members, registrants, or users believe that the proposed rule effectively induces the appropriate level of cybersecurity effort among Market Entities, smaller Market Entities would likely benefit the most from these improved perceptions, as they would be thought to have sufficient cybersecurity policies and procedures in place compared to not having enough cybersecurity protections. Similar differential effects can occur within a particular group of Market Entities and service providers that are more (or less) focused on their cybersecurity.

With respect to competition among Covered Entities' service providers, the overall effect of the proposed rule and amendments is similarly ambiguous. It is likely that requiring affected Covered

⁸⁷⁵ See sections IV.B. and IV.D. of this release (discussing the broad economic considerations and benefits and costs of the proposals, respectively).

⁸⁷⁶ See section IV.C.1. of this release. Here, the Commission is concerned about the degree to which Market Entities' state of cybersecurity preparations diverge from socially optimal levels.

⁸⁷⁷ Formally, the marginal product of the proposed policies and procedures in the production of cybersecurity defenses.

⁸⁷⁸ Formally, customers', counterparties', members', registrants', and users' utility functions—specifically the marginal utilities of Covered Entities' and Non-Covered Broker-Dealers' cybersecurity policies and procedures.

⁸⁷⁹ In other words, the degree to which customers, counterparties, members, registrants, or users can affect the policies of Market Entities. Generally, the Commission expects that customers, counterparties, members, registrants, or users may be smaller than the affected Market Entity with which they conduct business and thus be subject to asymmetry and have limited ability to affect the policies of the Market Entity. However, that may not always be the case. For example, for customers of broker-dealers, the situation is likely to involve more heterogeneity, with some parties (e.g., small retail clients) wielding very little power over the broker-dealer's policies while others (e.g., large institutional investors) wielding considerable power.

⁸⁸⁰ In certain cases, a Covered Entity may determine that a competing service provider can be used as a bargaining chip in the renegotiation of existing service agreements, potentially imposing substantial contracting costs on the parties, which

would eventually be passed on to the Covered Entities' customers, counterparties, members, participants, or users.

⁸⁸¹ *Id.*

⁸⁸² See sections IV.D.2.a. and IV.D.2.b. of this release.

⁸⁸³ See section IV.D.3. of this release.

⁸⁸⁴ See section IV.B. of this release.

⁸⁸⁵ See section VI.C. of this release (noting that certain small broker-dealers would meet the definition of "covered entity" for purposes of the proposed rule).

Entities to request oversight of service providers' cybersecurity practices pursuant to a written contract would lead some service providers to cease offering services to affected Covered Entities.⁸⁸⁶ The additional regulation could serve as a barrier to entry to new service providers and could disproportionately affect would-be Market Entities.

In terms of capital formation, the proposed rule would have second-order effects, namely through a safer financial marketplace. As noted above, FSOC states that a destabilizing cybersecurity incident could potentially threaten the stability of the U.S. financial system by causing, among other things, a loss of confidence among a broad set of market participants, which could cause participants to question the safety or liquidity of their assets or transactions, and lead to significant withdrawal of assets or activity.⁸⁸⁷ The Market Entities covered by this rule play important roles in capital formation through the various services they provide.⁸⁸⁸ Due to their interconnected systems, a significant cybersecurity incident affecting Market Entities could have a cascading effect across the U.S. financial system with a significant impact on investor confidence, resulting in withdrawal of assets and impairment of capital formation.

The proposed rule provides the backbone for having sufficient cybersecurity measures in place to protect customer information, funds, and securities. Moreover, proposed provisions likely would lead to increased efficiency in the market, thus resulting in improved capital formation.⁸⁸⁹ With a more predictable investment environment due to improved cybersecurity implementation by Market Entities and service providers, capital formation through the demand for securities offerings will be less prone to interruptions.

As part of the analysis on competition, efficiency, and capital formation, the Commission requests comment from all parties, particularly the Market Entities that are affected by these proposed rule:

a. Do firms within the Covered Entity and Non-Covered Broker-Dealer groups

compare their cybersecurity safety measures among themselves or among firms of a particular type within a group (e.g., national securities exchanges only or transfer agents only)? Does one entity's level of cybersecurity protection incentivize competing entities to improve their cybersecurity policies and procedures? Is it possible that an entity with subpar cybersecurity protocols may be forced to exit the market, either because of business migrating to its competitors or because of the sheer number of cybersecurity incidents at that entity?

b. Would better cybersecurity policies and procedures, especially those that are reviewed and updated, provide more stability in the securities markets that encourages additional investment?

c. Would public disclosures of cybersecurity risks and significant cybersecurity incidents during the current or previous calendar year encourage investment in cybersecurity protections that later provide more stability in the market, thus encouraging capital formation?

d. Does the Commission's knowledge of cybersecurity incidents as well as of the policy and procedures at Market Entities lead to a calming effect on the market though oversight and compliance with the proposed rule, which would then foster greater capital formation?

F. Reasonable Alternatives

1. Alternatives to the Policies and Procedures Requirements of Proposed Rule 10

a. Require Only Disclosure of Cybersecurity Policies and Procedures Without Prescribing Specific Elements

Rather than requiring Covered Entities to adopt cybersecurity policies and procedures with specific enumerated elements, the Commission considered requiring Covered Entities to only provide explanations or summaries of their cybersecurity practices to their customers, counterparties, members, registrants, or users. In this alternative scenario, each Covered Entity would provide a disclosure containing a general overview of its existing cybersecurity policies and procedures, rather than be required to establish cybersecurity policies and procedures pursuant to the requirements of paragraph (b) of proposed Rule 10. Under this alternative, the general disclosure about the Covered Entity's cybersecurity policies and procedures would be publicly available to its customers, counterparties, members, registrants, and users, but it would not reveal specific details of the Covered

Entity's policies and procedures. Further, under this alternative, detailed and comprehensive information about the Covered Entity's cybersecurity risks and protocols—including the policies and procedures themselves—would remain internal to the Covered Entity. The only other organizations that would be able to review or examine this more detailed information would be the Commission, FINRA, the MSRB (to the extent applicable), and other regulators with authority to examine this information in the course of their oversight activities.

This alternative approach would create weaker incentives for Covered Entities to address potential underspending on cybersecurity measures, as it would rely, in part, on customers', counterparties', members', registrants', or users' (or third parties' providing analyses to those customers, counterparties, members, registrants, or users)⁸⁹⁰ ability to assess the effectiveness of Covered Entities' cybersecurity practices from the Covered Entities' public disclosures. Further, any benefits to be gained by requiring public disclosure of a Covered Entity's cybersecurity policies and procedures can also be realized through the proposed rule's public disclosure requirement. In particular, proposed Rule 10 would require each Covered Entity to provide a summary description of the cybersecurity risks that could materially affect its business and operations and how the Covered Entity assesses, prioritizes, and addresses those cybersecurity risks. In addition, each Covered Entity would need to disclose a summary description of each significant cybersecurity incident that occurred during the current or previous calendar year, if applicable. This disclosure would serve as another way for market participants to evaluate the Covered Entity's cybersecurity risks and vulnerabilities apart from the general disclosure of its cybersecurity risks. As mentioned above, this information could be useful to the Covered Entity's customers, counterparties, members, registrants, or users to manage their own cybersecurity risks and, to the extent they have choice, select a Covered Entity with whom to transact or otherwise conduct business.⁸⁹¹

Given the cybersecurity risks of disclosing detailed explanations of

⁸⁹⁰ See section IV.D.1.a. of this release.

⁸⁹¹ Furthermore, third-party financial service firms could conduct studies on cybersecurity preparedness at Market Entities, such as certain entities not being in line with industry practices or standards, which also could inform the choices of customers, counterparties, members, registrants, or users.

⁸⁸⁶ See section I.A.1. of this release.

⁸⁸⁷ See FSOC 2021 Annual Report.

⁸⁸⁸ See sections I.A.1. and II.A.1. of this release.

⁸⁸⁹ The proposed provisions do not implicate channels typically associated with capital formation (e.g., taxation policy, financial innovation, capital controls, intellectual property, rule-of-law, and diversification). Thus, the proposed rule are likely to have only indirect, second order effects on capital formation arising from any improvements to economic efficiency. Qualitatively, these effects are expected to be small.

cybersecurity practices (which would necessarily be disclosed if the Covered Entity would be required to disclose its existing cybersecurity policies and procedures),⁸⁹² it is likely that requiring such disclosure would result in the Covered Entity including only general language in its disclosure and providing few, if any, specific details that could be used by threat actors to take advantage of weak links in a Covered Entity's cybersecurity preparedness. Consequently, this alternative "disclosure-only" regime for cybersecurity policies and procedures would be unlikely to provide enough information and detail to differentiate between one Covered Entity's cybersecurity policies and procedures from another's policies and procedures, thus maintaining information asymmetry between the Covered Entity and other market participants. If information asymmetry was maintained, it is unlikely that meaningful change could be effected in the Covered Entities' cybersecurity practices through market pressure or Commission oversight over the Covered Entity's policies and procedures.⁸⁹³ Furthermore, not requiring specific enumerated elements in cybersecurity policies and procedures would likely result in less uniform cybersecurity preparedness across Covered Entities, leaving market participants with inconsistent information about the robustness of Covered Entities' cybersecurity practices. However, if Market Entities believed that providing more detailed information would give them a competitive advantage, they would do so.

On the other hand, the costs associated with this alternative likely would be minimal relative to those associated with the proposed requirements regarding written policies and procedures, as Covered Entities would be unlikely to face pressure to adjust their existing cybersecurity policies and procedures as long as they do not experience any significant cybersecurity incidents. However, if a Covered Entity does experience a significant cybersecurity incident, it may force the Covered Entity to revise its existing cybersecurity policies and procedures and consequently revise its disclosures to other market participants concerning its cybersecurity policies and procedures. It is also conceivable that being required to make public

⁸⁹² See section IV.D.2.b. of this release (discussing tradeoffs of cybersecurity disclosure).

⁸⁹³ Here, changes in cybersecurity practices would depend entirely on market discipline exerted by relatively uninformed market participants.

disclosures regarding its cybersecurity policies and procedures or undergoing third-party market analyses that aggregate these types of disclosures (and may focus on, for example, the Covered Entity's lack of conformity with industry practices and standards) may provide the impetus for a Covered Entity to make its cybersecurity policies and procedures more robust.

b. Limiting the Scope of the Proposed Cybersecurity Policies and Procedures With Respect to Third-Party Service Providers

The Commission also considered limiting the scope of the proposed requirement that the Covered Entity's policies and procedures require oversight of service providers that receive, maintain, or process the Covered Entity's information, or are otherwise permitted to access the Covered Entity's information systems and the information residing on those systems, pursuant to a written contract between the Covered Entity and the service provider.⁸⁹⁴ Specifically, the Commission considered narrowing the scope of service providers in the enumerated categories discussed above⁸⁹⁵ and requiring a periodic review and assessment of the pared-down list of service providers' cybersecurity policies and procedures rather than apply the Service Provider Oversight requirement to each service provider that receives, maintains, or processes the Covered Entity's information, or is otherwise permitted to access the Covered Entity's information systems and the information residing on those systems. The types of service providers that would still be covered by the written contract requirement would be those that provide cybersecurity related-services as well as business-critical services that are necessary for a Covered Entity to operate its core functions. The Commission further considered requiring service providers that receive, maintain, or process the Covered Entity's information, or are otherwise permitted to access the Covered Entity's information systems and the information residing on those systems to provide security certifications in lieu of the written contract requirement.

Narrowing the scope of the types of service providers affected by the proposal could lower costs for Covered Entities, especially smaller Covered Entities that rely on generic contracts

⁸⁹⁴ See paragraph (b)(1)(iii)(B) of proposed Rule 10 (setting forth the Service Provider Oversight Requirement).

⁸⁹⁵ See section IV.C.2.h. of this release.

with service providers (because they have less negotiating power with their service providers) and would have difficulty effecting changes in contractual terms with such service providers.⁸⁹⁶ However, in the current technological context in which businesses increasingly rely on third-party "cloud services" that effectively place business data out of the business' immediate control, the cybersecurity risk exposure of Covered Entities is unlikely to be limited to (or even concentrated in) certain named service providers. Narrowing the scope of service providers likely would lead to lower costs only insofar as it reduces effectiveness of the regulation. A related basis to reject this alternative is the signaling effect that it sends to threat actors. By excluding certain categories of service providers, the Commission could be providing information to threat actors about which service providers would be easiest to attack, as that universe of excluded vendors may have relatively inferior policies and procedures than vendors that are covered by the proposed rule.

Alternatively, maintaining the proposed scope but only requiring a standard, recognized, certification in lieu of a written contract could also lead to cost savings for Covered Entities, particularly if the certification is completed in-house or if a particular entity has many service contracts with different third parties that specify they are in compliance with the certification.⁸⁹⁷ However, the Commission preliminary believes that it would be difficult to prescribe a set of characteristics for such a "standard" certification that would sufficiently address the varied types of Covered Entities and their respective service providers.⁸⁹⁸ Another difficulty may be that if a single third-party entity is used for the certification, that entity would have to be well-versed in all contracted services in order to accurately assess them for compliance. In contrast, individualized contracts with each

⁸⁹⁶ See section IV.D.1.b. of this release (discussing service providers).

⁸⁹⁷ Service providers may currently be providing certifications as part of a registrant's policies and procedures. See also section II.B.1.g. of this release (seeking comment on alternative approaches to the Service Provider Oversight Requirement, including whether this cybersecurity risk could be addressed through policies and procedures to obtain written assurances or certifications from service providers that the service provider manages cybersecurity risk in a manner that would be consistent with how the Covered Entity would need to manage this risk under paragraph (b) of proposed Rule 10).

⁸⁹⁸ See section IV.C.3. of this release (discussing the variety of affected registrants); see also section IV.F.1. of this release (discussing the limitations of uniform prescriptive requirements).

service provider likely would ensure better compliance with the intent of the proposed rule as those third-party providers specialize in the services that they offer.

c. Require Specific Standardized Elements for Addressing Cybersecurity Risks of Covered Entities

The Commission considered including more standardized elements in that would need to be included in a Covered Entity's cybersecurity policies and procedures. For example, Covered Entities could be required to implement particular controls (*e.g.*, specific encryption protocols, network architecture, or authentication procedures) that are designed to address each general element of the required cybersecurity policies and procedures. Given the considerable diversity in the size, focus, and technical sophistication of affected Covered Entities,⁸⁹⁹ any specific requirements likely would result in some Covered Entities needing to substantially alter their cybersecurity policies and procedures.

The potential benefit of such an approach would be to provide assurance that Covered Entities have implemented certain specific cybersecurity practices. But this approach would also entail considerably higher costs, as many Covered Entities would need to adjust their existing practices to something else that is more costly than potential alternatives that could provide the same outcome level of protection. In addition, considering the variety of Covered Entities registered with the Commission, it would be exceedingly difficult for the Commission to devise specific requirements that are appropriately suited for all Covered Entities: a uniform set of requirements would certainly be both over- and under-inclusive, while providing varied requirements based on the circumstances of each Covered Entity would be complex and impractical. For example, standardized requirements that ensure reasonably designed cybersecurity policies and procedures for the largest, most sophisticated and active Covered Entities would likely be overly burdensome for smaller and less sophisticated Covered Entities with more limited cybersecurity risk exposures. Conversely, if these standardized requirements were tailored to smaller Covered Entities with more limited operations or cybersecurity risks, such requirements likely would be inadequate in addressing larger Covered Entities' cybersecurity risks. As a result, instituting blanket requirements likely

would not provide the most efficient and cost-effective way of instituting appropriate cybersecurity policies and procedures.

An important cost associated with this approach is the burden and complexity of prescribing detailed technical requirements tailored to the broad variety of Covered Entities that would be subject to proposed Rule 10. More broadly, imposing standardized requirements would effectively place the Commission in the role of dictating details related to the information technology practices of Covered Entities without the benefit of the Covered Entities' knowledge of their own particular circumstances. Moreover, given the complex and constantly evolving cybersecurity landscape, detailed regulatory requirements for cybersecurity practices would likely limit Covered Entities' ability to adapt quickly to changes in the cybersecurity landscape.⁹⁰⁰

d. Require Audits of Internal Controls Regarding Cybersecurity

Instead of requiring all Market Entities to establish, maintain, and enforce cybersecurity policies and procedures, the Commission considered requiring these entities to obtain audits of the effectiveness of their existing cybersecurity controls—for example, obtaining third-party audits with respect to their cybersecurity practices. This approach would not require Market Entities to establish, maintain, and enforce written policies and procedures that are reasonably designed to address their cybersecurity risks as proposed, but instead would require Market Entities to engage an independent, qualified third party to assess their cybersecurity controls and prepare a report describing its assessment and any potential deficiencies.

Under this alternative, an independent third party (*e.g.*, an auditing firm) would certify to the effectiveness of the Market Entities' cybersecurity practices. If the firms providing such certifications have sufficient reputational motives to issue credible assessment,⁹⁰¹ and if the scope of such certifications is not overly

⁸⁹⁹ If as in the previous example, the Commission were to require Covered Entities to adopt a specific encryption algorithm, future discovery of vulnerabilities in that algorithm would prevent registrants from fully mitigating the vulnerability (*i.e.*, switching to improved algorithms) in the absence of Commission action.

⁹⁰¹ This would be the case if there was sufficient market pressure or regulatory requirements to obtain certification from "reputable" third-parties with business models premised on operating as a going-concern and maintaining a reputation for honesty.

circumscribed,⁹⁰² it is likely that Market Entities' cybersecurity practices would end up being more robust under this alternative than under the current proposal. By providing certification of a Market Entities' cybersecurity practices, a firm would—in effect—be lending its reputation to the Market Entity. Because "lenders" are naturally most sensitive to downside risks (here, loss of reputation, lawsuits, damages, and regulatory enforcement actions), one would expect them to avoid "lending" to Market Entities with cybersecurity practices whose effectiveness is questionable.⁹⁰³

While certification by industry-approved third parties could lead to more robust cybersecurity practices, the costs of such an approach would likely be considerably higher. Because of the aforementioned sensitivity to downside risk, firms would likely be hesitant to provide cybersecurity certifications without a thorough understanding of a Market Entity's systems and practices. In many cases, developing such an understanding would involve considerable effort particularly for certain larger and more sophisticated Covered Entities.⁹⁰⁴ In addition, there may be a need for a consensus as to what protocols constitute industry standards in which certifying third parties would need to stay proficient. Finally, while such a scenario is somewhat similar to the Service Provider Oversight Requirement, this alternative does not allow for immediate repercussions or remediation if the third-party finds deficiencies in the Covered Entity's cybersecurity policies and procedures. The Commission would need to have a copy of the report and audit the Market Entity to ensure that Market Entity subsequently resolved the problem(s). This leads to an inefficient method of implementing reasonably

⁹⁰² In this alternative, it is assumed that certification would not be limited to only evaluating whether a Market Entity's stated policies and procedures are reasonably designed, but rather also would include an assessment of whether the policies and procedures are actually implemented in an effective manner.

⁹⁰³ Under the proposal it is the Market Entity itself that effectively "certifies" its own cybersecurity policies and procedures. Like the third-party auditor, the Market Entity faces downside risks from "certifying" inadequate cybersecurity practices (*i.e.*, Commission enforcement actions). However, unlike the auditor, the Market Entity also realizes the potential up-side: cost savings through reduced cybersecurity expenditures.

⁹⁰⁴ It would be difficult for an auditor to provide a credible assessment of the effectiveness of the Market Entity's cybersecurity practices without first understanding the myriad of systems involved and how those practices are implemented. Presumably, a Market Entity would not bear these costs as it is likely to possess such an understanding.

⁸⁹⁹ See section IV.C.3. of this release.

designed cybersecurity policies and procedures.

e. Bifurcate Non-Broker-Dealer Market Entities Into Covered Entities and Non-Covered Entities

The Commission considered bifurcating other categories of Market Entities into Covered Entities and Non-Covered Entities (in addition to broker-dealers) based on certain characteristics of the firm such that the Non-Covered Entities would not be required to include certain elements in their cybersecurity risk management policies and procedures. For example, the Commission considered defining as Non-Covered Entities Market Entities with assets below a certain threshold or with only a limited number of customers, counterparties, members, registrants, or users. This approach also could be scaled based on a Covered Entity's size, business, or another criterion, similar to the proposed distinction between Covered Broker-Dealers and Non-Covered Broker-Dealers. However, as discussed above, cybersecurity risks are likely to be unique to each Covered Entity primarily because Covered Entities vary drastically based on their size, business, and the services they provide. It would be difficult come up with one characteristic that is common to all Covered Entities such that each of them can be both broken out into separate groups. For example, it would be difficult to differentiate between transfer agents the same way one could distinguish between large and small clearing agencies or even harder, national securities associations. The only effective way to differentiate firms with a given Covered Entity category is to choose a characteristic that is sensible for the type of Covered Entity.⁹⁰⁵

Finally, as discussed earlier, in determining which Market Entities should be Covered Entities and which should be Non-Covered Entities, the Commission considered: (1) how the category of Market Entity supports the fair, orderly, and efficient operation of the U.S. securities markets and the consequences if that type of Market Entity's critical functions were disrupted or degraded by a significant cybersecurity incident; (2) the harm that could befall investors, including retail

investors, if that category of Market Entity's functions were disrupted or degraded by a significant cybersecurity incident; (3) the extent to which the category of Market Entity poses cybersecurity risk to other Market Entities through information system connections, including the number of connections; (4) the extent to which the category of Market Entity would be an attractive target for threat actors; and (5) the personal, confidential, and proprietary business information about the category of Market Entity and other persons (e.g., investors) stored on the Market Entity's information systems and the harm that could be caused if that information were accessed or used by threat actors through a cybersecurity breach.⁹⁰⁶ However, the Commission seeks comment on this topic, particularly if certain proposed Covered Entities should be Non-Covered Entities with attendant reduced requirements.⁹⁰⁷

f. Administration and Oversight of Cybersecurity Policies and Procedures of Covered Entities

The Commission considered various alternative requirements with respect to administration and oversight of Covered Entities' cybersecurity policies and procedures, such as requiring them to designate a CISO (or another individual that serves in a similar capacity) or requiring the boards of directors (to the extent applicable), to oversee directly a Covered Entity's cybersecurity policies and procedures. There is a broad spectrum of potential approaches to this alternative, ranging from the largely nominal (e.g., requiring Covered Entities simply to designate someone to be a CISO) to the stringent (e.g., requiring a highly-qualified CISO to attest to the effectiveness of the Covered Entities' policies).

Stringent requirements, such as requiring an attestation from a highly qualified CISO as to the effectiveness of a Covered Entity's cybersecurity practices in specific enumerated areas, could be quite effective. Expert practitioners in cybersecurity are in high demand and command high salaries.⁹⁰⁸ Thus, such an approach would impose substantial ongoing costs on Covered Entities who do not already

have appropriately qualified individuals on staff. This burden would be disproportionately borne by smaller Covered Entities, such as small Covered Broker-Dealers or small transfer agents, for whom keeping a dedicated CISO on staff would be cost prohibitive. Allowing Covered Entities to employ part-time CISOs would mitigate this cost burden, but such requirements would likely create a *de facto* audit regime. Such an audit regime would certainly be more effective if explicitly designed to function as such.⁹⁰⁹

2. Alternatives to the Requirements of Proposed Form SCIR and Related Notification and Disclosure Requirements of Proposed Rule 10

a. Public Disclosure of Part I of Proposed Form SCIR

The Commission considered requiring the public disclosure of Part I of proposed Form SCIR. Making Part I of proposed Form SCIR filings public would increase the knowledge of a Covered Entity's customer, counterparties, members, registrants, or users about significant cybersecurity incidents impacting the Covered Entity and thus improve their ability to draw inferences about a Covered Entity's level of cybersecurity preparations. At the same time, doing so could assist would-be threat actors, who may gain additional insight into the vulnerabilities of a Covered Entity's system. As discussed above, releasing too much detail about a significant cybersecurity incident could further compromise cybersecurity of the victim, especially in the short term.⁹¹⁰ Given these risks, requiring public disclosure of Part I of proposed Form SCIR filings would likely have the effect of incentivizing Covered Entities to significantly reduce the detail provided in these filings. As a result, the information set of customers, counterparties, members, registrants, users, and would-be attackers would remain largely unchanged (*vis-à-vis* the proposal), while the ability of the Commission to facilitate information sharing and to coordinate responses aimed at reducing overall risks to the financial system would be diminished.

⁹⁰⁶ See section II.A.1. of this release.

⁹⁰⁷ See section II.A.10. of this release.

⁹⁰⁸ A recent survey reports CISO median total compensation of \$668,903 for CISOs at companies with revenues of \$5 billion or less. See Matt Aiello and Scott Thompson, *2020 North American Chief Information Security Officer (CISO) Compensation Survey* (2020), available at <https://www.heidrick.com/-/media/heidrickcom/publications-and-reports/2020-north-american-chief-information-security-officer-ciso-compensation-survey.pdf>.

⁹⁰⁹ In designing an effective audit regime, aligning incentives of auditors to provide credible assessments is a central concern. In the context of audit regimes, barriers to entry and the reputation motives of auditing firms helps align incentives. It would be considerably more difficult to obtain similar incentive alignment with itinerant part-time CISOs. See section IV.F.1.e. of this release (describing the audit regime alternative).

⁹¹⁰ See section IV.B. of this release.

⁹⁰⁵ For additional detail on the importance of each of the proposed Covered Entity's role in the U.S. securities markets, see section I.A.2. of this release (discussing critical operations of each Market Entity). See also section II.A.1. of this release (discussing why it would not be appropriate to exclude small transfer agents and certain small broker-dealers from the definition of Covered Entity).

b. Modify the Standard Identifier Requirements for Proposed Form SCIR

In addition to proposing to require Covered Entities to identify themselves on Parts I and II of proposed Form SCIR with CIK numbers, the proposed rule requests that Covered Entities with a UIC—such as an LEI—include that identifier, if available, on both parts of proposed Form SCIR. Those Covered Entities that do not have a UIC may file either part of proposed Form SCIR without a UIC; they are not required to obtain a UIC prior to filing proposed Form SCIR.

The Commission considered modifying the requirement that Covered Entities identify themselves on proposed Form SCIR with CIK numbers and UICs (if they have UICs). For example, the Commission could eliminate the requirement that Covered Entities identify themselves on the forms with a standard identifier, or the Commission could allow Covered Entities to select a different standard identifier (or identifiers) other than CIK numbers or UICs (if available). Alternatively, the Commission could require the use of only one proposed standard identifier—either CIK numbers, UICs (which would require Covered Entities to obtain a UIC—such as an LEI—if they do not have one),⁹¹¹ or some other standard identifier. While CIK numbers are necessary to file in EDGAR and, as discussed earlier, the Commission anticipates that significant benefits would flow from requiring Parts I and II of proposed Form SCIR to be filed centrally in EDGAR using a structured data language. Accordingly, the Commission's proposal would require Covered Entities to identify themselves on the forms with CIK numbers. One limitation of CIK numbers, however, is that they are a Commission-specific identifier, which limits their utility for aggregating, analyzing, and comparing financial market data involving market participants that are not Commission registrants and EDGAR filers.

While the proposed rule does not require the inclusion of UICs on

⁹¹¹ Further, the Commission recognizes that some Covered Entities may not have LEIs, which means that those Covered Entities would have to register with a Local Operating Unit ("LOU") of the Global LEI System and pay fees initially and annually to obtain and renew the LEI. See LEIROC, *How To Obtain an LEI*, available at <https://www.leiroc.org/lei/how.htm>. A list of LOUs accredited by GLEIF can be found at <https://www.gleif.org/en/about-lei/get-an-lei-find-lei-issuing-organizations>. Currently, U.S. entities may obtain an LEI for a one-time fee of \$65 and an annual renewal fee of \$50. See Bloomberg Finance L.P., *Fees, Payments & Taxes* (2022), available at <https://lei.bloomberg.com/docs/faq#what-fees-are-involved>.

proposed Form SCIR for those Covered Entities that do not have a UIC, the Commission notes that the use of UICs would be beneficial because the LEI, as a Commission-approved UIC, is a low-cost, globally-utilized financial institution identifier that is available even to firms that are not EDGAR filers or Commission registrants. For that reason, the Commission considered proposing to require that every Covered Entity that would need to file Part I or II of proposed Form SCIR to identify themselves with a UIC. There is benefit to including a UIC identifier on proposed Form SCIR. Among the alternative entity identifier policy choices considered, requiring Covered Entities to identify themselves on Parts I and II of proposed Form SCIR with a UIC is superior to other alternatives, such as not requiring an entity identifier on proposed Form SCIR or requiring only CIK numbers. Specifically, the mandatory inclusion of a UIC on (Parts I and II of) proposed Form SCIR could allow for greater inter-governmental and international coordination of responses to cybersecurity incidents affecting financial institutions globally because the LEI is a globally-utilized digital identifier that is not specific to the Commission. Other regulatory entities and bodies, including the CFTC, Alberta Securities Commission (Canada), European Markets and Securities Authority, and Monetary Authority of Singapore, require the use of an LEI.⁹¹² Another benefit of the LEI is that the legal entity's identity is verified by a third party upon issuance of the LEI and upon annual renewal of the LEI. Additionally, LEIs contain "Level 2" information about the linkages between the entities being identified and their various parents and subsidiaries, which is particularly beneficial considering that some financial firms and Commission registrants have complex, interlocking relationships with affiliates and subsidiaries that can be different types of Commission-regulated firms.

A UIC requirement for Parts I and II of proposed Form SCIR would not impose additional costs on those Covered Entities that already have an LEI. For those Covered Entities that do not have an LEI, they would need to obtain one before filing either part of proposed Form SCIR. An LEI can be obtained for a \$65 initial cost and a \$50 per year renewal cost.⁹¹³ There also are administrative costs associated with

⁹¹² In addition, the FSB has stated that "[t]he use of the LEI in regulatory reporting can significantly improve the ability of the public sector to understand and identify the build-up of risk across multiple jurisdictions and across complex global financial processes." FSB Peer Review Report.

filling out the paperwork to obtain the LEI as well as to process payments for the initial issuance of an LEI and its maintenance. The Commission expects that this cost would be small relative to the benefit that could be reaped if a significant cybersecurity incident were to occur that impacted financial institutions across multiple domestic and international jurisdictions.

After considering the benefits and costs of requiring the LEI as an identifier for all Covered Entities via a UIC requirement, the Commission is proposing to require Covered Entities to identify themselves with a UIC on proposed Form SCIR only if they already have a UIC so as to minimize the burden on Covered Entities and because multiple other Commission disclosure forms also only require registrants to identify themselves with UICs if they already have UICs.⁹¹⁴ In conclusion, requiring Covered Entities to identify themselves on both parts of proposed Form SCIR with a CIK and with a UIC (*i.e.*, the LEI) if they already have a UIC is consistent with the existing regulatory framework.

Although CIK numbers and UICs (such as in the form of LEIs) are the primary two entity standard identifiers used in Commission regulations, the Commission could instead propose to require Covered Entities to identify themselves with an alternative entity identifier other than CIK numbers and UICs for the proposed rule. For the reasons stated above, there are benefits from the use of CIK numbers (*i.e.*, CIK numbers enable EDGAR filing, which facilitates aggregation and analysis of the information) and LEIs (*i.e.*, the LEI is an affordable, international standard identifier that facilitates information sharing). Accordingly, the Commission decided against proposing to require the use of another standard entity identifier for the purposes of this proposal.

c. Require Only One Location for the Public Disclosures

Rather than requiring Covered Entities to publicly disclose their cybersecurity risks and significant cybersecurity incidents during the current or previous calendar year both on their websites and also file that information centrally on Part II of proposed Form SCIR in EDGAR, the Commission considered requiring that Covered Entities provide the public disclosures on their websites only.

Requiring Covered Entities to place the cybersecurity disclosures only on their websites could provide modest,

⁹¹⁴ Covered Entities that do not have an LEI may obtain one if they so choose.

incremental reductions in the burdens associated with providing those disclosures both on Covered Entity websites and through filing Part II of proposed Form SCIR with the Commission. Additionally, the websites of Covered Entities might be the natural place for their customers, counterparties, members, registrants, or users to look for information about the Covered Entity. Alternatively, requiring Covered Entities to place their cybersecurity disclosures (Part II of Form SCIR) only in EDGAR in a structured data language also could provide modest, incremental reductions in the burdens associated with placing those disclosures on their websites.

Accordingly, the Commission is proposing to require Covered Entities to provide the information both on their websites and in EDGAR on Part II of proposed Form SCIR.⁹¹⁵ Publication on Covered Entity websites is advantageous because that is where many Covered Entities' customers, counterparties, members, registrants, or users will look for information about their financial intermediaries. Centralized filing of structured public disclosures of cybersecurity risks and significant cybersecurity incidents during the current or previous calendar year in EDGAR by Covered Entities would enable customers, counterparties, members, registrants, and users, as well as financial analysts—and even the Covered Entities themselves—to more efficiently discern broad trends in cybersecurity risks and incidents, which would enable Covered Entities and other market participants to more efficiently determine if they need to modify, change, or upgrade their cybersecurity defense measures in light of those trends. Accordingly, the Commission is proposing to require Covered Entities to publish the required cybersecurity disclosures on their websites and provide the information in Part II of proposed Form SCIR, which would be filed in EDGAR using a custom XML.

d. Modify the Location of the EDGAR-Filed Public Cybersecurity Disclosures for Some Covered Entities

Rather than requiring Covered Entities to provide the public cybersecurity disclosures in EDGAR using Part II of proposed Form SCIR, the Commission considered requiring Covered Entities that currently are required to file forms in EDGAR to provide the disclosures in structured attachments to existing EDGAR-filed forms. Currently, only SBS

Entities and transfer agents are required to file EDGAR forms. SBSDs and MSBSPs must file in EDGAR registration applications on Form SBSE, SBSE-A, or SBSE-BD, amendments to those Forms if the information in them is or has become inaccurate, and certifications on Form SBSE-C.⁹¹⁶ As discussed above, Commission regulations require SBSDRs to file Form SDR in EDGAR but the Commission temporarily relieved SBSDRs of the EDGAR-filing requirement. Transfer agents file Forms TA-1, TA-2, and TA-W in EDGAR in a custom XML.⁹¹⁷ The Commission considered permitting those types of Covered Entities that are not currently subject to an EDGAR-filing requirement to file the cybersecurity disclosures only on their individual firm websites (without needing to also file the disclosures in EDGAR). Therefore, rather than requiring all Covered Entities to file the cybersecurity disclosures using Part II of proposed Form SCIR, the Commission could require Covered Entities that are SBS Entities or transfer agents to provide the same information as structured attachments to Form SBSE (for SBS Entities) and Form TA-1 (for transfer agents). Likewise, the Commission could require SBSDRs to file the cybersecurity disclosures as attachments to Form SDR once the Commission temporary relief from the EDGAR-filing requirement expires.

Requiring all Covered Entities to provide the disclosures on a single, uniform form would likely be simpler (because the information would be in one location)—and thereby more efficient—for the Commission, Covered Entities, and others who might seek the information in the cybersecurity disclosures (including Covered Entities' users, members, customers, or counterparties) than putting the cybersecurity disclosures in attachments on disparate forms and (for those firms not subject to EDGAR-filing requirements) on individual Covered Entity websites.

e. Modify the Structured Data Requirement for the Public Cybersecurity Disclosures

Rather than requiring Covered Entities to file Part II of proposed Form SCIR in EDGAR using a custom XML, the Commission could either eliminate the structured data language requirement for some or all Covered Entities or

require the use of a different structured data language, such as Inline XBRL.⁹¹⁸ For example, the Commission could eliminate the requirement that Covered Entities file Part II of proposed Form SCIR in a custom XML or in any structured data language. By eliminating the structured data requirement, the Commission would allow Covered Entities to submit the new cybersecurity disclosures in unstructured HTML or ASCII, thereby avoiding the need to put the information for Part II of proposed Form SCIR into a fillable web form that EDGAR would use to generate the custom XML filing, or instead file Part II of proposed Form SCIR directly in custom XML using the XML schema for proposed Form SCIR, as published on the Commission's website.

Another option is that the Commission could remove the structured data filing requirement for some subset of Covered Entities. For example, the Commission could instead require only certain types of Covered Entities, such as national securities exchanges or SBS Entities, to file Part II of proposed Form SCIR in a custom XML. Alternatively, the Commission could require the use of a structured data language only for those Covered Entities that exceeded some threshold, be it assets or trading volumes, depending on the type of Covered Entity in question. Eliminating the requirement that Part II of proposed Form SCIR be filed in a structured data language, however, would reduce the benefits of the proposed rule because the use of a structured data language would make the information contained in Part II of proposed Form SCIR easier and more efficient for Commission staff—as well as the Covered Entity's customers, counterparties, members, registrants, or users—to assemble, review, and analyze. Financial analysts at third-party information providers also could use the public disclosures to produce analyses and reports that market participants may find useful.

The Commission could require Covered Entities to file Part II of proposed Form SCIR in Inline XBRL rather than in custom XML on the grounds that Inline XBRL is an internationally-recognized freely available industry standard for reporting business-related information and a data

⁹¹⁸ XBRL is a structured data language that is specifically designed to handle business-related information, including financial information, entity descriptions, corporate actions, ledgers and sub-ledgers, and other summary and ledger-level information. By comparison, Inline XBRL is a structured data language that embeds XBRL data directly into an HTML document, enabling a single document to provide both human-readable and structured machine-readable data.

⁹¹⁵ The Commission is seeking comment on this topic. See section II.B.3.c. of this release.

⁹¹⁶ See Instruction A.2 to Form SBSE, Instruction A.2 to Form SBSE-A, Instruction A.3 to Form SBSE-BD, and Instruction A.2 to Form SBSE-C.

⁹¹⁷ See Commission, Electronic Filing of Transfer Agent Forms (Nov. 14, 2007), available at <https://www.sec.gov/info/edgar/ednews/ta-filing.htm>.

language that allows EDGAR filers to prepare single documents that are both human-readable and machine-readable, particularly in connection with forms containing publicly-available registrant financial statements. The Commission believes that the use of a form-specific XML would be appropriate here given the relative simplicity of Part II of proposed Form SCIR disclosures and the ability for EDGAR to provide fillable web forms for entities to comply with their custom XML requirements, leading to a lower burden of compliance for Covered Entities without Inline XBRL experience.

3. General Request for Comment

The Commission requests comment on the benefits and costs associated the alternatives outlined above.

V. Paperwork Reduction Act Analysis

Certain provisions of the proposed rule, form, and rule amendments in this release would contain a new “collection of information” within the meaning of the Paperwork Reduction Act of 1995 (“PRA”).⁹¹⁹ The Commission is submitting the proposed rule amendments and proposed new rules to the Office of Management and Budget (“OMB”) for review and approval in accordance with the PRA and its implementing regulations.⁹²⁰ An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a currently valid OMB control number.⁹²¹ The titles for the collections of information are:

- (1) Rule 10;
- (2) Form SCIR;
- (3) Rule 17a-4—Records to be preserved by certain exchange members, brokers and dealers (OMB control number 3235-0279);
- (4) Rule 17ad-7—Record retention (OMB control number 3235-0291);
- (5) Rule 18a-6—Records to be preserved by certain security-based swap dealers and major security-based swap participants (OMB control number 3235-0751); and
- (6) Rule 3a71-6—Substituted Compliance for Foreign Security-Based Swap Entities (OMB control number 3235-0715).

The burden estimates contained in this section do not include any other possible costs or economic effects beyond the burdens required to be calculated for PRA purposes.

A. Summary of Collections of Information

1. Proposed Rule 10

Proposed Rule 10 would require all Market Entities (Covered Entities and non-Covered Entities) to establish, maintain, and enforce written policies and procedures that are reasonably designed to address their cybersecurity risks.⁹²² All Market Entities also, at least annually, would be required to review and assess the design and effectiveness of their cybersecurity policies and procedures, including whether the policies and procedures reflect changes in cybersecurity risk over the time period covered by the review.⁹²³ They also would be required to prepare a report (in the case of Covered Entities) and a record (in the case of non-Covered Entities) with respect to the annual review.⁹²⁴ Finally, all Market Entities would need to give the Commission immediate written electronic notice of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring.⁹²⁵

Market Entities that meet the definition of “covered entity” would be subject to certain additional requirements under proposed Rule 10.⁹²⁶ First, their cybersecurity risk management policies and procedures would need to include the following elements:

- Periodic assessments of cybersecurity risks associated with the Covered Entity’s information systems and written documentation of the risk assessments;
- Controls designed to minimize user-related risks and prevent unauthorized access to the Covered Entity’s information systems;
- Measures designed to monitor the Covered Entity’s information systems

⁹²² See paragraphs (b) through (d) of proposed Rule 10 (setting forth the requirements for Market Entities that meet the definition of “covered entity”); paragraph (e)(1) of proposed Rule 10. See also Sections II.B.1 and II.C. of this release (discussing these proposed requirements in more detail).

⁹²³ See paragraph (b)(2) of proposed Rule 10; paragraph (e)(1) of proposed Rule 10. See also Sections II.B.1.f. and II.C. of this release (discussing these proposed requirements in more detail).

⁹²⁴ See paragraph (b)(2) of proposed Rule 10; paragraph (e)(1) of proposed Rule 10. See also Sections II.B.1.f. and II.C. of this release (discussing these proposed requirements in more detail).

⁹²⁵ See paragraph (c)(1) of proposed Rule 10; paragraph (e)(2) of proposed Rule 10. See also sections II.B.2.a. and II.C. of this release (discussing these proposed requirements in more detail).

⁹²⁶ See paragraph (b) through (d) of proposed Rule 10 (setting forth the requirements for Market Entities that meet the definition of “covered entity”); paragraph (e) of proposed Rule 10 (setting forth the requirements for Market Entities that do not meet the definition of “covered entity”).

and protect the Covered Entity’s information from unauthorized access or use, and oversight of service providers that receive, maintain, or process information, or are otherwise permitted to access the Covered Entity’s information systems;

- Measures to detect, mitigate, and remediate any cybersecurity threats and vulnerabilities with respect to the Covered Entity’s information systems; and
- Measures to detect, respond to, and recover from a cybersecurity incident and written documentation of any cybersecurity incident and the response to and recovery from the incident.⁹²⁷

Second, Covered Entities—in addition to providing the Commission with immediate written electronic notice of a significant cybersecurity incident—would need to report and update information about the significant cybersecurity incident by filing Part I of proposed Form SCIR with the Commission through the EDGAR system.⁹²⁸ The form would elicit information about the significant cybersecurity incident and the Covered Entity’s efforts to respond to, and recover from, the incident.

Third, Covered Entities would need to publicly disclose summary descriptions of their cybersecurity risks and the significant cybersecurity incidents they experienced during the current or previous calendar year on Part II of proposed Form SCIR.⁹²⁹ The form would need to be filed with the Commission through the EDGAR system and posted on the Covered Entity’s business internet website and, in the case of Covered Entities that are carrying or introducing broker-dealers, provided to customers at account opening and annually thereafter.

Covered Entities and Non-Covered Entities would need to preserve certain records relating to the requirements of proposed Rule 10 in accordance with amended or existing recordkeeping requirements applicable to them or, in the case of exempt clearing agencies,

⁹²⁷ See sections II.B.1.a. through II.B.1.e. of this release (discussing these proposed requirements in more detail). In the case of non-Covered Entities, as discussed in more detail below in Section II.C. of this release, the design of the cybersecurity risk management policies and procedures would need to take into account the size, business, and operations of the broker-dealer. See paragraph (e) of proposed Rule 10.

⁹²⁸ See sections II.B.2. and II.B.4. of this release (discussing these proposed requirements in more detail).

⁹²⁹ See sections II.B.3. and II.B.4. of this release (discussing these proposed requirements in more detail).

⁹¹⁹ See 44 U.S.C. 3501 *et seq.*

⁹²⁰ See 44 U.S.C. 3507; 5 CFR 1320.11.

⁹²¹ See 5 CFR 1320.11(l).

pursuant to conditions in relevant exemption orders.⁹³⁰

2. Form SCIR

Proposed Rule 10 would require Covered Entities to: (1) report and update information about a significant cybersecurity incident;⁹³¹ and (2) publicly disclose summary descriptions of their cybersecurity risks and the significant cybersecurity incidents they experienced during the current or previous calendar year.⁹³² Parts I and II of proposed Form SCIR would be used by Covered Entities, respectively, to report and update information about a significant cybersecurity incident and publicly disclose summary descriptions of their cybersecurity risks and the significant cybersecurity incidents they experienced during the current or previous calendar year.

3. Rules 17a-4, 17ad-7, 18a-6 and Clearing Agency Exemption Orders

Rules 17a-4, 17ad-7, and 18a-6—which apply to broker-dealers, transfer agents, and SBS Entities, respectively—would be amended to establish preservation and maintenance requirements for the written policies and procedures, annual reports, Parts I and II of proposed Form SCIR, and records required to be made pursuant to proposed Rule 10 (*i.e.*, the Rule 10 Records).⁹³³ The proposed amendments would specify that the Rule 10 Records must be retained for three years. In the case of the written policies and procedures to address cybersecurity risks, the record would need to be maintained until three years after the termination of the use of the policies and procedures. In addition, orders exempting certain clearing agencies from registering with the Commission would be amended to establish preservation and maintenance requirements for the Rule 10 Records that would apply to the exempt clearing agencies subject to those orders.⁹³⁴ The amendments to the orders would

⁹³⁰ See sections II.B.5. and II.C. of this release (discussing these proposed requirements in more detail).

⁹³¹ See sections II.B.2. and II.B.4. of this release (discussing these proposed requirements in more detail).

⁹³² See sections II.B.3. and II.B.4. of this release (discussing these proposed requirements in more detail).

⁹³³ See sections II.B.5. and II.C. of this release (discussing these proposed amendments in more detail). Rule 17a-4 sets forth record preservation and maintenance requirements for broker-dealers, Rule 17ad-7 sets forth record preservation and maintenance requirements for transfer agents, and Rule 18a-6 sets forth record preservation and maintenance requirements for SBS Entities.

⁹³⁴ See section II.B.5. of this release (discussing these proposed amendments in more detail).

provide that the records need to be retained for five years (consistent with Rules 13n-7 and 17a-1).⁹³⁵ In the case of the written policies and procedures to address cybersecurity risks, the record would need to be maintained until five years after the termination of the use of the policies and procedures.

4. Substituted Compliance (Rule 3a71-6)

Paragraph (d)(1) of Rule 3a71-6 would be amended to add proposed Rule 10 and Form SCIR to the list of Commission requirements eligible for a substituted compliance determination.⁹³⁶ If adopted, this amendment together with existing paragraph (d)(6) of Rule 3a71-6 would permit eligible SBS Entities to file an application requesting that the Commission make a determination that compliance with specified requirements under a foreign regulatory system may satisfy the requirements of proposed Rule 10, Form SCIR, and the related record preservation requirements. As provided by Exchange Act Rule 0-13,⁹³⁷ which the Commission adopted in 2014,⁹³⁸ applications for substituted compliance determinations must be accompanied by supporting documentation necessary for the Commission to make the determination, including information regarding applicable requirements established by the foreign financial regulatory authority or authorities, as well as the methods used by the foreign financial regulatory authority or authorities to monitor and enforce compliance; applications should cite to and discuss applicable precedent.⁹³⁹

⁹³⁵ For the reasons discussed in section II.B.5.a. of this release, the proposal would not amend Rules 13n-7 or 17a-1. As explained in that section of the release, the existing requirements of Rule 13n-7 (which applies to SBSDRs) and Rule 17a-1 (which applies to registered clearing agencies, the MSRB, national securities associations, and national securities exchanges) will require these Market Entities to retain the Rule 10 Records for five years and, in the case of the written policies and procedures, for five years after the termination of the use of the policies and procedures.

⁹³⁶ See section II.D. of this release (discussing these proposed amendments in more detail).

⁹³⁷ 17 CFR 240.0-13.

⁹³⁸ See SBS Entity Definitions Adopting Release, 79 FR at 47357-59.

⁹³⁹ See 17 CFR 240.0-13(e). In adopting Rule 0-13, the Commission noted that because Rule 0-13 was a procedural rule that did not provide any substituted compliance rights, “collections of information arising from substituted compliance requests, including associated control numbers, [would] be addressed in connection with any applicable substantive rulemakings that provide for substituted compliance.” See SBS Entity Definitions Adopting Release, 79 FR at 47366 n.778.

B. Proposed Use of Information

The proposed requirements to have written policies and procedures to address cybersecurity risks, to document risk assessments and significant cybersecurity incidents, to create a report or record of the annual review of the policies and procedures, to provide immediate notification and subsequent reporting of significant cybersecurity incidents, to publicly disclose summary descriptions of cybersecurity risks and significant cybersecurity incidents, and to preserve the written policies and procedures, reports, and records would constitute collection of information requirements under the PRA. Collectively, these collections of information are designed to address cybersecurity risk and the threat it poses to Market Entities and the U.S. securities markets.

Market Entities would use the written policies and procedures, the records required to be made pursuant to those policies and procedures, and the report or record of the annual review of the policies and procedures to address the specific cybersecurity risks to which they are exposed. The Commission could use the written policies and procedures, reports, and records to review Market Entities' compliance with proposed Rule 10.

Market Entities would use the immediate written electronic notifications to notify the Commission (and, in some cases, other regulators) about significant cybersecurity incidents they experience pursuant to proposed Rule 10. The Commission could use the immediate written electronic notification to promptly begin to assess the situation by, for example, when warranted, assessing the Market Entity's operating status and engaging in discussions with the Market Entity to understand better what steps it is taking to protect its customers, counterparties, members, registrants, or users.

Covered Entities would use Part I of proposed Form SCIR to report to the Commission (and, in some cases, other regulators) significant cybersecurity incidents they experienced pursuant to proposed Rule 10. The Commission could use the reports of significant cybersecurity incidents filed using Part I of proposed Form SCIR to understand better the nature and extent of a particular significant cybersecurity incident and the efficacy of the Covered Entity's response to mitigate the disruption and harm caused by the incident. The Commission staff could use the reports to focus on the Covered Entity's operating status and to facilitate their outreach to, and discussions with,

personnel at the Covered Entity who are addressing the significant cybersecurity incident. In addition, the reporting would provide the staff with a view into the Covered Entity’s understanding of the scope and impact of the significant cybersecurity incident. All of this information would be used by the Commission and its staff in assessing the significant cybersecurity incident impacting the Covered Entity. Further, the Commission would use the database of reports to assess the potential cybersecurity risks affecting U.S. securities markets more broadly. This information could be used to address future significant cybersecurity incidents. For example, these reports could assist the Commission in identifying patterns and trends across Covered Entities, including widespread cybersecurity incidents affecting multiple Covered Entities at the same time. Further, the reports could be used to evaluate the effectiveness of various approaches to respond to and recover from a significant cybersecurity incident.

Covered Entities would use Part II of proposed Form SCIR to publicly disclose summary descriptions of their

cybersecurity risks and the significant cybersecurity incidents they experienced during the current or previous calendar year pursuant to proposed Rule 10. These disclosures would be used to provide greater transparency to customers, counterparties, registrants, or members of the Covered Entity, or to users of its services, about the Covered Entity’s cybersecurity risk profile. This information could be used by these persons to manage their own cybersecurity risk and, to the extent they have choice, select a Covered Entity with whom to transact or otherwise conduct business. In addition, because the reports would be filed through EDGAR, Covered Entities’ customers, counterparties, members, registrants, or users would be able to run search queries to compare the disclosures of multiple Covered Entities. This would make it easier for Commission staff and others to assess the cybersecurity risk profiles of different types of Covered Entities and could facilitate trend analysis by members of the public of significant cybersecurity incidents.

Under the proposed amendment to Rule 3a71–6, the Commission would use the information collected to evaluate requests for substituted compliance with respect to proposed Rule 10, Form SCIR, and the related record preservation requirements applicable to SBS Entities. Consistent with Exchange Act Rule 0–13(h),⁹⁴⁰ the Commission would publish in the **Federal Register** a notice that a complete application had been submitted, and provide the public the opportunity to submit to the Commission any information that relates to the Commission action requested in the application, subject to appropriate requests for confidential treatment being submitted pursuant to any applicable provisions governing confidentiality under the Exchange Act.⁹⁴¹

C. Respondents

The following table summarizes the estimated number of respondents that would be subject to the proposed Rule 10, Form SCIR, and recordkeeping burdens.

Type of registrant	Number
Covered Broker-Dealers	1,541
Non-Covered Broker-Dealers	1,969
Clearing agencies and exempt clearing agencies	16
MSRB	1
National securities exchanges	24
National securities associations	1
SBS Entities	50
SBSDRs	3
Transfer agents	353
<i>Total Covered Entities</i>	<i>1,989</i>
<i>Total Non-Covered Broker-Dealers</i>	<i>1,969</i>
<i>Total Respondents</i>	<i>3,958</i>

The respondents subject to these collection of information requirements include the following:

1. Broker-Dealers

Each broker-dealer registered with the Commission would be subject to proposed Rule 10 as either a Covered Entity or a Non-Covered Broker-Dealer. As of September 30, 2022, there were 3,510 broker-dealers registered with the Commission.⁹⁴² The Commission estimates that 1,541 of these broker-dealers would be Covered Entities under the proposed rule because they fit

within one or more of the following categories: carrying broker-dealer; broker-dealer that introduces customer accounts to a carrying broker-dealer on a fully disclosed basis; broker-dealer with regulatory capital equal to or exceeding \$50 million; broker-dealer with total assets equal to or exceeding \$1 billion; broker-dealer that operates as a market maker under the securities laws; or a broker-dealer that operates as an ATS.⁹⁴³ The Commission estimates that 1,969 broker-dealers (*i.e.*, the remaining broker-dealers registered

with/the Commission) would be Non-Covered Broker-Dealers for purposes of the rules.

2. Clearing Agencies

With regard to clearing agencies, respondents under these rules are: (1) nine registered clearing agencies;⁹⁴⁴ and (2) five exempt clearing agencies.⁹⁴⁵ The Commission estimates for purposes of the PRA that two additional entities may seek to register as a clearing agency in the next three years, and so for purposes of this proposal the Commission has assumed sixteen total

⁹⁴⁰ 17 CFR 240.0–13(h).

⁹⁴¹ See section V.F of this release.

⁹⁴² This estimate is derived from broker-dealer FOCUS filings and ATS Form ATS–R quarterly reports as of September 30, 2022.

⁹⁴³ *Id.*

⁹⁴⁴ The registered and active clearing agencies are: (1) DTC; (2) FICC; (3) NSCC; (4) ICC; (5) ICEEU; (6) the Options Clearing Corp.; and (7) LCH SA. The clearing agencies that are registered with the Commission but conduct no clearance or settlement operations are: (1) BSECC; and (2) SCCP.

⁹⁴⁵ The exempt clearing agencies that provide matching services are: (1) DTCC ITP Matching U.S. LLC; (2) Bloomberg STP LLC; (3) SS&C Technologies, Inc.; (4) Euroclear Bank SA/NV; and (5) Clearstream Banking, S.A.

clearing agency and exempt clearing agency respondents.

3. The MSRB

The sole respondent to the proposed collection of information for the MSRB is the MSRB itself.

4. National Securities Exchanges and National Securities Associations

The respondents to the proposed collections of information for national securities exchanges and national securities associations would be the 24 national securities exchanges currently registered with the Commission under section 6 of the Exchange Act,⁹⁴⁶ and the one national securities association currently registered with the Commission under section 15A of the Exchange Act.⁹⁴⁷

5. SBS Entities

As of January 4, 2023, 50 SBSDs have registered with the Commission, while no MSBSPs have registered with the Commission.⁹⁴⁸ Of the 50 SBSDs that have registered with the Commission, 7 entities are also broker-dealers.⁹⁴⁹

Requests for a substituted compliance determination under Rule 3a71–6 with respect to the proposed Rule 10, Form SCIR, and the related record preservation requirements may be filed by foreign financial authorities, or by non-U.S. SBSDs or MSBSPs. The Commission had previously estimated that there may be approximately 22 non-U.S. entities that may potentially register as SBSDs, out of approximately

50 total entities that may register as SBSDs.⁹⁵⁰ Potentially all non-U.S. SBSDs, or some subset thereof, may seek to rely on a substituted compliance determination in connection with the proposed cybersecurity risk management requirements.⁹⁵¹ However, the Commission had expected that the great majority of substituted compliance applications would be submitted by foreign authorities⁹⁵² given their expertise in connection with the relevant substantive requirements, and in connection with their supervisory and enforcement oversight with regard to SBSDs and their activities.⁹⁵³ The Commission expected that very few substituted compliance requests would come from SBS Entities.⁹⁵⁴ For purposes of PRA assessments, the Commission estimated that three SBS Entities would submit such applications.⁹⁵⁵ Although, as of January 4, 2023, 30 entities had identified themselves as a nonresident SBSD in their application for

registration with the Commission,⁹⁵⁶ the Commission has issued only one order in response to a request for substituted compliance from potential registrants.⁹⁵⁷ The Commission continues to believe that its estimate that three such entities will submit applications remains appropriate for purposes of this PRA assessment because applicants may file additional requests.

6. SBSDRs

Two SBSDRs are currently registered with the Commission.⁹⁵⁸ The Commission estimates for purposes of the PRA that one additional entity may seek to register as an SBSDR in the next three years, and so for purposes of this proposal the Commission has assumed three SBSDR respondents.

7. Transfer Agents

The proposed rule would apply to every transfer agent as defined in section 3(a)(25) of the Exchange Act that is registered or required to be registered with an appropriate regulatory agency as defined in section 3(a)(34)(B) of the Exchange Act. As of December 31, 2022, there were 353 transfer agents that were either registered with the Commission through Form TA–1 or registered with other appropriate regulatory agencies.

D. Total Initial and Annual Reporting Burdens

As stated above, each requirement to disclose information, offer to provide information, or adopt policies and procedures constitutes a collection of information requirement under the PRA. The Commission discusses below the collection of information burdens associated with the proposed rule and rule amendment.

1. Proposed Rule 10

The Commission has made certain estimates of the burdens associated with

⁹⁴⁶ See 15 U.S.C. 78f. The national securities exchanges registered with the Commission are: (1) BOX Options Exchange LLC; (2) Cboe BZX Exchange, Inc.; (3) Cboe BYX Exchange, Inc.; (4) Cboe C2 Exchange, Inc.; (5) Cboe EDGA Exchange, Inc.; (6) Cboe EDGX, Inc.; (7) Cboe Exchange, Inc.; (8) Investors Exchange Inc.; (9) Long-Term Stock Exchange, Inc.; (10) MEMX, LLC; (11) Miami International Securities Exchange LLC; (12) MIAX PEARL, LLC; (13) MIAX Emerald, LLC; (14) NASDAQ BX, Inc.; (15) NASDAQ GEMX, LLC; (16) NASDAQ ISE, LLC; (17) NASDAQ MRX, LLC; (18) NASDAQ PHLX LLC; (19) The NASDAQ Stock Market LLC; (20) New York Stock Exchange LLC; (21) NYSE MKT LLC; (22) NYSE Arca, Inc.; (23) NYSE Chicago Stock Exchange, Inc.; and (24) NYSE National, Inc.

⁹⁴⁷ See 15 U.S.C. 78o-3. The one national securities association registered with the Commission is FINRA.

⁹⁴⁸ See *List of Registered Security-Based Swap Dealers and Major Security-Based Swap Participants*, available at: <https://www.sec.gov/tm/List-of-SBS-Dealers-and-Major-SBS-Participants>.

⁹⁴⁹ A Covered Entity that is both a broker-dealer and an SBS Entity (which includes all seven of these broker-dealers) will have burdens with respect to the proposed rule, Form SCIR, and recordkeeping amendments as they apply to both its broker-dealer business and its security-based swap business. Therefore, such “dual-hatted” entities will be counted as both Covered Entities that are broker-dealers and as SBS Entities for purposes of the PRA.

⁹⁵⁰ See Proposed Rule Amendments and Guidance Addressing Cross-Border Application of Certain Security-Based Swap Requirements, Exchange Act Release No. 85823 (May 10, 2019), 84 FR 24206, 24253 (May 24, 2019). See also Security-Based Swap Transactions Connected With a Non-U.S. Person's Dealing Activity That Are Arranged, Negotiated, or Executed by Personnel Located in a U.S. Branch or Office or in a U.S. Branch or Office of an Agent; Security-Based Swap Dealer De Minimis Exception, Exchange Act Release No. 77104 (Feb. 10, 2016), 81 FR 8597, 8605 (Feb. 19, 2016) (“SBS Entity U.S. Activity Adopting Release”); Business Conduct Standards Adopting Release, 81 FR at 30090, 30105; SBS Entity Recordkeeping and Reporting Release, 84 FR at 68607–09; and Capital, Margin, and Segregation Requirements Adopting Release, 84 FR at 43960–61.

⁹⁵¹ Consistent with prior estimates, the Commission further believes that there may up to five MSBSPs. See *Registration Process for Security-Based Swap Dealers and Major Security-Based Swap Participants*, Exchange Act Release No. 75611 (Aug. 5, 2015), 80 FR 48963, 48990 (Aug. 14, 2015) (“SBS Entity Registration Adopting Release”); see also SBS Entity Business Conduct Standards Adopting Release, 81 FR at 30089, 30099. It is possible that some subset of those entities will be non-U.S. MSBSPs that will seek to rely on substituted compliance in connection with proposed Rule 10, Form SCIR, and the related record preservation requirements.

⁹⁵² See SBS Entity Risk Mitigation Adopting Release, 85 FR at 6389. See also SBS Entity Business Conduct Standards Adopting Release, 81 FR at 30097; SBS Entity Trade Acknowledgement and Verification Adopting Release, 81 FR at 39832.

⁹⁵³ See SBS Entity Risk Mitigation Adopting Release, 85 FR at 6384. See also SBS Entity Business Conduct Standards Adopting Release, 81 FR at 30090; SBS Entity Trade Acknowledgement and Verification Adopting Release, 81 FR at 39832.

⁹⁵⁴ See SBS Entity Risk Mitigation Adopting Release, 85 FR at 6389. See also SBS Entity Business Conduct Standards Adopting Release, 81 FR at 30097, n.1582 and accompanying text; SBS Entity Trade Acknowledgement and Verification Adopting Release, 81 FR at 39832.

⁹⁵⁵ *Id.* See also SBS Entity Recordkeeping and Reporting Adopting Release, 84 FR at 68609; Capital, Margin, and Segregation Requirements Adopting Release, 84 FR at 43967.

⁹⁵⁶ No entity has registered as an MSBSP. See *List of Registered Security-Based Swap Dealers and Major Security-Based Swap Participants*, available at: <https://www.sec.gov/tm/List-of-SBS-Dealers-and-Major-SBS-Participants> (providing the list of registered SBSDs and MSBSPs that was updated as of January 4, 2023).

⁹⁵⁷ See *Order Granting Conditional Substituted Compliance in Connection With Certain Requirements Applicable to Non-U.S. Security-Based Swap Dealers Subject to Regulation in the Swiss Confederation*, Exchange Act Release No. 93284 (Oct. 8, 2021), 86 FR 57455 (Oct. 15, 2021) (File No. S7–07–21). The Commission's other substituted compliance orders have been in response to requests from foreign authorities; see <https://www.sec.gov/tm/Jurisdiction-Specific-Apps-Orders-and-MOU>.

⁹⁵⁸ The Commission approved the registration of two SBSDRs in 2021. The two registered SBSDRs are: (1) DTCC Data Repository (U.S.), LLC; and (2) ICE Trade Vault, LLC.

the policies and procedures and review and report of the review requirements of proposed Rule 10 applicable to Covered Entities solely for the purpose of this

PRA analysis.⁹⁵⁹ Table 1 below summarizes the initial and ongoing annual burden and cost estimates associated with the policies and

procedures and review and report of the review requirements.

TABLE 1—RULE 10 PRA ESTIMATES—CYBERSECURITY POLICIES AND PROCEDURES AND REVIEW AND REPORT OF THE REVIEW REQUIREMENTS FOR COVERED ENTITIES

	Internal initial burden hours	Internal annual burden hours ¹	Wage rate ²	Internal time costs	Annual external cost burden
PROPOSED RULE 10 ESTIMATES					
Adopting and implementing policies and procedures ³ .	50	⁴ 21.67	\$462 (blended rate for compliance attorney and assistant general counsel).	\$10,011.54	⁵ \$1,488
Annual review of policies and procedures and report of review.	0	⁶ 10	\$462 (blended rate for compliance attorney and assistant general counsel).	4,620	⁷ 1,984
Total new annual burden per Covered Entity.		31.67		14,631.54	3,472
Number of Covered Entities		× 1,989		× 1,989	× 1,989
Total new annual aggregate burden		62,991.63		29,102,133.06	6,905,808

Notes:

¹ Includes initial burden estimates annualized over a 3-year period.

² The Commission's estimates of the relevant wage rates are based on salary information for the securities industry compiled by Securities Industry and Financial Markets Association's Office Salaries in the Securities Industry 2013, as modified by Commission staff for 2022 ("SIFMA Wage Report"). The estimated figures are modified by firm size, employee benefits, overhead, and adjusted to account for the effects of inflation.

³ These estimates are based on an average. Some firms may have a lower burden in the case they will be evaluating exiting policies and procedures with respect to any cybersecurity risks and/or incidents, while other firms may be creating new cybersecurity policies and procedures altogether.

⁴ Includes initial burden estimates annualized over a three-year period, plus 5 ongoing annual burden hours. The estimate of 21.67 hours is based on the following calculation: ((50 initial hours/3) + 5 additional ongoing burden hours) = 21.67 hours.

⁵ This estimated burden is based on the estimated wage rate of \$496/hour, for 3 hours, for outside legal services.

The Commission's estimates of the relevant wage rates for external time costs, such as outside legal services, take into account staff experience, a variety of sources including general information websites, and adjustments for inflation.

⁶ The Commission estimates 10 additional ongoing burden hours.

⁷ This estimated burden is based on the estimated wage rate of \$496/hour, for 4 hours, for outside legal services. See note 5 (regarding wage rates with respect to external cost estimates).

The Commission has made certain estimates of the burdens associated with the policies and procedures and review and record of the review requirements of proposed Rule 10 applicable to Non-

Covered Broker-Dealers solely for the purpose of this PRA analysis.⁹⁶⁰ Table 2 below summarizes the initial and ongoing annual burden and cost estimates associated with the proposed

rule's policies and procedures and review and record of the review requirements for Non-Covered Broker-Dealers.

TABLE 2—RULE 10 PRA ESTIMATES—CYBERSECURITY POLICIES AND PROCEDURES AND REVIEW AND RECORD OF THE REVIEW REQUIREMENTS FOR NON-COVERED BROKER-DEALERS

	Internal initial burden hours	Internal annual burden hours ¹	Wage rate ²	Internal time costs	Annual external cost burden
PROPOSED RULE 10 ESTIMATES					
Adopting and implementing policies and procedures ³ .	30	⁴ 15	\$462 (blended rate for compliance attorney and assistant general counsel).	\$6,930	⁵ \$1,488
Annual review of policies and procedures and report of review.	0	⁶ 6	\$462 (blended rate for compliance attorney and assistant general counsel).	2,772	⁷ 992
Total new annual burden per Non-Covered Broker-Dealer.		21		9,702	2,480
Number of Non-Covered Broker-Dealers		× 1,969		× 1,969	× 1,969
Total new annual aggregate burden		41,349		19,103,238	4,883,120

Notes:

¹ Includes initial burden estimates annualized over a 3-year period.

² The Commission's estimates of the relevant wage rates are based on salary information for the securities industry compiled by Securities Industry and Financial Markets Association's Office Salaries in the Securities Industry 2013, as modified by Commission staff for 2022 ("SIFMA Wage Report"). The estimated figures are modified by firm size, employee benefits, overhead, and adjusted to account for the effects of inflation.

³ These estimates are based on an average. Some firms may have a lower burden in the case they will be evaluating exiting policies and procedures with respect to any cybersecurity risks and/or incidents, while other firms may be creating new cybersecurity policies and procedures altogether.

⁴ Includes initial burden estimates annualized over a three-year period, plus 5 ongoing annual burden hours. The estimate of 15 hours is based on the following calculation: ((30 initial hours/3) + 5 additional ongoing burden hours) = 15 hours.

⁵ This estimated burden is based on the estimated wage rate of \$496/hour, for 3 hours, for outside legal services.

The Commission's estimates of the relevant wage rates for external time costs, such as outside legal services, take into account staff experience, a variety of sources including general information websites, and adjustments for inflation.

⁶ The Commission estimates 6 additional ongoing burden hours.

⁷ This estimated burden is based on the estimated wage rate of \$496/hour, for 2 hours, for outside legal services. See note 5 (regarding wage rates with respect to external cost estimates).

⁹⁵⁹ These requirements are discussed in section II.B.1. of this release.

⁹⁶⁰ These requirements are discussed in section II.C. of this release.

The Commission has made certain estimates of the burdens associated with the notification requirement of proposed Rule 10 applicable to Market Entities

solely for the purpose of this PRA analysis.⁹⁶¹ Table 3 below summarizes the initial and ongoing annual burden and cost estimates associated with the

proposed rule's notification requirements for Market Entities.

TABLE 3—RULE 10 PRA ESTIMATES—NOTIFICATION REQUIREMENTS FOR MARKET ENTITIES

	Internal initial burden hours	Internal annual burden hours		Wage rate	Internal time costs	Annual external cost burden
PROPOSED RULE 10 ESTIMATES						
Making a determination of significant cybersecurity incident and immediate notice to the Commission.	5	14.67	×	\$353 (blended rate for assistant general counsel, compliance manager and systems analyst).	\$1,648.51	² \$1,488
Total new annual burden per Market Entity.	4.67	1,648.51	1,488
Number of Market Entities	×	3,958	×	3,958
Total new aggregate annual burden	18,483.86	6,524,802.58	5,889,504

Notes:
¹ Includes initial burden estimates annualized over a three-year period, plus 3 ongoing annual burden hours. The estimate of 4.67 hours is based on the following calculation: ((5 initial hours/3) + 3 additional ongoing burden hours) = 4.67 hours.
² This estimated burden is based on the estimated wage rate of \$496/hour, for 3 hours, for outside legal services.
 The Commission's estimates of the relevant wage rates for external time costs, such as outside legal services, take into account staff experience, a variety of sources including general information websites, and adjustments for inflation.

The Commission has made certain estimates of the burdens associated with the requirement of proposed Rule 10 that Covered Broker-Dealers provide the disclosures that would need to be made on Part II of proposed Form SCIR

requirements to their customers solely for the purpose of this PRA analysis.⁹⁶² Table 4 below summarizes the initial and ongoing annual burden and cost estimates associated with the requirement of proposed Rule 10 that

Covered Broker-Dealers provide the disclosures that would need to be made on Part II of proposed Form SCIR requirements to their customers.

TABLE 4—RULE 10 PRA ESTIMATES—ADDITIONAL DISCLOSURE REQUIREMENTS FOR BROKER-DEALERS THAT ARE COVERED ENTITIES

	Internal initial burden hours	Internal annual burden hours		Wage rate	Internal time costs	Annual external cost burden
PROPOSED RULE 10 ESTIMATES						
Delivery of disclosures to new customers ...	16.68	6.68	×	\$69 (general clerk)	\$460.92	\$0
Annual delivery of disclosures to existing customers.	² 44.48	44.48	\$69 (general clerk)	3,076.02	0
Total new annual burden per broker-dealer Covered Entities.	51.26	3,536.94
Number of broker-dealer Covered Entities	×	1,541	×	1,541
Total new aggregate annual burden	78,991.66	5,450,424.54

Notes:
¹ The Commission estimates that a broker-dealer that is a Covered Entity will require no more than 0.02 hours to send the broker-dealer's required disclosures to each new customer, or an annual burden of 6.68 hours per broker-dealer. (0.02 hours per customer × 334 median number of new customers per broker-dealer based on FOCUS Schedule I data as of December 31, 2022 = approximately 6.68 hours per broker-dealer.) The Commission notes that the burden for preparing disclosures to customers is already incorporated into a separate burden estimate under other broker-dealer rules promulgated by the Commission (e.g., 17 CFR 240.17a-3) and FINRA rules. The Commission expects that broker-dealers subject to this new disclosure requirement will make their delivery of disclosures to new customers as part of an email or mailing they already send to new customers; therefore, the Commission estimates that the additional burden will be adding a few pages to the email attachment or mailing.
² The Commission estimates that, with a bulk mailing or email, a broker-dealer that is a Covered Entity will require no more than 0.02 hours to send the broker-dealer's required disclosures to each existing customer, or an annual burden of 44.58 hours per broker-dealer. (0.02 hours per customer × 2,229 median number of customers per broker-dealer based on FOCUS Schedule I data as of December 31, 2022 = approximately 44.58 hours per broker-dealer.) The Commission notes that the burden for preparing disclosures to customers is already incorporated into a separate burden estimate under other broker-dealer rules promulgated by the Commission (e.g., 17 CFR 240.17a-3) and FINRA rules. The Commission expects that broker-dealers subject to this new disclosure requirement will make their annual delivery to existing customers as part of an email or mailing of an account statement they already send to customers; therefore, the Commission estimates that the additional burden will be adding a few pages to the email attachment or mailing.

2. Form SCIR

The Commission has made certain estimates of the burdens associated with

filing the initial and amended Part I of Form SCIR under proposed Rule 10 applicable to Covered Entities solely for the purpose of this PRA analysis.⁹⁶³

Table 5 below summarizes the initial and ongoing annual burden and cost estimates associated with filing proposed Form SCIR.

⁹⁶¹ This requirement is discussed in section II.B.2.a. of this release.

⁹⁶² These requirements are discussed in section II.B.3.b. of this release.

⁹⁶³ These requirements are discussed in sections II.B.2. and II.B.4. of this release.

TABLE 5—PART I OF FORM SCIR PRA ESTIMATES

	Internal initial burden hours	Internal annual burden hours		Wage rate	Internal time costs	Annual external cost burden
PROPOSED PART I OF FORM SCIR ESTIMATES						
Filing out initial Part I of Form SCIR	3	¹ 1.5		\$431 (blended rate for assistant general counsel, compliance manager).	\$646.50	² \$496
Filing an amended Part I of SCIR	1	1		\$431 (blended rate for assistant general counsel, compliance manager).	431	³ 496
Total new annual burden per Covered Entity		2.5		1077.50	992
Number of Covered Entity		× 1,989		× 1,989	× 1,989
Total new aggregate annual burden		4,972.5		2,143,147.5	1,973,088

Notes:

¹ Includes initial burden estimates annualized over a three-year period, plus 0.5 ongoing annual burden hours. The estimate of 1.5 hours is based on the following calculation: ((3 initial hours/3) + 0.5 additional ongoing burden hours) = 1.5 hours.

² This estimated burden is based on the estimated wage rate of \$496/hour, for 1 hour, for outside legal services.

The Commission's estimates of the relevant wage rates for external time costs, such as outside legal services, takes into account staff experience, a variety of sources including general information websites, and adjustments for inflation.

³ This estimated burden is based on the estimated wage rate of \$496/hour, for 1 hour, for outside legal services.

The Commission has made certain estimates of the burdens associated with filing the Part II of Form SCIR under proposed Rule 10 applicable to Covered

Entities solely for the purpose of this PRA analysis.⁹⁶⁴ Table 6 below summarizes the initial and ongoing annual burden and cost estimates

associated with the proposed rule's disclosure requirements for Covered Entities.

TABLE 6—PART II OF FORM SCIR PRA ESTIMATES

	Internal initial burden hours	Internal annual burden hours		Wage rate	Internal time costs	Annual external cost burden
PROPOSED PART II OF FORM SCIR ESTIMATES						
Disclosure of significant cybersecurity incidents and cybersecurity risks on Part II of Form SCIR and posting form on website.	5	¹ 3.67	×	\$375.33 per hour (blended rate for assistant general counsel, senior compliance examiner and compliance manager) ³ .	\$1,377.46	² \$1,488
Total new annual burden per Covered Entity		3.67		1,377.46	1,488
Number of Covered Entities		× 1,989		× 1,989	× 1,989
Total new aggregate annual burden		7,299.63		2,739,767.94	2,959,632

Notes:

¹ Includes initial burden estimates annualized over a three-year period, plus 2 ongoing annual burden hours. The estimate of 3 hours is based on the following calculation: ((5 initial hours/3) + 2 additional ongoing burden hours) = 3.67 hours.

² This estimated burden is based on the estimated wage rate of \$496/hour, for 3 hours, for outside legal services.

The Commission's estimates of the relevant wage rates for external time costs, such as outside legal services, take into account staff experience, a variety of sources including general information websites, and adjustments for inflation.

³ The \$375.33 wage rate reflects current estimates from the SIFMA Wage Report of the blended hourly rate for an assistant general counsel (\$518), senior compliance examiner (\$264) and a compliance manager (\$344). (\$518 + \$264 + \$344)/3 = \$375.33.

In addition, the requirement to file Form SCIR in EDGAR using a form-specific XML may impose some compliance costs. Covered Entities that are not otherwise required to file in EDGAR—for example, clearing agencies, the MSRB, national securities associations, and national securities exchanges, as well as any broker-dealer

Covered Entities that choose not to file Form X-17A-5 Part III or Form 17-H through the EDGAR system, would need to complete Form ID to obtain the EDGAR-system access codes that enable entities to file documents through the EDGAR system.⁹⁶⁵ The Commission estimates that each filer that currently does not have access to EDGAR would

incur an initial, one-time burden of 0.30 hours to complete and submit a Form ID.⁹⁶⁶ Therefore, the Commission believes the one-time industrywide reporting burden associated with the proposed requirements to file on

⁹⁶⁴ These requirements are discussed in sections II.B.3. and II.B.4. of this release.

⁹⁶⁵ Form ID (OMB control number 3235-0328) must be completed and filed with the Commission by all individuals, companies, and other organizations who seek access to file electronically on EDGAR. Accordingly, a filer that does not already have access to EDGAR must submit a Form

ID, along with the notarized signature of an authorized individual, to obtain an EDGAR identification number and access codes to file on EDGAR. The Commission currently estimates that Form ID would take 0.30 hours to prepare, resulting in an annual industry-wide burden of 17,199 hours. See Supporting Statement for the Paperwork Reduction Act Information Collection Submission for Form ID (Dec. 20 2021), available at [https://](https://www.reginfo.gov/public/do/PRAViewDocument?ref_nbr=202112-3235-003)

www.reginfo.gov/public/do/PRAViewDocument?ref_nbr=202112-3235-003.

⁹⁶⁶ The Commission does not estimate a burden for SBS Entities since these firms have already filed Form ID so they can file Form SBSE on EDGAR. Similarly, the Commission does not estimate a burden for transfer agents since these firms already file their annual report on Form TA-2 on EDGAR.

EDGAR is 4.8 hours for clearing agencies,⁹⁶⁷ 0.30 hours for the MSRB,⁹⁶⁸ 7.5 hours for national securities exchanges and associations;⁹⁶⁹ 0.9 hours for SBSDRs;⁹⁷⁰ and 242.4 hours for Covered Broker-Dealers not already filing their annual audits on EDGAR.⁹⁷¹ In addition, the requirement to file Form SCIR using custom XML (with which a Covered Entity would be able to comply by inputting its disclosures into a fillable web form), the Commission

estimates each Covered Entity would incur an internal burden of 0.5 hours per filing.⁹⁷² Accordingly, the Commission estimates that Covered Entities will collectively have an ongoing burden of 994.5 hours⁹⁷³ with respect to filing Form SCIR in custom XML.

3. Rules 17a-4, 17ad-7, 18a-6, and Clearing Agency Exemption Orders (and Existing Rules 13n-7 and 17a-1)

The Commission has made certain estimates of the burdens associated with the proposed record preservation requirements solely for the purpose of this PRA analysis.⁹⁷⁴ Table 7 below summarizes the initial and ongoing annual burden and cost estimates associated with the additional recordkeeping requirements.

TABLE 7—PRA ESTIMATES—PROPOSED AMENDMENTS TO RULES 17a-4, 18a-6, AND 17ad-7 AND CLEARING AGENCY EXEMPTION ORDERS (AND EXISTING RULES 17a-1 AND 13n-7)⁹⁷⁵

	Internal annual hour burden		Wage rate	Internal time costs	Annual external cost burden
PROPOSED ESTIMATES FOR RECORDKEEPING BURDENS					
Retention of cybersecurity policies and procedures.	1	×	\$73.5 (blended rate for general clerk and compliance clerk).	\$73.5	\$0
Total burden per Covered Entity or Non-Covered Broker-Dealer.	1			73.5	0
Total number of affected entities ...	×	3,918		×	3,918
Sub-total burden	3,918 hours			287,973	0
Retention of written report documenting annual review.	1	×	73.5 (blended rate for general clerk and compliance clerk).	73.5	0
Total annual burden per Covered Entity or Non-Covered Broker-Dealer.	1			73.5	0
Total number of affected entities ...	×	3,918		×	3,918
Sub-total burden	3,918 hours			287,973	0
Retention of copy of any Form SCIR or immediate notice to the Commission.	1	×	73.5 (blended rate for general clerk and compliance clerk).	73.5	0
Total annual burden per Covered Entity or Non-Covered Broker-Dealer.	1			73.5	0
Total number of affected entities ...	×	3,918		×	3,918
Sub-total burden	3,918 hours			287,973	0
Retention of records documenting a cybersecurity incident.	1	×	73.5 (blended rate for general clerk and compliance clerk).	73.5	0
Total annual burden per Covered Entity.	1			73.5	0
Total number of affected Covered Entities.	×	1,949		×	1,949
Sub-total burden	1,949 hours			143,251.50	0
Retention of records documenting a Covered Entity's cybersecurity risk assessment.	1	×	73.5 (blended rate for general clerk and compliance clerk).	73.5	0
Total annual burden per Covered Entity.	1			73.5	0
Total number of affected Covered Entities.	×	1,949		×	1,949
Sub-total burden	1,949 hours			143,251.50	0
Retention of copy of any public disclosures.	1	×	73.5 (blended rate for general clerk and compliance clerk).	73.5	0
Total annual burden per Covered Entity.	1			73.5	0
Total number of affected Covered Entities.	×	1,949		×	1,949
Sub-total burden	1,949 hours			143,251.50	0

⁹⁶⁷ 0.30 hours × 16 clearing agencies = 4.8 hours.

⁹⁶⁸ 0.30 hours × 1 MSRB = 0.30 hours.

⁹⁶⁹ 0.30 hours × (24 national securities exchanges and 1 national securities association) = 7.5 hours.

⁹⁷⁰ 0.30 hours × 3 SBSRs = 0.9 hours.

⁹⁷¹ 0.30 hours × 808 Covered Broker-Dealers not already filing on EDGAR = 242.4 hours.

⁹⁷² This estimate would mirror the Commission's internal burden hour estimate for a proposed custom XML requirement for Schedules 13D and 13G. See Modernization of Beneficial Ownership Reporting Release.

⁹⁷³ 1,989 Covered Entities × .5 hours = 994.5 hours.

⁹⁷⁴ These requirements are discussed in sections II.B.5.a. and II.C. of this release.

⁹⁷⁵ Given the general nature of the recordkeeping requirements for national securities exchanges, national securities associations, registered clearing agencies, and the MSRB under Rule 17a-1 (OMB control number 3235-0208, Recordkeeping Rule for National Securities Exchanges, National Securities Associations, Registered Clearing Agencies, and the Municipal Securities Rulemaking Board) and for

SBSDRs under Rule 13n-7 (OMB control number 3235-0719, Security-Based Swap Data Repository Registration, Duties, and Core Principles and Form SDR), it is anticipated that the new recordkeeping requirements proposed in this release would result in a one-time nominal increase in burden per entity that would effectively be encompassed by the existing burden estimates associated with these existing rules as described in those collections of information. Below, the Commission solicits comment regarding all of the PRA estimates discussed in this release.

TABLE 7—PRA ESTIMATES—PROPOSED AMENDMENTS TO RULES 17a–4, 18a–6, AND 17ad–7 AND CLEARING AGENCY EXEMPTION ORDERS (AND EXISTING RULES 17a–1 AND 13n–7)⁹⁷⁵—Continued

	Internal annual hour burden	Wage rate	Internal time costs	Annual external cost burden
Total annual aggregate burden of recordkeeping obligations.	17,601 hours		1,293,673.5	0

4. Substituted Compliance—Rule 3a71–6

Rule 3a71–6 would require submission of certain information to the Commission to the extent SBS Entities elect to request a substituted compliance determination with respect to proposed Rule 10, Form SCIR, and the related record preservation requirements. Consistent with Exchange Act Rule 0–13, such applications must be accompanied by supporting documentation necessary for the Commission to make the determination, including information regarding applicable foreign requirements, and the methods used by foreign authorities to monitor and enforce compliance. If Rule 3a71–6 is amended as proposed, the Commission expects that the majority of such requests will be made during the first year following the effective date.

The Commission expects that the great majority of substituted compliance applications will be submitted by foreign authorities, and that very few substituted compliance requests will come from SBS Entities. For purposes of this assessment, the Commission estimates that three such SBS Entities will submit such an application.⁹⁷⁶

The Commission has previously estimated that the paperwork burden associated with filing a request for a substituted compliance determination related to existing business conduct, supervision, chief compliance officer, and trade acknowledgement and verification requirements described in Rule 3a71–6(d)(1)–(3) was approximately 80 hours of in-house counsel time, plus \$84,000⁹⁷⁷ for the services of outside professionals, and

⁹⁷⁶ See SBS Entity Risk Mitigation Adopting Release, 85 FR at 6389. See also SBS Entity Business Conduct Standards Adopting Release, 81 FR at 30097, n.1582 and accompanying text; SBS Entity Trade Acknowledgement and Verification Adopting Release, 81 FR at 39832; SBS Entity Recordkeeping and Reporting Adopting Release, 84 FR at 68609; Capital, Margin, and Segregation Requirements Adopting Release, 84 FR at 43967.

⁹⁷⁷ Based on 200 hours of outside time × \$420 per hour. This estimated burden also includes the burden associated with making a request for a substituted compliance determination related to the portfolio reconciliation, portfolio compression, and trading relationship documentation requirements described in Rule 3a71–6(d)(7); see SBS Entity Risk Mitigation Adopting Release, 85 FR at 6389.

the paperwork burden estimate associated with making a request for a substituted compliance determination related to the existing recordkeeping and reporting requirements described in Rule 3a71–6(d)(6) was approximately 80 hours of in-house counsel time, plus \$84,000⁹⁷⁸ for the services of outside professionals.⁹⁷⁹ To the extent that an SBS Entity files a request for a substituted compliance determination in connection with Rule 10, Form SCIR, the related record preservation requirements, and requirements currently identified in Rule 3a71–6(d) as eligible for substituted compliance determinations, the Commission believes that the paperwork burden associated with the request would be greater than that associated with a narrower request due to the need for more information regarding the comparability of the relevant rules and the adequacy of the associated supervision and enforcement practices. However, the Commission believes that its prior paperwork burden estimate is sufficient to cover a combined substituted compliance request that also seeks a determination in connection with Rule 10, Form SCIR, and the related record preservation requirements.⁹⁸⁰

Nevertheless, the Commission is revising its estimate of the hourly rate for outside professionals to \$496,

⁹⁷⁸ Based on 200 hours of outside time × \$420 per hour.

⁹⁷⁹ See *Supporting Statement for the Paperwork Reduction Act Information Collection Submission for Exchange Act Rule 3a71–6* (June 10, 2021), available at https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=202106-3235-008.

⁹⁸⁰ Although applicants may file requests for substituted compliance determinations related to multiple eligible requirements, applicants may instead file requests for substituted compliance determinations related to individual eligible requirements. As such, the Commission’s estimates reflect the total paperwork burden of requests filed by (i) applicants that would be seeking a substituted compliance determination related to Rule 10, Form SCIR, and the related record preservation requirements combined with a request for a substituted compliance determination related to other eligible requirements, and (ii) applicants that previously filed requests for substituted compliance determinations related to other eligible requirements and would be seeking an additional substituted compliance determination in connection with Rule 10, Form SCIR, and the related record preservation requirements.

consistent with the other paperwork burden estimates in this release. Therefore, the Commission estimates that the total paperwork burden incurred by entities associated with preparing and submitting a request for a substituted compliance determination in connection with the proposed cybersecurity risk management requirements applicable to SBS Entities would be reflected in the estimated burden of a request for a substituted compliance determination related to the business conduct, supervision, chief compliance officer, trade acknowledgement and verification, and the portfolio reconciliation, portfolio compression, and trading relationship documentation requirements described in Rule 3a71–6(d)(1)–(3) and (7) of approximately 80 hours of in-house counsel time, plus \$99,200 for the services of outside professionals,⁹⁸¹ and the paperwork burden associated with making a request for a substituted compliance determination related to the recordkeeping and reporting requirements described in Rule 3a71–6(d)(6) of approximately 80 hours of in-house counsel time, plus \$99,200 for the services of outside professionals.⁹⁸² This estimate results in an aggregate total one-time paperwork burden associated with preparing and submitting requests for substituted compliance determinations relating to the requirements described in Rule 3a71–6(d)(1) through (3), (6) and (7), including the proposed cybersecurity risk management requirements, of approximately 480 internal hours,⁹⁸³ plus \$595,200 for the services of outside professionals⁹⁸⁴ for all three requests.

E. Collection of Information is Mandatory

The collections of information pursuant to proposed Rule 10, Form SCIR, and the relevant recordkeeping

⁹⁸¹ Based on 200 hours of outside time × \$496 per hour.

⁹⁸² Based on 200 hours of outside time × \$496 per hour.

⁹⁸³ (80 hours related to Rule 3a71–6(d)(1) through (3), (7) plus 80 hours related to Rule 3a71–6(d)(6)) * 3 requests.

⁹⁸⁴ (\$99,200 related to Rule 3a71–6(d)(1) through (3), (7) plus \$99,200 related to Rule 3a71–6(d)(6)) * 3 requests.

rules are mandatory, as applicable, for Market Entities. With respect to Rule 3a71-6, the application for substituted compliance is mandatory for all foreign financial regulatory authorities or SBS Entities that seek a substituted compliance determination.

F. Confidentiality of Responses to Collection of Information

The Commission expects to receive confidential information in connection with the collections of information. A Market Entity can request confidential treatment of the information.⁹⁸⁵ If such confidential treatment request is made, the Commission anticipates that it will keep the information confidential subject to applicable law.⁹⁸⁶

With regard to Rule 3a71-6, the Commission generally will make requests for a substituted compliance determination public, including supporting documentation provided by the requesting party, subject to requests for confidential treatment being submitted pursuant to any applicable provisions governing confidentiality under the Exchange Act.⁹⁸⁷ If confidential treatment is granted, the Commission would keep such information confidential, subject to the provisions of applicable law.⁹⁸⁸

G. Retention Period for Recordkeeping Requirements

Rule 17a-4, as proposed to be amended, specifies the required retention periods for records required to be made and preserved by a broker-dealer, whether electronically or otherwise.⁹⁸⁹ Rule 17ad-7, as proposed to be amended, specifies the required retention periods for records required to be made and preserved by transfer agents, whether electronically or otherwise.⁹⁹⁰ Rule 18a-6, as proposed to be amended, specifies the required retention periods for records required to be made and preserved by SBSs or MSBSPs, whether electronically or otherwise.⁹⁹¹ All records required of certain of the Market Entities pursuant to the proposed rule amendments must

be retained for three years.⁹⁹² Existing Rule 17a-1 specifies the required retention periods for records required to be made and preserved by national securities exchanges, national securities associations, registered clearing agencies, and the MSRB, whether electronically or otherwise.⁹⁹³ Under the existing provisions of Rule 17a-1, registered clearing agencies, the MSRB, national securities associations, and national securities exchanges would be required to preserve at least one copy of the Rule 10 Records for at least five years, the first two years in an easily accessible place. Existing Rule 13n-7, which is not proposed to be amended, specifies the required retention periods for records required to be made and preserved by SBSs, whether electronically or otherwise.⁹⁹⁴ Rule 13n-7 provides that the SBS must keep the documents for a period of not less than five years, the first two years in a place that is immediately available to representatives of the Commission for inspection and examination.⁹⁹⁵ Finally, exempt clearing agencies are generally subject to conditions that mirror certain of the recordkeeping requirements in Rule 17a-1.⁹⁹⁶ Nonetheless, the Commission is proposing to amend the clearing agency exemption orders to add a condition that each exempt clearing agency must retain the Rule 10 Records for a period of at least five years after the record is made or, in the case of the written policies and procedures to address cybersecurity risks, for at least five years after the termination of the use of the policies and procedures.

H. Request for Comment

Pursuant to 44 U.S.C. 3506(c)(2)(B), the Commission solicits comment on the proposed collections of information in order to:

- Evaluate whether the proposed collections of information are necessary for the proper performance of the functions of the Commission, including whether the information would have practical utility;

- Evaluate the accuracy of the Commission's estimates of the burden of the proposed collections of information;

- Determine whether there are ways to enhance the quality, utility, and clarity of the information to be collected; and

- Evaluate whether there are ways to minimize the burden of the collection of information on those who respond, including through the use of automated collection techniques or other forms of information technology.

Persons submitting comments on the collection of information requirements should direct them to the Office of Management and Budget, Attention: Desk Officer for the Securities and Exchange Commission, Office of Information and Regulatory Affairs, Washington, DC 20503, and should also send a copy of their comments to Vanessa A. Countryman, Secretary, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549-1090, with reference to File Number S7-06-23. Requests for materials submitted to OMB by the Commission with regard to this collection of information should be in writing, with reference to File Number S7-06-23 and be submitted to the Securities and Exchange Commission, Office of FOIA/PA Services, 100 F Street NE, Washington, DC 20549-2736. As OMB is required to make a decision concerning the collections of information between 30 and 60 days after publication, a comment to OMB is best assured of having its full effect if OMB receives it within 30 days of publication.

VI. Initial Regulatory Flexibility Act Analysis

The RFA requires the Commission, in promulgating rules, to consider the impact of those rules on small entities.⁹⁹⁷ Section 603(a) of the Administrative Procedure Act,⁹⁹⁸ as amended by the RFA, generally requires the Commission to undertake a regulatory flexibility analysis of all proposed rules to determine the impact of such rulemaking on "small entities."⁹⁹⁹ Section 605(b) of the RFA states that this requirement shall not apply to any proposed rule which, if adopted, would not have a significant

⁹⁸⁵ See 17 CFR 200.83. Information regarding requests for confidential treatment of information submitted to the Commission is available on the Commission's website at <https://www.sec.gov/foia/howfo2.htm#privacy>.

⁹⁸⁶ See, e.g., 5 U.S.C. 552 et seq.; 15 U.S.C. 78x (governing the public availability of information obtained by the Commission).

⁹⁸⁷ See, e.g., 17 CFR 200.83; 17 CFR 240.24b-2; see also SBS Entity Definitions Adopting Release, 79 FR at 47359.

⁹⁸⁸ See, e.g., 5 U.S.C. 552 et seq.; 15 U.S.C. 78x (governing the public availability of information obtained by the Commission).

⁹⁸⁹ See Rule 17a-4, as proposed to be amended.

⁹⁹⁰ See Rule 17ad-7, as proposed to be amended.

⁹⁹¹ See Rule 18a-6, as proposed to be amended.

⁹⁹² See Rules 17a-4, 17A-d, and 18a-6, as proposed to be amended.

⁹⁹³ See Rule 17a-1.

⁹⁹⁴ See Rule 13n-7.

⁹⁹⁵ See paragraph (b)(2) of Rule 13n-7.

⁹⁹⁶ See, e.g., BSTP SS&C Order, 80 FR at 75411 (conditioning BSTP's exemption by requiring BSTP to, among other things, preserve a copy or record of all trade details, allocation instructions, central trade matching results, reports and notices sent to customers, service agreements, reports regarding affirmation rates that are sent to the Commission or its designee, and any complaint received from a customer, all of which pertain to the operation of its matching service and ETC service. BSTP shall retain these records for a period of not less than five years, the first two years in an easily accessible place).

⁹⁹⁷ See 5 U.S.C. 601 et seq.

⁹⁹⁸ 5 U.S.C. 603(a).

⁹⁹⁹ Section 601(b) of the RFA permits agencies to formulate their own definitions of "small entities." See 5 U.S.C. 601(b). The Commission has adopted definitions for the term "small entity" for the purposes of rulemaking in accordance with the RFA. These definitions, as relevant to this proposed rulemaking, are set forth in Rule 0-10.

economic impact on a substantial number of small entities.¹⁰⁰⁰

The Commission has prepared the following Initial Regulatory Flexibility Analysis (“IRFA”) in accordance with section 3(a) of the RFA.¹⁰⁰¹ It relates to: (1) proposed Rule 10 under the Exchange Act; (2) proposed Form SCIR; and (3) proposed amendments to Rules 17a-4, 17ad-7, and 18a-6 under the Exchange Act.¹⁰⁰²

A. Reasons for, and Objectives of, Proposed Action

The reasons for, and objectives of, the proposed rule and rule amendments are discussed above.¹⁰⁰³

1. Proposed Rule 10 and Parts I and II of Proposed Form SCIR

Proposed Rule 10 would require all Market Entities (Covered Entities and non-Covered Entities) to establish, maintain, and enforce written policies and procedures that are reasonably designed to address their cybersecurity risks.¹⁰⁰⁴ All Market Entities also, at least annually, would be required to review and assess the design and effectiveness of their cybersecurity policies and procedures, including whether the policies and procedures reflect changes in cybersecurity risk over the time period covered by the review.¹⁰⁰⁵ They also would be required to prepare a report (in the case of Covered Entities) and a record (in the case of non-Covered Entities) with respect to the annual review.¹⁰⁰⁶ Finally, all Market Entities would need to give the Commission immediate written electronic notice of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring.¹⁰⁰⁷

Market Entities that meet the definition of “covered entity” would be subject to certain additional requirements under proposed Rule 10.¹⁰⁰⁸ First, their cybersecurity risk management policies and procedures would need to include the following elements:

- Periodic assessments of cybersecurity risks associated with the Covered Entity’s information systems and written documentation of the risk assessments;
- Controls designed to minimize user-related risks and prevent unauthorized access to the Covered Entity’s information systems;
- Measures designed to monitor the Covered Entity’s information systems and protect the Covered Entity’s information from unauthorized access or use, and oversight of service providers that receive, maintain, or process information, or are otherwise permitted to access the Covered Entity’s information systems;
- Measures to detect, mitigate, and remediate any cybersecurity threats and vulnerabilities with respect to the Covered Entity’s information systems; and
- Measures to detect, respond to, and recover from a cybersecurity incident and written documentation of any cybersecurity incident and the response to and recovery from the incident.¹⁰⁰⁹

Second, Covered Entities—in addition to providing the Commission with immediate written electronic notice of a significant cybersecurity incident—would need to report and update information about the significant cybersecurity incident by filing Part I of proposed Form SCIR with the Commission through the EDGAR system.¹⁰¹⁰ The form would elicit information about the significant cybersecurity incident and the Covered Entity’s efforts to respond to, and recover from, the incident.

Third, Covered Entities would need to publicly disclose summary descriptions of their cybersecurity risks and the

significant cybersecurity incidents they experienced during the current or previous calendar year on Part II of proposed Form SCIR.¹⁰¹¹ The form would need to be filed with the Commission through the EDGAR system and posted on the Covered Entity’s business internet website and, in the case of Covered Entities that are carrying or introducing broker-dealers, provided to customers at account opening and annually thereafter.

Covered Entities and Non-Covered Entities would need to preserve certain records relating to the requirements of proposed Rule 10 in accordance with amended or existing recordkeeping requirements applicable to them or, in the case of exempt clearing agencies, pursuant to conditions in relevant exemption orders.¹⁰¹²

Collectively, these requirements are designed to address cybersecurity risk and the threat it poses to Market Entities and the U.S. securities markets. The written policies and procedures, the records required to be made pursuant to those policies and procedures, and the report or record of the annual review of the policies and procedures would address the specific cybersecurity risks to which Market Entities are exposed. The Commission could use these written policies and procedures, reports, and records to review Market Entities’ compliance with proposed Rule 10.

The Commission could use the immediate written electronic notification of significant cybersecurity incidents to promptly begin to assess the situation by, for example, when warranted, assessing the Market Entity’s operating status and engaging in discussions with the Market Entity to understand better what steps it is taking to protect its customers, counterparties, members, registrants, or user. The Commission could use the subsequent reports about the significant cybersecurity incident filed by Covered Entities using Part I of proposed Form SCIR to understand better the nature and extent of a particular significant cybersecurity incident and the efficacy of the Covered Entity’s response to mitigate the disruption and harm caused by the incident. The Commission staff could use the reports to focus on the Covered Entity’s operating status and to facilitate their outreach to, and discussions with, personnel at the Covered Entity who are addressing the significant cybersecurity incident. In

¹⁰⁰⁰ See 5 U.S.C. 605(b).

¹⁰⁰¹ 5 U.S.C. 603(a).

¹⁰⁰² The Commission is also certifying that amendments to Rule 3a71-6 will not have a significant economic impact on a substantial number of small entities for purposes of the RFA. See section VI.C.5. of this release.

¹⁰⁰³ See sections I and II of this release.

¹⁰⁰⁴ See paragraphs (b) through (d) of proposed Rule 10 (setting forth the requirements for Market Entities that meet the definition of “covered entity”); paragraph (e)(1) of proposed Rule 10. See also sections II.B.1 and II.C. of this release (discussing these proposed requirements in more detail).

¹⁰⁰⁵ See paragraph (b)(2) of proposed Rule 10; paragraph (e)(1) of proposed Rule 10. See also sections II.B.1.f. and II.C. of this release (discussing these proposed requirements in more detail).

¹⁰⁰⁶ See paragraph (b)(2) of proposed Rule 10; paragraph (e)(1) of proposed Rule 10. See also sections II.B.1.f. and II.C. of this release (discussing these proposed requirements in more detail).

¹⁰⁰⁷ See paragraph (c)(1) of proposed Rule 10; paragraph (e)(2) of proposed Rule 10. See also sections II.B.2.a. and II.C. of this release (discussing these proposed requirements in more detail).

¹⁰⁰⁸ See paragraph (b) through (d) of proposed Rule 10 (setting forth the requirements for Market Entities that meet the definition of “covered entity”); paragraph (e) of proposed Rule 10 (setting forth the requirements for Market Entities that do not meet the definition of “covered entity”).

¹⁰⁰⁹ See sections II.B.1.a. through II.B.1.e. of this release (discussing these proposed requirements in more detail). In the case of non-Covered Entities, as discussed in more detail below in section II.C. of this release, the design of the cybersecurity risk management policies and procedures would need to take into account the size, business, and operations of the broker-dealer. See paragraph (e) of proposed Rule 10.

¹⁰¹⁰ See sections II.B.2. and II.B.4. of this release (discussing these proposed requirements in more detail).

¹⁰¹¹ See sections II.B.3. and II.B.4. of this release (discussing these proposed requirements in more detail).

¹⁰¹² See sections II.B.5. and II.C. of this release (discussing these proposed requirements in more detail).

addition, the reporting would provide the staff with a view into the Covered Entity's understanding of the scope and impact of the significant cybersecurity incident. All of this information could be used by the Commission and its staff in assessing the significant cybersecurity incident impacting the Covered Entity. Further, the Commission could be use the database of reports to assess the potential cybersecurity risks affecting U.S. securities markets more broadly. This information could be used to address future significant cybersecurity incidents. For example, these reports could assist the Commission in identifying patterns and trends across Covered Entities, including widespread cybersecurity incidents affecting multiple Covered Entities at the same time. Further, the reports could be used to evaluate the effectiveness of various approaches to respond to and recover from a significant cybersecurity incident.

The disclosures by Covered Entities on Part II of proposed Form SCIR would be used to provide greater transparency to customers, counterparties, registrants, or members of the Covered Entity, or to users of its services, about the Covered Entity's cybersecurity risk profile. This information could be used by these persons to manage their own cybersecurity risk and, to the extent they have choice, select a Covered Entity with whom to transact or otherwise conduct business. In addition, because the reports would be filed through EDGAR, Covered Entities' customers, counterparties, members, registrants, or users would be able to run search queries to compare the disclosures of multiple Covered Entities. This would make it easier for Commission staff and others to assess the cybersecurity risk profiles of different types of Covered Entities and could facilitate trend analysis by members of the public of significant cybersecurity incidents.

2. Rules 17a-4, 17ad-7, 18a-6 and Clearing Agency Exemption Orders

Rules 17a-4, 17ad-7, and 18a-6—which apply to broker-dealers, transfer agents, and SBS Entities, respectively—would be amended to establish preservation and maintenance requirements for the written policies and procedures, annual reports, Parts I and II of proposed form SCIR, and records required to be made pursuant to proposed Rule 10 (*i.e.*, the Rule 10 Records).¹⁰¹³ The proposed

¹⁰¹³ See sections II.B.5. and II.C. of this release (discussing these proposed amendments in more

amendments would specify that the Rule 10 Records must be retained for three years. In the case of the written policies and procedures to address cybersecurity risks, the record would need to be maintained until three years after the termination of the use of the policies and procedures.¹⁰¹⁴ In addition, orders exempting certain clearing agencies from registering with the Commission would be amended to establish preservation and maintenance requirements for the Rule 10 Records that would apply to the exempt clearing agencies subject to those orders.¹⁰¹⁵ The amendments would provide that the records need to be retained for five years (consistent with Rules 13n-7 and 17a-1).¹⁰¹⁶ In the case of the written policies and procedures to address cybersecurity risks, the record would need to be maintained until five years after the termination of the use of the policies and procedures. The preservation of these records would make them available for examination by the Commission and other regulators.

B. Legal Basis

The Commission is proposing Rule 10 and Form SCIR under the Exchange Act, as well as amendments to Rules 17a-4, 17ad-7, and 18a-6 under the Exchange Act, under the following authorities under the Exchange Act: (1) Sections 15, 17, and 23 for broker-dealers (15 U.S.C. 78o, 78q, and 78w); (2) Sections 17, 17A, and 23 for clearing agencies (15 U.S.C. 78q, 17q-1, and 78w(a)(1)); (3) Sections 15B, 17, and 23 for the MSRB (15 U.S.C. 78o-4, 78q(a), and 78w); (4) Sections 6(b), 11A, 15A, 17, and 23 for national securities exchanges and national securities associations (15 U.S.C. 78f, 78k-1, 78o-3, and 78w); (5) Sections 15F, 23, and 30(c) for SBS Entities (15 U.S.C. 78o-10, 78w, and 78dd(c)); (6) Sections 13 and 23 for SBSDRs (15 U.S.C. 78m and 78w); and (7) Sections 17a, 17A, and 23 for transfer agents (78q, 17q-1, and 78w).

detail). Rule 17a-4 sets forth record preservation and maintenance requirements for broker-dealers, Rule 17ad-7 sets forth record preservation and maintenance requirements for transfer agents, and Rule 18a-6 sets forth record preservation and maintenance requirements for SBS Entities.

¹⁰¹⁴ See proposed amendments to Rule 17a-4.
¹⁰¹⁵ See section II.B.5. of this release (discussing these proposed amendments in more detail).

¹⁰¹⁶ For the reasons discussed in section II.B.5.a. of this release, the proposal would not amend Rules 13n-7 or 17a-1. As explained in that section of the release, the existing requirements of Rule 13n-7 (which applies to SBSDRs) and Rule 17a-1 (which applies to registered clearing agencies, the MSRB, national securities associations, and national securities exchanges) will require these Market Entities to retain the Rule 10 Records for five years and, in the case of the written policies and procedures, for five years after the termination of the use of the policies and procedures.

C. Small Entities Subject to Proposed Rule, Form SCIR, and Recordkeeping Rule Amendments

As discussed above, the Commission estimates that a total of approximately 1,989 Covered Entities (consisting of 1,541 broker-dealers, 16 clearing agencies, the MSRB, 25 total national securities exchanges and national securities associations, 50 SBS Entities, 3 SBSDRs, and 353 transfer agents) and 1,969 Non-Covered Broker-Dealers would be subject to the new cybersecurity requirements and related recordkeeping requirements as a result of: (1) proposed Rule 10 under the Exchange Act; (2) proposed Form SCIR; and (3) proposed amendments to Rules 17a-4, 17ad-7, and 18a-6 under the Exchange Act. The number of these firms that may be considered "small entities" are discussed below.

1. Broker-Dealers

For purposes of Commission rulemaking, a small entity includes, when used with reference to a broker-dealer, a broker-dealer that: (1) had total capital (net worth plus subordinated liabilities) of less than \$500,000 on the date in the prior fiscal year as of which its audited financial statements were prepared pursuant to Rule 17a-5(d) under the Exchange Act, or, if not required to file such statements, a broker-dealer with total capital (net worth plus subordinated liabilities) of less than \$500,000 on the last day of the preceding fiscal year (or in the time that it has been in business, if shorter); and (2) is not affiliated with any person (other than a natural person) that is not a small business or small organization.¹⁰¹⁷

Based on FOCUS Report data, the Commission estimates that as of September 30, 2022, approximately 764 broker-dealers total (195 broker-dealers that are Covered Entities and 569 broker-dealers that are Non-Covered Broker-Dealers) that might be deemed small entities for purposes of this analysis.

2. Clearing Agencies

For the purposes of Commission rulemaking, a small entity includes, when used with reference to a clearing agency, a clearing agency that: (1) compared, cleared, and settled less than \$500 million in securities transactions during the preceding fiscal year; (2) had less than \$200 million of funds and securities in its custody or control at all times during the preceding fiscal year (or at any time that it has been in business, if shorter); and (3) is not

¹⁰¹⁷ See paragraph (c) of Rule 0-10.

affiliated with any person (other than a natural person) that is not a small business or small organization.¹⁰¹⁸

Based on the Commission's existing information about the clearing agencies currently registered with the Commission, the Commission preliminarily believes that such entities exceed the thresholds defining "small entities" set out above. While other clearing agencies may emerge and seek to register as clearing agencies, the Commission preliminarily does not believe that any such entities would be "small entities" as defined in Exchange Act Rule 0–10. Consequently, the Commission certifies that the proposed rule and form would not, if adopted, have a significant economic impact on a substantial number of small entities.

3. The MSRB

The Commission's rules do not define "small business" or "small organization" for purposes of entities like the MSRB. The MSRB does not fit into one of the categories listed under the Commission rule that provides guidelines for a defined group of entities to qualify as a small entity for purposes of Commission rulemaking under the RFA.¹⁰¹⁹ The RFA in turn, refers to the Small Business Administration ("SBA") in providing that the term "small business" is defined as having the same meaning as the term "small business concern" under section 3 of the Small Business Act.¹⁰²⁰ The SBA provides a comprehensive list of categories with accompanying size standards that outline how large a business concern can be and still qualify as a small business.¹⁰²¹ The industry categorization that appears to best fit the MSRB under the SBA table is Professional Organization. The SBA defines a Professional Organization as an entity having average annual receipts of less than \$15 million. Within the MSRB's 2021 Annual Report the organization reported total revenue exceeding \$35 million for fiscal year 2021.¹⁰²² The Report also stated that the organization's total revenue for fiscal year 2020 exceeded \$47 million.¹⁰²³ The Commission is using the SBA's

definition of small business to define the MSRB for purposes of the RFA and has concluded that the MSRB is not a "small entity." Consequently, the Commission certifies that the proposed rule and form would not, if adopted, have a significant economic impact on a substantial number of small entities.

4. National Securities Exchanges and National Securities Associations

For the purposes of Commission rulemaking, and with respect to the national securities exchanges, the Commission has defined a "small entity" as an exchange that has been exempt from the reporting requirements of Rule 601 of Regulation NMS and is not affiliated with any person (other than a natural person) that is not a small business or small organization.¹⁰²⁴ None of the national securities exchanges registered under section 6 of the Exchange Act that would be subject to the proposed rule and form is a "small entity" for purposes of the RFA.

There is only one national securities association (FINRA), and the Commission has previously stated that it is not a small entity as defined by 13 CFR 121.201.¹⁰²⁵ Consequently, the Commission certifies that the proposed rule and form would not, if adopted, have a significant economic impact on a substantial number of small entities.

5. SBS Entities

For purposes of Commission rulemaking, a small entity includes: (1) when used with reference to an "issuer" or a "person," other than an investment company, an "issuer" or "person" that, on the last day of its most recent fiscal year, had total assets of \$5 million or less;¹⁰²⁶ or (2) a broker-dealer with total capital (net worth plus subordinated liabilities) of less than \$500,000 on the date in the prior fiscal year as of which its audited financial statements were prepared pursuant to Rule 17a–5(d) under the Exchange Act,¹⁰²⁷ or, if not required to file such statements, a broker-dealer with total capital (net worth plus subordinated liabilities) of less than \$500,000 on the last day of the preceding fiscal year (or in the time that it has been in business, if shorter); and is not affiliated with any person (other than a natural person) that is not a small business or small organization.¹⁰²⁸

With respect to SBS Entities, based on feedback from market participants and our information about the security-based swap markets, and consistent with our position in prior rulemakings arising out of the Dodd-Frank Act, the Commission continues to believe that: (1) the types of entities that will engage in more than a *de minimis* amount of dealing activity involving security-based swaps—which generally would be large financial institutions—would not be "small entities" for purposes of the RFA, and (2) the types of entities that may have security-based swap positions above the level required to be MSBSPs would not be "small entities" for purposes of the RFA.¹⁰²⁹

Consequently, the Commission certifies that with respect to SBS Entities the proposed rule and form (as well as the amendments to Rule 3a71–6) would not, if adopted, have a significant economic impact on a substantial number of small entities.

6. SBSDRs

For purposes of Commission rulemaking regarding SBSDRs, a small entity includes: (1) when used with reference to an "issuer" or a "person," other than an investment company, an "issuer" or "person" that, on the last day of its most recent fiscal year, had total assets of \$5 million or less;¹⁰³⁰ or (2) a broker-dealer with total capital (net worth plus subordinated liabilities) of less than \$500,000 on the date in the prior fiscal year as of which its audited financial statements were prepared pursuant to Rule 17a–5(d) under the Exchange Act,¹⁰³¹ or, if not required to file such statements, a broker-dealer with total capital (net worth plus subordinated liabilities) of less than \$500,000 on the last day of the preceding fiscal year (or in the time that it has been in business, if shorter); and is not affiliated with any person (other than a natural person) that is not a small business or small organization.¹⁰³²

Based on the Commission's existing information about the SBSDRs currently registered with the Commission, and consistent with the Commission's prior

¹⁰¹⁸ See paragraph (d) of Rule 0–10.

¹⁰¹⁹ See Rule 0–10.

¹⁰²⁰ See 5 U.S.C. 601(3).

¹⁰²¹ See 13 CFR 121.201. See also SBA, Table of Small Business Size Standards Marched to North American Industry Classification System Codes, available at https://www.sba.gov/sites/default/files/files/Size_Standards_Table.pdf (outlining the list of small business size standards within 13 CFR 121.201).

¹⁰²² See MSRB, 2021 Annual Report, 16, available at <https://msrb.org/-/media/Files/Resources/MSRB-2021-Annual-Report.ashx>.

¹⁰²³ *Id.*

¹⁰²⁴ See paragraph (e) of Rule 0–10.

¹⁰²⁵ See, e.g., Securities Exchange Act Release No. 62174 (May 26, 2010), 75 FR 32556, 32605 n.416 (June 8, 2010) ("FINRA is not a small entity as defined by 13 CFR 121.201").

¹⁰²⁶ See paragraph (a) of Rule 0–10.

¹⁰²⁷ 17 CFR 240.17a–5(d).

¹⁰²⁸ See paragraph (c) of Rule 0–10.

¹⁰²⁹ See, e.g., SBS Entity Risk Mitigation Adopting Release, 85 FR at 6411; SBS Entity Registration Adopting Release, 80 FR at 49013; Recordkeeping and Reporting Requirements for Security-Based Swap Dealers, Major Security-Based Swap Participants, and Broker-Dealers; Capital Rule for Certain Security-Based Swap Dealers, Exchange Act Release No. 71958 (Apr. 17, 2014), 79 FR 25193, 25296–97 and n.1441 (May 2, 2014); Further Definition Release, 77 FR at 30743.

¹⁰³⁰ See paragraph (a) of Rule 0–10.

¹⁰³¹ 17 CFR 240.17a–5(d).

¹⁰³² See paragraph (c) of Rule 0–10.

rulemakings,¹⁰³³ the Commission preliminarily believes that such entities exceed the thresholds defining “small entities” set out above. While other SBSDRs may emerge and seek to register as SBSDRs, the Commission preliminarily does not believe that any such entities would be “small entities” as defined in Exchange Act Rule 0–10. Consequently, the Commission certifies that the proposed rule and form would not, if adopted, have a significant economic impact on a substantial number of small entities.

7. Transfer Agents

For purposes of Commission rulemaking, Exchange Act Rule 0–10(h) provides that the term small business or small organization shall, when used with reference to a transfer agent, mean a transfer agent that: (1) received less than 500 items for transfer and less than 500 items for processing during the preceding six months (or in the time that it has been in business, if shorter); (2) transferred items only of issuers that would be deemed “small businesses” or “small organizations” as defined in this section; and (3) maintained master shareholder files that in the aggregate contained less than 1,000 shareholder accounts or was the named transfer agent for less than 1,000 shareholder accounts at all times during the preceding fiscal year (or in the time that it has been in business, if shorter); and (4) is not affiliated with any person (other than a natural person) that is not a small business or small organization under this section.¹⁰³⁴ As of March 31, 2022, the Commission estimates there were 158 transfer agents that were considered small organizations. Our estimate is based on the number of transfer agents that reported a value of fewer than 1,000 for items 4(a) and 5(a) on Form TA–2 for the 2021 annual

¹⁰³³ See, e.g., SBSDR Adopting Release, 80 FR at 14548–49 (stating that “[i]n the Proposing Release, the Commission stated that it did not believe that any persons that would register as SBSDRs would be considered small entities. The Commission stated that it believed that most, if not all, SBSDRs would be part of large business entities with assets in excess of \$5 million and total capital in excess of \$500,000. As a result, the Commission certified that the proposed rules would not have a significant impact on a substantial number of small entities and requested comments on this certification. The Commission did not receive any comments that specifically addressed whether Rules 13n–1 through 13n–12 and Form SBSDR would have a significant economic impact on small entities. Therefore, the Commission continues to believe that Rules 13n–1 through 13n–12 and Form SBSDR will not have a significant economic impact on a substantial number of small entities. Accordingly, the Commission hereby certifies that, pursuant to 5 U.S.C. 605(b), Rules 13n–1 through 13n–12, Form SBSDR will not have a significant economic impact on a substantial number of small entities”).

¹⁰³⁴ See paragraph (h) of Rule 0–10.

reporting period (which was required to be filed by March 31, 2022).¹⁰³⁵

D. Reporting, Recordkeeping, and Other Compliance Requirements

1. Proposed Rule 10 and Parts I and II of Proposed Form SCIR

The proposed requirements under proposed Rule 10 and Parts I and II of proposed Form SCIR, including compliance and recordkeeping requirements, are summarized in this IRFA.¹⁰³⁶ The burdens on respondents, including those that are small entities, are discussed above in the Commission’s economic analysis and PRA analysis.¹⁰³⁷ They also are discussed below.

As discussed above, there are approximately 764 small entity broker-dealers. 195 of these broker-dealers would be Covered Entities and 569 of these broker-dealers would be Non-Covered Broker-Dealers under proposed Rule 10. In addition, there are approximately 158 small entity transfer agents, all of which would be Covered Entities (resulting in a total of 353 small entities that would be Covered Entities). The total number of small entity broker-dealers or transfer agents that would be subject to the requirements of proposed Rule 10 as either Covered Entities or Non-Covered Broker-Dealers is 922.

The requirements under proposed Rule 10 to implement and review certain policies and procedures would result in costs to these small entities. For Covered Entities, this would create a new annual burden of approximately 31.67 hours per firm, or 11,179.51 hours in aggregate for small entities. The Commission therefore expects the annual monetized aggregate cost to small entities to be \$5,164,933.62.¹⁰³⁸ For Non-Covered Broker-Dealers, the requirements would create a new annual burden of approximately 21 hours per firm, or 11,949 hours in aggregate for small entities. The Commission therefore expects the

¹⁰³⁵ Item 4(a) on Form TA–2 requires each transfer agent to provide the number of items received for transfer during the reporting period. Item 5(a) on Form TA–2 requires each transfer agent to provide its total number of individual securityholder accounts, including accounts in the Direct Registration System (DRS), dividend reinvestment plans and/or direct purchase plans as of December 31.”

¹⁰³⁶ See section VI.A. of this release. See also section II of this release (discussing the requirements of proposed Rule 10 and Parts I and II of proposed Form SCIR in more detail).

¹⁰³⁷ See sections IV and V of this release (setting forth the Commission’s economic analysis and PRA analysis, respectively).

¹⁰³⁸ \$29,102,133.06 total cost × (353 small entities/1,989 total entities) = \$5,164,933.62.

annual monetized aggregate cost to small entities to be \$5,520,438.¹⁰³⁹

In addition, there are approximately 922 small entities that would be subject to the notification requirements of proposed Rule 10. The requirement to make a determination regarding a significant cybersecurity incident and immediate notice to the Commission would create a new annual burden of approximately 4.67 hours per Market Entity, or 4,305.74 hours in aggregate for small entities. The Commission therefore expects the annual monetized aggregate cost to small entities associated with the proposed notification requirement under Rule 10 to be \$1,519,926.22.¹⁰⁴⁰ The 353 small entities that would be Covered Entities would also be subject to the requirements to file Part I of proposed Form SCIR. This would create a new annual burden of approximately 2.5 hours per Covered Entity, or 882.5 hours in aggregate for small entities. The Commission therefore expects the annual monetized aggregate cost to small entities associated with Part I of proposed Form SCIR to be \$380,357.50.¹⁰⁴¹

In addition, the approximately 353 small entities that are Covered Entities would be subject to the disclosure requirements of proposed Rule 10. These 353 small entities would be required to make certain public disclosures on Part II of proposed Form SCIR. This would create a new annual burden of approximately 3.67 hours per Covered Entity, or 1,295.51 hours in aggregate for small entities. The Commission therefore expects the annual monetized aggregate cost to small entities associated with Part II of proposed Form SCIR to be \$486,243.38.¹⁰⁴²

Furthermore, the requirement to file Form SCIR using a form-specific XML may impose some compliance costs for entities not already required to file in EDGAR. Because all transfer agents are already required to file in EDGAR their annual reports on Form TA–2, no small entity transfer agent will incur an additional burden for filing their public disclosures in EDGAR. Assuming all 195 small broker-dealers that are Covered Entities do not already file in EDGAR, the requirement to file the public disclosures in EDGAR would create an initial, one-time burden of

¹⁰³⁹ \$19,103,238 total cost × (569 small entities/1,969 total entities) = \$5,520,438.

¹⁰⁴⁰ \$6,524,802.58 total cost × (922 small entities/3,958 total entities) = \$1,519,926.22.

¹⁰⁴¹ \$2,143,147.5 total cost × (353 small entities/1,989 total entities) = \$380,357.50.

¹⁰⁴² \$2,739,767.94 total cost × (353 small entities/1,989 total entities) = \$486,243.38.

approximately 0.30 hours per Covered Entity, or 58.5 hours in aggregate for small entities, to complete and submit a Form ID. In addition, the requirement to file Form SCIR using custom XML (with which a Covered Entity would be able to comply by inputting its disclosures into a fillable web form) would create an ongoing burden of 0.5 hours per filing, or 176.5 hours for all small entities collectively.

As discussed above, there are approximately 195 small entity broker-dealers that would be subject to the additional disclosure requirements under proposed Rule 10 for customers of Covered Broker-Dealers. This would create a new annual burden of approximately 51.26 hours per Covered Entity, or 9,995.7 hours in aggregate for small entities. The Commission therefore expects the annual monetized aggregate cost to small entities associated with the proposed disclosure requirements for Covered Broker-Dealers to be \$689,703.30.¹⁰⁴³

2. Rules 17a-4, 17ad-7, and 18a-6

The proposed amendments to Rules 17a-4, 17ad-7, and 18a-6 would impose certain recordkeeping requirements, which—with respect to 17a-4 and 17ad-7—includes requirements for those that are small entities.¹⁰⁴⁴ The proposed amendments are discussed above in detail,¹⁰⁴⁵ and the requirements and the burdens on respondents, including those that are small entities, are discussed above in the economic analysis and PRA, respectively.¹⁰⁴⁶

There are approximately 353 small entities that would be subject to the proposed amendments to Rules 17a-4 and 17ad-7 as Covered Entities. As discussed above in the PRA analysis in section V, the proposed amendments to Rules 17a-4 and 17ad-7 would require Market Entities to retain certain copies of documents required under proposed Rule 10, and would create a new annual burden of approximately 6 hours per entity, or 2,118 hours in aggregate for small entities. The Commission therefore expects the annual monetized aggregate cost to small entities associated with the proposed amendments would be \$155,673.¹⁰⁴⁷

As discussed above, there are approximately 569 small entity broker-dealers that would be subject to the proposed amendments to Rule 17a-4 as

Non-Covered Broker-Dealers. As discussed above in the PRA analysis, in section V, the proposed amendments to Rule 17a-4 would require Market Entities to retain certain copies of documents required under proposed Rule 10, which would create a new annual burden of approximately 3 hours per entity, or 1,707 hours in aggregate for small entities. The Commission therefore expects the annual monetized aggregate cost to small entities associated with the proposed amendments would be \$125,464.50.¹⁰⁴⁸

E. Duplicative, Overlapping, or Conflicting Federal Rules

1. Proposed Rule 10 and Parts I and II of Proposed Form SCIR

As discussed above certain broker-dealers—including an operator of an ATS—and transfer agents would be small entities. Proposed Rule 10 would require all Market Entities to establish, maintain, and enforce written policies and procedures that are reasonably designed to address their cybersecurity risks, and, at least annually, review and assess the design and effectiveness of these policies and procedures.¹⁰⁴⁹ As discussed earlier, broker-dealers are subject to Regulation S-P and Regulation S-ID.¹⁰⁵⁰ In addition, ATSs that trade certain stocks exceeding specific volume thresholds are subject to Regulation SCI. Further, an ATS is subject to Regulation ATS. Transfer agents registered with the Commission (but not transfer agents registered with another appropriate regulatory agency) are subject to the Regulation S-P Disposal Rule.¹⁰⁵¹ Transfer agents also may be subject to Regulation S-ID if they are “financial institutions” or “creditors.”¹⁰⁵²

As discussed earlier, these other regulations have provisions that require policies and procedures that address

¹⁰⁴⁸ \$434,164.50 total cost × (569 small entities/1,969 total entities) = \$125,464.50.

¹⁰⁴⁹ See paragraphs (b)(1) and (e)(1) of proposed Rule 10 (requiring Covered Entities and Non-Covered Broker-Dealers, respectively, to have policies and procedures to address their cybersecurity risks); sections II.B.1. and II.C.1. of this release (discussing the requirements of paragraphs (b)(1) and (e)(1) of proposed Rule 10 in more detail).

¹⁰⁵⁰ See section IV.C.1.b.i. of this release (discussing current relevant regulations applicable to broker-dealers).

¹⁰⁵¹ See section IV.C.1.b.v. of this release (discussing current relevant regulations applicable to transfer agents).

¹⁰⁵² See 17 CFR 248.201 and 202. The scope of Regulation S-ID includes any financial institution or creditor, as defined in the Fair Credit Reporting Act (15 U.S.C. 1681) that is required to be “registered under the Securities Exchange Act of 1934.” See 17 CFR 248.201(a).

certain cybersecurity risks.¹⁰⁵³ However, the policies and procedures requirements of proposed Rule 10 are intended to differ in scope and purpose from those other regulations, and because the policies and procedures required under proposed Rule 10 are consistent with the existing and proposed requirements of those other regulations that pertain to cybersecurity.

Proposed Rule 10 would require all Market Entities to give the Commission immediate written electronic notice of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring.¹⁰⁵⁴ Covered Entities—in addition to providing the Commission with immediate written electronic notice of a significant cybersecurity incident—would need to report and update information about the significant cybersecurity incident by filing Part I of proposed Form SCIR with the Commission.¹⁰⁵⁵ Recently, the OCC, Federal Reserve Board, and FDIC adopted a new rule that would require certain banking organizations to notify the appropriate banking regulator of any cybersecurity incidents within 36 hours of discovering an incident.¹⁰⁵⁶ Certain transfer agents are banking organizations and, therefore, may be required to provide notification to the Commission and other regulators under proposed Rule 10 and to their banking regulator under this new rule if they experience a significant cybersecurity incident.¹⁰⁵⁷ However, the burdens of providing these notices are minor and each requirement is designed to alert separate regulators who have oversight responsibilities with respect to transfer agents about cybersecurity incidents that could adversely impact the transfer agent.

Proposed Rule 10 would require a Covered Entity to make two types of public disclosures relating to cybersecurity on Part II of proposed

¹⁰⁵³ See section II.F.1.c. of this release.

¹⁰⁵⁴ See paragraph (c)(1) of proposed Rule 10; paragraph (e)(2) of proposed Rule 10. See also sections II.B.2.a. and II.C. of this release (discussing these proposed requirements in more detail).

¹⁰⁵⁵ See sections II.B.2. and II.B.4. of this release (discussing these proposed requirements in more detail).

¹⁰⁵⁶ See section IV.C.1.d. of this release (discussing this requirement in more detail).

¹⁰⁵⁷ Similarly, to the extent that a Covered Entity is subject to NFA rules, there may be overlapping notification requirements. See NFA Interpretive Notice 9070—NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs (effective March 1, 2016; April 1, 2019 and September 30, 2019) available at <https://www.nfa.futures.org/rulebook/rules.aspx?RuleID=9070&Section=9>.

¹⁰⁴³ \$5,450,424.54 total cost × (195 small entities/1,541 total entities) = \$689,703.30.

¹⁰⁴⁴ See section VI.A.3. of this release.

¹⁰⁴⁵ See sections II.B.5. and II.C. of this release.

¹⁰⁴⁶ See sections IV and V of the release.

¹⁰⁴⁷ \$877,149 total cost × (353 small entities/1,989 total entities) = \$155,673.

Form SCIR.¹⁰⁵⁸ Covered Entities would be required to make the disclosures by filing Part II of proposed Form SCIR on EDGAR and posting a copy of the filing on their business internet websites.¹⁰⁵⁹ In addition, a Covered Entity that is either a carrying or introducing broker-dealer would be required to provide a copy of the most recently filed Part II of Form SCIR to a customer as part of the account opening process. Thereafter, the carrying or introducing broker-dealer would need to provide the customer with the most recently filed form annually. Regulation SCI requires that SCI entities disseminate information to their members, participants, or customers (as applicable) regarding SCI events, including systems intrusions.¹⁰⁶⁰

Consequently, a Covered Entity would, if it experiences a “significant cybersecurity incident,” be required to make updated disclosures under proposed Rule 10 by filing Part II of proposed Form SCIR on EDGAR, posting a copy of the form on its business internet website, and, in the case of a carrying or introducing broker-dealer, by sending the disclosure to its customers using the same means that the customer elects to receive account statements. Moreover, if Covered Entity is an SCI entity and the significant cybersecurity incident is or would be an SCI event under the current or proposed requirements of Regulation SCI, the Covered Entity also could be required to disseminate certain information about the SCI event to certain of its members, participants, or customers (as applicable).

As discussed above, proposed Rule 10 and Regulation SCI require different types of information to be disclosed. In addition, the disclosures, for the most part, would be made to different persons: (1) the public at large in the case of proposed Rule 10;¹⁰⁶¹ and (2) affected members, participants, or customers (as applicable) of the SCI entity in the case of Regulation SCI. For these reasons, the Commission proposes to apply the disclosure requirements of proposed Rule 10 to Covered Entities even if they would be subject to the disclosure requirements of Regulation SCI.

2. Rules 17a–4, 17ad–7, 18a–6 and Clearing Agency Exemption Orders

As part of proposed Rule 10, the Commission is proposing corresponding amendments to the books and records rules for Market Entities. There are no duplicative, overlapping, or conflicting Federal rules with respect to the proposed amendments to Rules 17a–4, 17ad–7, 18a–6 and clearing agency exemption orders.

F. Significant Alternatives

The RFA directs the Commission to consider significant alternatives that would accomplish our stated objectives, while minimizing any significant adverse effect on small entities.

1. Broker-Dealers

As discussed above, the proposal would apply to all registered broker-dealers. Under the proposal, the following broker-dealers would be Covered Entities: (1) broker-dealers that maintain custody of securities and cash for customers or other broker-dealers (*i.e.*, carrying broker-dealers); (2) broker-dealers that introduce their customer accounts to a carrying broker-dealer on a fully disclosed basis (*i.e.*, introducing broker-dealers); (3) broker-dealers with regulatory capital equal to or exceeding \$50 million; (4) broker-dealers with total assets equal to or exceeding \$1 billion; (5) broker-dealers that operate as market makers; and (6) broker-dealers that operate an ATS. Broker-dealers that do not fit into at least one of these categories would not be Covered Entities (*i.e.*, they would be Non-Covered Broker-Dealers). As discussed earlier, Covered Entities would be subject to additional requirements under proposed Rule 10.¹⁰⁶²

Of the 1,541 broker-dealers that would be Covered Entities, approximately 195 are considered small entities. All but one of these small entities are broker-dealers that introduce their customer accounts to a carrying broker-dealer on a fully disclosed basis. The remaining small entity broker-dealer is an operator of an ATS. The Commission considered the following alternatives for small entities that are Covered Broker-Dealers in relation to the proposal: (1) differing compliance or reporting requirements that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance and reporting requirements

under the proposed rule for such small entities; (3) the use of design rather than performance standards; and (4) an exemption from coverage of the proposed rule, or any part thereof, for such small entities.

Regarding the first and fourth alternatives, the Commission decided not to include differing requirements or exemptions for introducing broker-dealers, regardless of size, and therefore, they would be Covered Entities under the proposed rule. This decision was based on a number of considerations.¹⁰⁶³ For example, introducing broker-dealers are a conduit to their customers’ accounts at the carrying broker-dealer and have access to information and trading systems of the carrying broker-dealer.

Consequently, a cybersecurity incident at an introducing firm could directly harm the introducing firm’s customers to the extent it causes them to lose access to the systems allowing them to view and transact in their securities accounts at the carrying broker-dealer. Further, a significant cybersecurity incident at an introducing broker-dealer could spread to the carrying broker-dealer given the information systems that connect the two firms. These connections also may make introducing broker-dealers attractive targets for threat actors seeking to access the information systems of the carrying broker-dealer to which the introducing broker-dealer is connected. In addition, introducing broker-dealers may store personal information about their customers on their information systems or be able to access this information on the carrying broker-dealer’s information systems. If this information is accessed or stolen by unauthorized users, it could result in harm (*e.g.*, identity theft or conversion of financial assets) to many individuals, including retail investors.

The Commission decided not to include differing requirements or exemptions for broker-dealers that operate an ATS, regardless of size, and therefore, they would be Covered Entities under the proposed rule. This decision was based on a number of considerations.¹⁰⁶⁴ The Commission also decided to include all broker-dealers, regardless of size, that operate an ATS as Covered Entities in the proposed rule because ATSs have become increasingly important venues for trading securities in a fast and automated manner. ATSs perform

¹⁰⁵⁸ See paragraph (d)(1) of proposed Rule 10.

¹⁰⁵⁹ See section II.B.3.b. of this release (discussing these proposed requirements in more detail).

¹⁰⁶⁰ See 17 CFR 242.1002(c).

¹⁰⁶¹ A carrying broker-dealer would be required to make the disclosures to its customers as well through the means by which they receive account statements.

¹⁰⁶² See paragraphs (b), (c), and (d) of proposed Rule 10 (setting forth the requirements for Covered Entities); paragraph (e) of proposed Rule 10 (setting forth the requirements for Non-Covered Broker-Dealers).

¹⁰⁶³ See section II.A.1.b. of this release (discussing why introducing broker-dealers would be Covered Entities in more detail).

¹⁰⁶⁴ See section II.A.1.b. of this release (discussing why broker-dealers that operate an ATS would be Covered Entities in more detail).

exchange functions to bring together buyers and sellers using limit order books and order types. These developments have made ATSs significant sources of orders and trading interest for securities. ATSs use data feeds, algorithms, and connectivity to perform their functions. In this regard, ATSs rely heavily on information systems, including to connect to other Market Entities such as other broker-dealers and principal trading firms. A significant cyber security incident that disrupts a broker-dealer that operates as an ATS could negatively impact the ability of investors to liquidate or purchase certain securities at favorable or predictable prices or in a timely manner to the extent the ATS provides liquidity to the market for those securities. Further, a significant cybersecurity incident at an ATS could provide a gateway for threat actors to attack other Market Entities that connect to it through information systems and networks of interconnected information systems. This could cause a cascading effect where a significant cybersecurity incident initially impacting an ATS spreads to other Market Entities causing major disruptions to the U.S. securities markets. In addition, ATS are connected to a number of different Market Entities through information systems, including national securities exchanges and other broker-dealers. Therefore, they create and are exposed to cybersecurity risk through the channels of these information systems.

Regarding the second alternative, the Commission believes the current proposal is clear and that further clarification, consolidation, or simplification of the compliance requirements is not necessary for small entities that are introducing broker-dealers or broker-dealers that operate as ATSs. As discussed above, proposed Rule 10 would require Covered Entities to establish, maintain, and enforce written cybersecurity policies and procedures that are reasonably designed to address their cybersecurity risks and that specifically address: (1) risk assessment; (2) user security and access; (3) information protection; (4) cybersecurity threat and vulnerability management; and (5) cybersecurity incident response and recovery.¹⁰⁶⁵ It also would require Covered Entities to conduct an annual review and assessment of these policies and procedures and produce a report documenting the review and assessment. Further, the proposed rule

would require them to provide immediate notification and subsequent reporting of significant cybersecurity incidents and to publicly disclose summary descriptions of their cybersecurity risks and, if applicable, summary descriptions of their significant cybersecurity incidents.¹⁰⁶⁶ The proposed rule would provide clarity in the existing regulatory framework regarding cybersecurity and serve as an explicit requirement for firms to establish, maintain, and enforce comprehensive cybersecurity programs to their address cybersecurity risks, provide information to the Commission about the significant cybersecurity incidents they experience, and publicly disclose information about their cybersecurity risks and significant cybersecurity incidents.

Regarding the third alternative, the Commission determined to use performance standards rather than design standards. Although the proposed rule requires Covered Entities to implement policies and procedures that are reasonably designed and that must include certain elements, the Commission does not place certain conditions or restrictions on how to establish, maintain, and enforce such policies and procedures. The general elements required to be included in the policies and procedures are designed to enumerate the core areas that firms would need to address when adopting, implementing, reassessing and updating their cybersecurity policies and procedures.

The policies and procedures that would be required by proposed Rule 10—because they would need to address the Covered Entity's cybersecurity risks—generally should be tailored to the nature and scope of the Covered Entity's business and address the Covered Entity's specific cybersecurity risks. Thus, proposed Rule 10 is not intended to impose a one-size-fits-all approach to addressing cybersecurity risks. In addition, cybersecurity threats are constantly evolving and measures to address those threats continue to evolve. Therefore, proposed Rule 10 is designed to provide Covered Entities with the flexibility to update and modify their policies and procedures as needed so that that they continue to be reasonably designed to address the Covered Entity's cybersecurity risks over time.

The remaining 569 small entity broker-dealers registered would not be Covered Entities. These firms are not

conduits to their customer accounts at a carrying broker-dealer. These firms also do not perform exchange-like functions such as offering limit order books and other order types, like an ATS would. As such, these firms are subject to differing compliance, reporting, and disclosure requirements that take into account the resources available to the entities. For example, these firms are subject to simplified requirements concerning their cybersecurity policies and procedures and annual review.¹⁰⁶⁷ In addition, these firms are exempted from the cybersecurity reporting and disclosure requirements that apply to Covered Entities.

2. Clearing Agencies

For the reasons stated above, this requirement is not applicable to clearing agencies.

3. The MSRB

For the reasons stated above, this requirement is not applicable to the MSRB.

4. National Securities Exchanges and National Securities Associations

For the reasons stated above, this requirement is not applicable to national securities exchanges and national securities associations.

5. SBS Entities

For the reasons stated above, this requirement is not applicable to SBS Entities.

6. SBSDRs

For the reasons stated above, this requirement is not applicable to SBSDRs.

7. Transfer Agents

The proposed rule would apply to every transfer agent as defined in section 3(a)(25) of the Exchange Act that is registered or required to be registered with an appropriate regulatory agency as defined in section 3(a)(34)(B) of the Exchange Act. As of December 31, 2022, there were 353 transfer agents that were either registered with the Commission through Form TA-1 or registered with

¹⁰⁶⁷ Non-Covered Broker-Dealers that are small entities are not, however, altogether exempted from the policies and procedures requirements because having appropriate cybersecurity policies and procedures in place would help address any cybersecurity risks and incidents that occur at the broker-dealer and help protect broker-dealers and their customers from greater risk of harm. The Commission anticipates that these benefits should apply to customers of smaller firms as well as larger firms. Non-Covered Broker-Dealers are also not exempted from the requirement to provide the Commission with immediate written electronic notice of a significant cybersecurity incident affecting the entity.

¹⁰⁶⁵ See paragraph (b) of proposed Rule 10. See also section II.B.1. of this release (discussing these requirements in more detail).

¹⁰⁶⁶ See paragraphs (c) and (d) of proposed Rule 10. See also sections II.B.2. through II.B.4. of this release (discussing these requirements in more detail).

other appropriate regulatory agencies through Form TA–2. As of March 31, 2022, the Commission estimates there were 158 transfer agents that were considered small organizations.

The Commission considered the following alternatives for small organizations that are transfer agents in relation to the proposal: (1) differing compliance or reporting requirements that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance and reporting requirements under the proposed rule for such small entities; (3) the use of design rather than performance standards; and (4) an exemption from coverage of the proposed rule, or any part thereof, for such small entities.

Regarding the first and fourth alternatives, the Commission decided not to include differing requirements or exemptions for transfer agents, regardless of size, and therefore, they would be Covered Entities under the proposed rule. This decision was based on a number of considerations.¹⁰⁶⁸ A transfer agent engages on behalf of an issuer of securities or on behalf of itself as an issuer of securities in (among other functions): (1) tracking, recording, and maintaining the official record of ownership of each issuer's securities; (2) canceling old certificates, issuing new ones, and performing other processing and recordkeeping functions that facilitate the issuance, cancellation, and transfer of those securities; (3) facilitating communications between issuers and registered securityholders; and (4) making dividend, principal, interest, and other distributions to securityholders. Their core recordkeeping systems provide a direct conduit to their issuer clients' master records that document and, in many instances provide the legal underpinning for, registered securityholders' ownership of the issuer's securities. If these functions were disrupted, investors might not be able to transfer ownership of their securities or receive dividends and interest due on their securities positions.

Transfer agents store proprietary information about securities ownership and corporate actions. A significant cybersecurity incident at a transfer agent could lead to the improper use of this information to harm securities holders (e.g., public exposure of confidential financial information) or provide the

unauthorized user with an unfair advantage over other market participants (e.g., trading based on confidential business information). Transfer agents also may store personal information including names, addresses, phone numbers, email addresses, employers, employment history, bank and specific account information, credit card information, transaction histories, securities holdings, and other detailed and individualized information related to the transfer agents' recordkeeping and transaction processing on behalf of issuers. Threat actors breaching the transfer agent's information systems could use this information to steal identities or financial assets of the persons to whom this information pertains. They also could sell it to other threat actors.

Regarding the second alternative, the Commission is not proposing further clarification, consolidation, or simplification of the compliance requirements for small organizations that are transfer agents. As discussed above, proposed Rule 10 would require Covered Entities to establish, maintain, and enforce written cybersecurity policies and procedures that are reasonably designed to address their cybersecurity risks and that specifically address: (1) risk assessment; (2) user security and access; (3) information protection; (4) cybersecurity threat and vulnerability management; and (5) cybersecurity incident response and recovery.¹⁰⁶⁹ It also would require Covered Entities to conduct an annual review and assessment of these policies and procedures and produce a report documenting the review and assessment. Further, the proposed rule would require them to provide immediate notification and subsequent reporting of significant cybersecurity incidents and to publicly disclose summary descriptions of their cybersecurity risks and, if applicable, summary descriptions of their significant cybersecurity incidents.¹⁰⁷⁰ The proposed rule would provide clarity in the existing regulatory framework regarding cybersecurity and serve as an explicit requirement for firms to establish, maintain, and enforce comprehensive cybersecurity programs to their address cybersecurity risks, provide information to the Commission about the significant cybersecurity incidents they experience, and publicly

disclose information about their cybersecurity risks and significant cybersecurity incidents.

Regarding the third alternative, the proposed rule requires Covered Entities to implement policies and procedures that are reasonably designed and that must include certain elements. However, the proposed rule does not place certain conditions or restrictions on how to establish, maintain, and enforce such policies and procedures. The general elements required to be included in the policies and procedures are designed to enumerate the core areas that firms would need to address when adopting, implementing, reassessing and updating their cybersecurity policies and procedures.

The policies and procedures that would be required by proposed Rule 10—because they would need to address the Covered Entity's cybersecurity risks—generally should be tailored to the nature and scope of the Covered Entity's business and address the Covered Entity's specific cybersecurity risks. Thus, proposed Rule 10 is not intended to impose a one-size-fits-all approach to addressing cybersecurity risks. In addition, cybersecurity threats are constantly evolving and measures to address those threats continue to evolve. Therefore, proposed Rule 10 is designed to provide Covered Entities with the flexibility to update and modify their policies and procedures as needed so that they continue to be reasonably designed to address the Covered Entity's cybersecurity risks over time.

G. Request for Comment

The Commission encourages written comments on the matters discussed in this IRFA. The Commission solicits comment on the number of small entities subject to the proposed Rule 10, Form SCIR, and proposed amendments to Rules 3a71–6, 17a–4, 18a–6, and 17ad–7. The Commission also solicits comment on the potential effects discussed in this analysis; and whether this proposal could have an effect on small entities that have not been considered. The Commission requests that commenters describe the nature of any effect on small entities and provide empirical data to support the extent of such effect. Such comments will be placed in the same public file as comments on the proposed rule and form and associated amendments. Persons wishing to submit written comments should refer to the instructions for submitting comments located at the front of this release.

¹⁰⁶⁸ See section II.A.1.c. of this release (discussing why transfer agents would be Covered Entities in more detail).

¹⁰⁶⁹ See paragraph (b) of proposed Rule 10. See also section II.B.1. of this release (discussing these requirements in more detail).

¹⁰⁷⁰ See paragraphs (c) and (d) of proposed Rule 10. See also sections II.B.2. through II.B.4. of this release (discussing these requirements in more detail).

VII. Small Business Regulatory Enforcement Fairness Act

For purposes of the Small Business Regulatory Enforcement Fairness Act of 1996, or "SBREFA," the Commission must advise OMB whether a proposed regulation constitutes a "major" rule. Under SBREFA, a rule is considered "major" where, if adopted, it results in or is likely to result in (1) an annual effect on the economy of \$100 million or more; (2) a major increase in costs or prices for consumers or individual industries; or (3) significant adverse effects on competition, investment or innovation. The Commission requests comment on the potential effect of the proposed amendments on the U.S. economy on an annual basis; any potential increase in costs or prices for consumers or individual industries; and any potential effect on competition, investment or innovation. Commenters are requested to provide empirical data and other factual support for their views to the extent possible.

VIII. Statutory Authority

The Commission is proposing new Rule 10 (17 CFR 242.10) and Form SCIR (17 CFR 249.624) and amending Regulation S-T (17 CFR 232.101), Rule 3a71-6 (17 CFR 240.3a71-6), Rule 17a-4 (17 CFR 240.17a-4), Rule 17ad-7 (17 CFR 240.17ad-7), Rule 18a-6 (17 CFR 240.18a-6), and Rule 18a-10 (17 CFR 240.18a-10) under the Commission's rulemaking authority set forth in the following sections of the Exchange Act: (1) sections 15, 17, and 23 for broker-dealers (15 U.S.C. 78o, 78q, and 78w); (2) sections 17, 17A, and 23 for clearing agencies (15 U.S.C. 78q, 17q-1, and 78w(a)(1)); (3) sections 15B, 17 and 23 for the MSRB (15 U.S.C. 78o-4, 78q(a), and 78w); (4) sections 6(b), 11A, 15A, 17, and 23 for national securities exchanges and national securities associations (15 U.S.C. 78f, 78k-1, 78o-3, and 78w); (5) sections 15F, 23, and 30(c) for SBS Entities (15 U.S.C. 78o-10, 78w, and 78dd(c)); (6) sections 13 and 23 for SBSDRs (15 U.S.C. 78m and 78w); and (7) sections 17a, 17A, and 23 for transfer agents (78q, 17q-1, and 78w).

List of Subjects in 17 CFR Part 232, 240, 242 and 249

Brokers, Confidential business information, Reporting and recordkeeping requirements, Securities, Security-based swaps, Security-based swap dealers, Major security-based swap participants.

Text of Proposed Rules and Rule Amendments

For the reasons set out in the preamble, the Commission is proposing

to amend title 17, chapter II of the Code of Federal Regulations as follows:

PART 232—REGULATION S-T—GENERAL RULES AND REGULATIONS FOR ELECTRONIC FILINGS

1. The general authority citation for part 232 is revised to read as follows:

Authority: 15 U.S.C. 77c, 77f, 77g, 77h, 77j, 77s(a), 77z-3, 77sss(a), 78c(b), 78l, 78m, 78n, 78o(d), 78o-10, 78w(a), 78ll, 80a-6(c), 80a-8, 80a-29, 80a-30, 80a-37, 80b-4, 80b-10, 80b-11, 7201 et seq.; and 18 U.S.C. 1350, unless otherwise noted.

* * * * *

2. Section § 232.101 is amended by revising paragraph (a)(1)(xxx) and adding paragraph (a)(1)(xxxi) to read as follows:

§ 232.101 Mandated electronic submissions and exceptions.

(a) * * *

(1) * * *

(xxx) Documents filed with the Commission pursuant to section 33 of the Investment Company Act (15 U.S.C. 80a-32); and

(xxxi) Form SCIR (§ 249.624 of this chapter).

* * * * *

PART 240—GENERAL RULES AND REGULATIONS, SECURITIES EXCHANGE ACT OF 1934

3. The authority citation for part 240 continues to read, in part, as follows:

Authority: 15 U.S.C. 77c, 77d, 77g, 77j, 77s, 77z-2, 77z-3, 77eee, 77ggg, 77nnn, 77sss, 77ttt, 78c, 78c-3, 78c-5, 78d, 78e, 78f, 78g, 78i, 78j, 78j-1, 78k, 78k-1, 78l, 78m, 78n, 78n-1, 78o, 78o-4, 78o-10, 78p, 78q, 78q-1, 78s, 78u-5, 78w, 78x, 78ll, 78mm, 80a-20, 80a-23, 80a-29, 80a-37, 80b-3, 80b-4, 80b-11, and 7201 et. seq., and 8302; 7 U.S.C. 2(c)(2)(E); 12 U.S.C. 5221(e)(3); 18 U.S.C. 1350; Pub. L. 111-203, 939A, 124 Stat. 1376 (2010); and Pub. L. 112-106, sec. 503 and 602, 126 Stat. 326 (2012), unless otherwise noted.

* * * * *

4. Section 240.3a71-6 is amended by revising paragraph (d)(1) to read as follows:

§ 240.3a71-6 Substituted compliance for security-based swap dealers and major security-based swap participants.

* * * * *

(d) * * *

(1) Business conduct, supervision, and risk management. The business conduct and supervision requirements of sections 15F(h) and (j) of the Act (15 U.S.C. 78o-10(h) and (j)) and §§ 240.15Fh-3 through 15Fh-6 (other than the antifraud provisions of section 15F(h)(4)(A) of the Act and § 240.15Fh-4(a), and other than the provisions of

sections 15F(j)(3) and 15F(j)(4)(B) of the Act), and the requirements of § 242.10 of this chapter and Form SCIR (§ 249.624 of this chapter); provided, however, that prior to making such a substituted compliance determination the Commission intends to consider whether the information that is required to be provided to counterparties pursuant to the requirements of the foreign financial regulatory system, the counterparty protections under the requirements of the foreign financial regulatory system, the mandates for supervisory systems under the requirements of the foreign financial regulatory system, and the duties imposed by the foreign financial regulatory system, are comparable to those associated with the applicable provisions arising under the Act and its rules and regulations.

* * * * *

5. Section 240.17a-4 is amended by adding paragraph (e)(13) to read as follows:

§ 240.17a-4 Records to be preserved by certain exchange members, brokers and dealers.

* * * * *

(e) * * *

(13)(i) The written policies and procedures required to be adopted and implemented pursuant to § 242.10(b)(1) or § 242.10(e)(1) of this chapter until three years after the termination of the use of the policies and procedures;

(ii) The written documentation of any risk assessment pursuant to § 242.10(b)(1)(i)(B) of this chapter for three years;

(iii) The written documentation of the occurrence of a cybersecurity incident pursuant to § 242.10(b)(1)(v)(B) of this chapter, including any documentation related to any response and recovery from such an incident, for three years;

(iv) The written report of the annual review required to be prepared pursuant to § 242.10(b)(2)(ii) of this chapter or the record of the annual review required pursuant to § 240.10(e)(1) for three years;

(v) A copy of any notice transmitted to the Commission pursuant to § 242.10(c)(1) or § 240.10(e)(2) of this chapter or any Part I of Form SCIR filed with the Commission pursuant to § 242.10(c)(2) of this chapter for three years; and

(vi) A copy of any Part II of Form SCIR filed with the Commission pursuant to § 242.10(d) of this chapter for three years.

* * * * *

6. Redesignate § 240.17Ad-7 as § 240.17ad-7.

■ 7. Newly redesignated § 240.17ad–7 is amended by revising the section heading, and adding paragraph (j) to read as follows:

§ 240.17ad–7 (Rule 17Ad–7) Record retention.

* * * * *

(j)(1) The written policies and procedures required to be adopted and implemented pursuant to § 242.10(b)(1) of this chapter until three years after the termination of the use of the policies and procedures;

(2) The written documentation of any risk assessment pursuant to § 242.10(b)(1)(i)(B) of this chapter for three years;

(3) The written documentation of the occurrence of a cybersecurity incident pursuant to § 242.10(b)(1)(v)(B) of this chapter, including any documentation related to any response and recovery from such an incident, for three years;

(4) The written report of the annual review required to be prepared pursuant to § 242.10(b)(2)(ii) of this chapter for three years;

(5) A copy of any notice transmitted to the Commission and any ARA pursuant to § 242.10(c)(1) of this chapter or any Part I of Form SCIR filed with the Commission pursuant to § 240.2.10(c)(2) for three years; and

(6) A copy of any Part II of Form SCIR filed with the Commission pursuant to § 240.2.10(d) for three years.

■ 8. Section 240.18a–6 is amended by adding paragraph (d)(6) to read as follows:

§ 240.18a–6 Records to be preserved by certain security-based swap dealers and major security-based swap participants

* * * * *

(d) * * *

(6)(i) The written policies and procedures required to be adopted and implemented pursuant to § 242.10(b)(1) of this chapter until three years after the termination of the use of the policies and procedures;

(ii) The written documentation of any risk assessment pursuant to § 242.10(b)(1)(i)(B) of this chapter for three years;

(iii) The written documentation of the occurrence of a cybersecurity incident pursuant to § 242.10(b)(1)(v)(B) of this chapter, including any documentation related to any response and recovery from such an incident, for three years;

(iv) The written report of the annual review required to be prepared pursuant to § 242.10(b)(2)(ii) of this chapter for three years;

(v) A copy of any notice transmitted to the Commission pursuant to § 242.10(c)(1) of this chapter or any Part

I of Form SCIR filed with the Commission pursuant to § 242.10(c)(2) of this chapter for three years; and

(vi) A copy of any Part II of Form SCIR filed with the Commission pursuant to § 242.10(d) of this chapter for three years.

* * * * *

■ 9. Section 240.18a–10 is amended by adding paragraph (g) to read as follows:

§ 240.18a–10 Alternative compliance mechanism for security-based swap dealers that are registered as swap dealers and have limited security-based swap activities

* * * * *

(g) The provisions of this section do not apply to the record maintenance and preservation requirements § 240.18a–6(d)(6)(i) through (vi).

PART 242—REGULATIONS M, SHO, ATS, AC, NMS, AND SBSR AND CUSTOMER MARGIN REQUIREMENTS FOR SECURITY FUTURES

■ 10. The general authority citation for part 242 is revised to read as follows:

Authority: 15 U.S.C. 77g, 77q(a), 77s(a), 78b, 78c, 78g(c)(2), 78i(a), 78j, 78k–1(c), 78l, 78m, 78n, 78o(b), 78o(c), 78o(g), 78o–10, 78q(a), 78q(b), 78q(h), 78w(a), 78dd–1, 78mm, 80a–23, 80a–29, and 80a–37.

■ 11. Section 242.10 is added to read as follows:

§ 242.10 Cybersecurity requirements.

(a) *Definitions:* For purposes of this section:

(1) *Covered entity* means:

(i) A broker or dealer registered with the Commission that:

(A) Maintains custody of cash and securities for customers or other brokers or dealers and is not exempt from the requirements of § 240.15c3–3 of this chapter;

(B) Introduces customer accounts on a fully disclosed basis to another broker or dealer described in paragraph (a)(1)(i)(A) of this section;

(C) Has regulatory capital equal to or exceeding \$50 million;

(D) Has total assets equal to or exceeding \$1 billion;

(E) Is a market maker under the Securities Exchange Act of 1934 (15 U.S.C. 78a, *et seq.*) (“Act”) or the rules thereunder (which includes a broker or dealer that operates pursuant to § 240.15c3–1(a)(6) of this chapter) or is a market maker under the rules of a self-regulatory organization of which the broker or dealer is a member; or

(F) Operates an alternative trading system as defined in § 242.300(a) or operates an NMS Stock ATS as defined in § 242.300(k).

(ii) A clearing agency (registered or exempt) under section 3(a)(23)(A) of the Act.

(iii) A major security-based swap participant registered pursuant to section 15F(b) of the Act.

(iv) The Municipal Securities Rulemaking Board.

(v) A national securities association registered under section 15A of the Act.

(vi) A national securities exchange registered under section 6 of the Act.

(vii) A security-based swap data repository under section 3(a)(75) of the Act.

(viii) A security-based swap dealer registered pursuant to section 15F(b) of the Act.

(ix) A transfer agent as defined in section 3(a)(25) of the Act that is registered or required to be registered with an appropriate regulatory agency as defined in section 3(a)(34)(B) of the Act (hereinafter also “ARA”).

(2) *Cybersecurity incident* means an unauthorized occurrence on or conducted through a market entity’s information systems that jeopardizes the confidentiality, integrity, or availability of the information systems or any information residing on those systems.

(3) *Cybersecurity risk* means financial, operational, legal, reputational, and other adverse consequences that could result from cybersecurity incidents, cybersecurity threats, and cybersecurity vulnerabilities.

(4) *Cybersecurity threat* means any potential occurrence that may result in an unauthorized effort to affect adversely the confidentiality, integrity, or availability of a market entity’s information systems or any information residing on those systems.

(5) *Cybersecurity vulnerability* means a vulnerability in a market entity’s information systems, information system security procedures, or internal controls, including, for example, vulnerabilities in their design, configuration, maintenance, or implementation that, if exploited, could result in a cybersecurity incident.

(6) *Information* means any records or data related to the market entity’s business residing on the market entity’s information systems, including, for example, personal information received, maintained, created, or processed by the market entity.

(7) *Information systems* means the information resources owned or used by the market entity, including, for example, physical or virtual infrastructure controlled by the information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the

covered entity's information to maintain or support the covered entity's operations.

(8) *Market Entity* means a "covered entity" as defined in this section and a broker or dealer registered with the Commission that is not a "covered entity" as defined in this section.

(9) *Personal information* means any information that can be used, alone or in conjunction with any other information, to identify a person, including, but not limited to, name, date of birth, place of birth, telephone number, street address, mother's maiden name, Social Security number, government passport number, driver's license number, electronic mail address, account number, account password, biometric records, or other non-public authentication information.

(10) *Significant cybersecurity incident* means a cybersecurity incident, or a group of related cybersecurity incidents, that:

(i) Significantly disrupts or degrades the ability of the market entity to maintain critical operations; or

(ii) Leads to the unauthorized access or use of the information or information systems of the market entity, where the unauthorized access or use of such information or information systems results in or is reasonably likely to result in:

(A) Substantial harm to the market entity; or

(B) Substantial harm to a customer, counterparty, member, registrant, or user of the market entity, or to any other person that interacts with the market entity.

(b)(1) *Cybersecurity policies and procedures*. A covered entity must establish, maintain, and enforce written policies and procedures that are reasonably designed to address the covered entity's cybersecurity risks, including policies and procedures that:

(i)(A) *Risk assessment*. Require periodic assessments of cybersecurity risks associated with the covered entity's information systems and information residing on those systems, including requiring the covered entity to:

(1) Categorize and prioritize cybersecurity risks based on an inventory of the components of the covered entity's information systems and information residing on those systems and the potential effect of a cybersecurity incident on the covered entity; and

(2) Identify the covered entity's service providers that receive, maintain, or process information, or are otherwise permitted to access the covered entity's information systems and any of the

covered entity's information residing on those systems, and assess the cybersecurity risks associated with the covered entity's use of these service providers.

(B) Require written documentation of the risk assessments.

(ii) *User security and access*. Require controls designed to minimize user-related risks and prevent unauthorized access to the covered entity's information systems and the information residing on those systems, including:

(A) Requiring standards of behavior for individuals authorized to access the covered entity's information systems and the information residing on those systems, such as an acceptable use policy;

(B) Identifying and authenticating individual users, including but not limited to implementing authentication measures that require users to present a combination of two or more credentials for access verification;

(C) Establishing procedures for the timely distribution, replacement, and revocation of passwords or methods of authentication;

(D) Restricting access to specific information systems of the covered entity or components thereof and the information residing on those systems solely to individuals requiring access to the systems and information as is necessary for them to perform their responsibilities and functions on behalf of the covered entity; and

(E) Securing remote access technologies.

(iii) *Information protection*. (A) Require measures designed to monitor the covered entity's information systems and protect the information residing on those systems from unauthorized access or use, based on a periodic assessment of the covered entity's information systems and the information that resides on the systems that takes into account:

(1) The sensitivity level and importance of the information to the covered entity's business operations;

(2) Whether any of the information is personal information;

(3) Where and how the information is accessed, stored and transmitted, including the monitoring of information in transmission;

(4) The information systems' access controls and malware protection; and

(5) The potential effect a cybersecurity incident involving the information could have on the covered entity and its customers, counterparties, members, or users, including the potential to cause a significant cybersecurity incident.

(B) Require oversight of service providers that receive, maintain, or

process the covered entity's information, or are otherwise permitted to access the covered entity's information systems and the information residing on those systems, pursuant to a written contract between the covered entity and the service provider, through which the service providers are required to implement and maintain appropriate measures, including the practices described in paragraphs (b)(1)(i) through (v) of this section, that are designed to protect the covered entity's information systems and information residing on those systems.

(iv) *Cybersecurity threat and vulnerability management*. Require measures designed to detect, mitigate, and remediate any cybersecurity threats and vulnerabilities with respect to the covered entity's information systems and the information residing on those systems;

(v) *Cybersecurity incident response and recovery*. (A) Require measures designed to detect, respond to, and recover from a cybersecurity incident, including policies and procedures that are reasonably designed to ensure:

(1) The continued operations of the covered entity;

(2) The protection of the covered entity's information systems and the information residing on those systems;

(3) External and internal cybersecurity incident information sharing and communications; and

(4) The reporting of significant cybersecurity incidents pursuant to paragraph (c) of this section.

(B) Require written documentation of any cybersecurity incident, including the covered entity's response to and recovery from the cybersecurity incident.

(2) *Annual Review*. A covered entity must, at least annually:

(i) Review and assess the design and effectiveness of the cybersecurity policies and procedures required by paragraph (b)(1) of this section, including whether the policies and procedures reflect changes in cybersecurity risk over the time period covered by the review; and

(ii) Prepare a written report that describes the review, the assessment, and any control tests performed, explains their results, documents any cybersecurity incident that occurred since the date of the last report, and discusses any material changes to the policies and procedures since the date of the last report.

(c) *Notification and reporting of significant cybersecurity incidents*—(1) *Immediate notice*. A covered entity must give the Commission immediate

written electronic notice of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring. The notice must identify the covered entity, state that the notice is being given to alert the Commission of a significant cybersecurity incident impacting the covered entity, and provide the name and contact information of an employee of the covered entity who can provide further details about the significant cybersecurity incident. The notice also must be given to:

(i) In the case of a broker or dealer, the examining authority of the broker or dealer; and

(ii) In the case of a transfer agent, the ARA of the transfer agent.

(2) *Report.* (i) A covered entity must report a significant cybersecurity incident, promptly, but no later than 48 hours, upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring by filing Part I of Form SCIR with the Commission electronically through the Electronic Data Gathering, Analysis, and Retrieval System (“EDGAR system”) in accordance with the EDGAR Filer Manual, as defined in Rule 11 of Regulation S–T (17 CFR 232.11), and Part I of Form SCIR must be filed in accordance with the requirements of Regulation S–T.

(ii) A covered entity must file an amended Part I of Form SCIR with the Commission electronically through the EDGAR system in accordance with the EDGAR Filer Manual, as defined in Rule 11 of Regulation S–T (17 CFR 232.11), and Part I of Form SCIR must be filed in accordance with the requirements of Regulation S–T promptly, but no later than 48 hours after each of the following circumstances:

(A) Any information previously reported to the Commission on Part I of Form SCIR pertaining to a significant cybersecurity incident becoming materially inaccurate;

(B) Any new material information pertaining to a significant cybersecurity incident previously reported to the Commission on Part I of Form SCIR being discovered;

(C) A significant cybersecurity incident is resolved; or

(D) An internal investigation pertaining to a significant cybersecurity incident is closed.

(iii)(A) If the covered entity is a broker or dealer, it must promptly transmit a copy of each Part I of Form SCIR it files with the Commission to its examining authority; and

(B) If the covered entity is a transfer agent, it must promptly transmit a copy of each Part I of Form SCIR it files with the Commission to its ARA.

(d) *Disclosure of cybersecurity risks and incidents*—(1) *Content of the disclosure*—(i) *Cybersecurity risks.* A covered entity must provide a summary description of the cybersecurity risks that could materially affect the covered entity’s business and operations and how the covered entity assesses, prioritizes, and addresses those cybersecurity risks.

(ii) *Significant cybersecurity incidents.* A covered entity must provide a summary description of each significant cybersecurity incident that has occurred during the current or previous calendar year. The description of each significant cybersecurity incident must include the following information to the extent known:

(A) The person or persons affected;

(B) The date the incident was discovered and whether it is ongoing;

(C) Whether any data was stolen, altered, or accessed or used for any other unauthorized purpose;

(D) The effect of the incident on the covered entity’s operations; and

(E) Whether the covered entity, or service provider, has remediated or is currently remediating the incident.

(2) *Methods of disclosure.* A covered entity must make the disclosures required pursuant to paragraph (d)(1) of this section by:

(i) Filing Part II of Form SCIR with the Commission electronically through the EDGAR system in accordance with the EDGAR Filer Manual, as defined in Rule 11 of Regulation S–T (17 CFR 232.11), and in accordance with the requirements of Regulation S–T; and

(ii) Posting a copy of the Part II of Form SCIR most recently filed pursuant to paragraph (d)(2)(i) of this section on an easily accessible portion of its business internet website that can be viewed by the public without the need of entering a password or making any type of payment or providing any other consideration.

(3) *Additional methods of disclosure required for certain brokers or dealers.* In addition to the method of disclosure required by paragraph (d)(2) of this section, a broker or dealer described in paragraph (a)(1)(i) or (ii) of this section must provide a copy of the Part II of Form SCIR most recently filed pursuant to paragraph (d)(2)(i) of this section to a customer as part of the account opening process and, thereafter, annually and as required by paragraph (d)(4) of this section using the same means that the customer elects to receive account statements.

(4) *Disclosure updates.* The covered entity must promptly provide an updated disclosure through the methods required by paragraphs (d)(2) and (3) of this section if the information required to be disclosed pursuant to paragraphs (d)(1)(i) or (ii) of this section materially changes, including, in the case of paragraph (d)(1)(ii) of this section, after the occurrence of a new significant cybersecurity incident or when information about a previously disclosed significant cybersecurity incident materially changes.

(e) *Requirements for brokers or dealers that are not covered entities.* (1) A broker or dealer that is not a “covered entity” as defined in this section must establish, maintain, and enforce written policies and procedures that are reasonably designed to address the cybersecurity risks of the broker or dealer taking into account the size, business, and operations of the broker or dealer. The broker or dealer must annually review and assess the design and effectiveness of the cybersecurity policies and procedures, including whether the policies and procedures reflect changes in cybersecurity risk over the time period covered by the review. The broker or dealer must make a written record that documents the steps taken in performing the annual review and the conclusions of the annual review.

(2) A broker or dealer that is not a “covered entity” as defined in this section must give the Commission immediate written electronic notice of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring. The notice must identify the broker or dealer, state that the notice is being given to alert the Commission of a significant cybersecurity incident impacting the broker or dealer, and provide the name and contact information of an employee of the broker or dealer who can provide further details about the significant cybersecurity incident. The notice also must be given to the examining authority of the broker or dealer.

* * * * *

PART 249—FORMS, SECURITIES EXCHANGE ACT OF 1934

■ 12. The authority citation for part 249 continues to read, in part, as follows:

Authority: 15 U.S.C. 78a, *et seq.*, unless otherwise noted.

* * * * *

■ 13. Section 249.624 is added to read as follows:

§ 249.624 Form SCIR.

Form SCIR shall be filed by a covered entity to report a significant

cybersecurity incident pursuant to the requirements of 17 CFR 242.10.

By the Commission.

Dated: March 15, 2023.

J. Matthew DeLesDernier,
Deputy Secretary.

BILLING CODE 8011-01-P

Note: The following appendix will not appear in the Code of Federal Regulations.

Form SCIR

Significant Cybersecurity Incidents and Risks

OMB Approval	
OMB Number:	[•]
Expires:	[•]
Estimated average burden hours	
per response:	[•]
per amendment:	[•]

FORM SCIR INSTRUCTIONS**A. GENERAL INSTRUCTIONS**

1. **FORM** – Part I of Form SCIR must be used by a covered entity to confidentially report a cybersecurity incident pursuant to the requirements of 17 CFR 242.10. Part II of Form SCIR must be used to publicly disclose cybersecurity risks and significant cybersecurity incidents pursuant to the requirements of 17 CFR 242.10.
2. **ELECTRONIC FILING** - A covered entity must file Parts I and II of Form SCIR through the EDGAR system, and must utilize the EDGAR Filer Manual (as defined in 17 CFR 232.11) to file Parts I and II of Form SCIR electronically to assure the timely acceptance and processing of the filing. Refer to 17 CFR 242.10 for other requirements with respect to filing Part I of Form SCIR with other regulators and for other requirements with respect to publicly disclosing Part II of Form SCIR.
3. **FEDERAL INFORMATION LAW AND REQUIREMENTS** - An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid control number. Sections 15F, 17(a), 17A, and 23(a) of the Exchange Act authorize the U.S. Securities and Exchange Commission (“Commission”) to collect the information on Form SCIR from covered entities. See 15 U.S.C. §§78o-10, 78q and 78w. Filing of Parts I and II Form SCIR is mandatory. The principal purpose of Part I of Form SCIR is to report information about a significant cybersecurity incident impacting a covered entity so the Commission can respond to the incident, evaluate the operating status of the covered entity, and assess the impact the significant cybersecurity incident may have on other participants in the U.S. securities markets. The principal purpose of Part II of Form SCIR is to publicly disclose summary descriptions of the cybersecurity risks of the covered entity and summary descriptions of each significant cybersecurity incident that covered entity has experienced in the current or previous calendar year (if applicable). Any member of the public may direct to the Commission any comments concerning the accuracy of the burden estimate on this form, and any suggestions for reducing this burden. This collection of information has been reviewed by the Office of Management and Budget in accordance with the clearance requirements of 44 U.S.C. §3507. The information contained in this form is part of a system of records subject to the Privacy Act of 1974, as amended. The Commission has published in the Federal Register the Privacy Act Systems of Records Notice for these records.
4. **FORMAT**
 - a. All Items must be answered and all fields requiring a response must be completed before the filing will be accepted.
 - b. A covered entity must complete the execution screen certifying that Form SCIR has been executed properly and that the information contained in the form is accurate and complete before the filing will be accepted.
 - c. A paper copy, with original signatures, of Part I and Part II of Form SCIR must be retained by the covered entity and be made available for inspection upon a regulatory request.
5. **EXPLANATION OF TERMS**
 - a. **COVERED ENTITY** – The term “covered entity” has the same meaning as that term is defined in 17 CFR 242.10 and, as used in Form SCIR, also refers to the person filing the Form.
 - b. **CYBERSECURITY INCIDENT** – The term “cybersecurity incident” has the same meaning as that term is defined in 17 CFR 242.10.
 - c. **CYBERSECURITY RISK** – The term “cybersecurity risk” has the same meaning as that term is defined in 17 CFR 242.10.
 - d. **INTERNAL INVESTIGATION** – The term “internal investigation” means a formal investigation of the significant cybersecurity incident by internal personnel of the covered entity or external personnel hired by the covered entity that seeks to determine any of the following: the cause of the significant cybersecurity incident; whether there was a failure to adhere to the covered entity’s policies and procedures to address cybersecurity risk; or whether the covered entity’s policies and procedures to address cybersecurity risk are effective.

- e. **PERSONAL INFORMATION** – The term “personal information” has the same meaning as that term is defined in 17 CFR 242.10].
- f. **SIGNIFICANT CYBERSECURITY INCIDENT** – The term “significant cybersecurity incident” has the same meaning as that term is defined in 17 CFR 242.10.
- g. **UNIQUE IDENTIFICATION CODE** – The term “unique identification code” means a unique identification code assigned to a person by an internationally recognized standards-setting system that is recognized by the Commission pursuant to Rule 903(a) of Regulation SBSR (17 CFR 242.903(a)).

B. INSTRUCTIONS TO PART I OF FORM SCIR

1. **INITIAL REPORT** - Pursuant to the requirements of 17 CFR 242.10, a covered entity must file an initial report on Part I of Form SCIR with respect to a significant cybersecurity incident upon having a reasonable basis to conclude that the incident has occurred or is occurring.
2. **AMENDED REPORT** - Pursuant to the requirements of 17 CFR 242.10, a covered entity must file an amended report on Part I of Form SCIR with respect to a significant cybersecurity incident after each of the following circumstances:
 - Any information on a previously filed Part I of Form SCIR pertaining to the significant cybersecurity incident becomes materially inaccurate;
 - Any new material information pertaining to a significant cybersecurity incident previously reported to the Commission on Part I of Form SCIR being discovered;
 - A significant cybersecurity incident is resolved; or
 - An internal investigation pertaining to a significant cybersecurity incident is closed.
3. **FINAL REPORT** - A covered entity filing a final report on Part I of Form SCIR must indicate on the final notification if: (i) the Part I of Form SCIR is being filed because the significant cybersecurity incident has been resolved and either no internal investigation pertaining to the significant cybersecurity incident is being or will be conducted or an internal investigation pertaining to the significant cybersecurity incident has been closed prior to the resolution of the incident; or (ii) the Part I of Form SCIR is being filed to report that an internal investigation pertaining to the significant cybersecurity incident has been closed and the significant cybersecurity incident is resolved. If a covered entity files a final report on Part I of Form SCIR with respect to a significant cybersecurity incident, and, thereafter, conducts an internal investigation pertaining to the significant cybersecurity incident, it must file another final report on Part I of Form SCIR when the investigation is closed pursuant to the requirements of 17 CFR 242.10.
4. **CONTACT EMPLOYEE** - The individual listed as the contact employee must be authorized by the covered entity to provide the Commission with information about the significant cybersecurity incident, and make information about the significant cybersecurity incident available to the Commission.
5. **LINE ITEMS**
 - a. **Line 2** – Provide the date the covered entity had a reasonable basis to conclude that the significant cybersecurity incident had occurred or was occurring. This can be based on, for example, reviewing or receiving a record, alert, log, or notice about the incident.
 - b. **Line 3.C.** – Provide the approximate date that the Covered Entity was no longer undergoing a significant cybersecurity incident.

C. INSTRUCTIONS TO PART II OF FORM SCIR

1. **PUBLIC DISSEMINATION** – Part II of Form SCIR will be publicly disseminated upon filing it with the Commission.
2. **DISCLOSURE UPDATES** - Pursuant to the requirements of 17 CFR 242.10, a covered entity must promptly provide an updated disclosure through the methods required by 17 CFR 242.10 if the information required to be disclosed pursuant to 17 CFR 242.10 materially changes, including

after the occurrence of a new significant cybersecurity incident or when information about a previously disclosed significant cybersecurity incident materially changes.

The mailing address for questions and correspondence is:

The Securities and Exchange Commission
Washington, DC 20549

FORM SCIR PART I		SIGNIFICANT CYBERSECURITY INCIDENTS		Official Use	Official Use Only
Page 1 (Execution Page)		Date: _____	SEC Filer No: _____		
WARNING		Failure to file Form SCIR as required by 17 CFR 242.10 would violate the Federal securities laws and may result in disciplinary, administrative, injunctive or criminal action.			
		INTENTIONAL MISSTATEMENTS OR OMISSIONS OF FACTS MAY CONSTITUTE FEDERAL CRIMINAL VIOLATIONS.			
		See 18 U.S.C. 1001 and 15 U.S.C. 78ff(a)			
INITIAL REPORT <input type="checkbox"/>		AMENDED REPORT <input type="checkbox"/>		FINAL AMENDED REPORT <input type="checkbox"/>	
				Check the reason for filing the Final Amended Report	
				Incident Resolved <input type="checkbox"/>	
				Investigation Closed <input type="checkbox"/>	
1. Information about the covered entity:					
A. i. Full legal name:					

ii. Business name if different than legal name:					

B. Tax Identification No.:		Covered Entity's UIC # (if any):		Covered Entity's CIK #:	
_____		_____		_____	
C. Main Address: (Do not use a P.O. Box)					
Number and Street 1:			Number and Street 2:		
_____			_____		
City:		State:		Country:	
_____		_____		Zip/Postal Code:	
_____		_____		_____	
D. Contact Employee					
Name:		Phone Number:		Email:	
_____		_____		_____	
E. Type of Covered Entity (Check all the apply):					
Broker or dealer <input type="checkbox"/>		Clearing Agency <input type="checkbox"/>		Major Security-Based Swap Participant <input type="checkbox"/>	
Municipal Securities Rulemaking Board <input type="checkbox"/>		National Securities Association <input type="checkbox"/>		National Securities Exchange <input type="checkbox"/>	
Security-Based Swap Dealer <input type="checkbox"/>		Security-Based Swap Data Repository <input type="checkbox"/>		Transfer Agent <input type="checkbox"/>	
EXECUTION:					
The undersigned certifies that this form was executed on behalf of, and with the authority of, the covered entity. The undersigned and covered entity represent that the information and statements contained herein are current, true and complete. The undersigned and covered entity further represent that to the extent any information previously submitted is not amended such information is current, true, and complete.					
_____			_____		
Date (MM/DD/YYYY)			Full Legal Name of Covered Entity		
By: _____			_____		
Signature			Name and Title of Person Signing on Covered Entity's behalf		
<i>This page must always be completed in full.</i>					
DO NOT WRITE BELOW THIS LINE – FOR OFFICIAL USE ONLY					

FORM SCIR PART I Page 2	Covered Entity Name: _____ Date: _____ SEC Filer No: _____	Official Use _____ _____	Official Use Only						
	2. The approximate date the significant cybersecurity incident was discovered: <table border="1" style="display: inline-table; vertical-align: middle;"> <tr> <td>DD</td> <td>MM</td> <td>YYYY</td> </tr> </table>			DD	MM	YYYY			
DD	MM	YYYY							
3. The approximate duration of the significant cybersecurity incident: A. Is the incident ongoing: Yes <input type="checkbox"/> No <input type="checkbox"/> Unknown <input type="checkbox"/> B. Approximate start date of incident: <table border="1" style="display: inline-table; vertical-align: middle;"> <tr> <td>DD</td> <td>MM</td> <td>YYYY</td> </tr> </table> Unknown <input type="checkbox"/> C. Approximate date incident was resolved: <table border="1" style="display: inline-table; vertical-align: middle;"> <tr> <td>DD</td> <td>MM</td> <td>YYYY</td> </tr> </table>				DD	MM	YYYY	DD	MM	YYYY
DD	MM	YYYY							
DD	MM	YYYY							
4. The status of an internal investigation pertaining to the significant cybersecurity incident: A. Is an internal investigation being conducted: Yes <input type="checkbox"/> No <input type="checkbox"/> B. If are yes, approximate date the internal investigation was closed: <table border="1" style="display: inline-table; vertical-align: middle;"> <tr> <td>DD</td> <td>MM</td> <td>YYYY</td> </tr> </table>				DD	MM	YYYY			
DD	MM	YYYY							
5. Has a law enforcement or government agency (other than the Commission) been notified of the significant cybersecurity incident: Yes <input type="checkbox"/> No <input type="checkbox"/> If yes, identify each law enforcement or government agency: _____ _____ _____ _____									
6. Describe the nature and scope of the significant cybersecurity incident, including the information systems affected by the incident and any effect on the covered entity's critical operations: _____ _____ _____ _____									
7. A. Has the threat actor(s) causing the significant cybersecurity incident been identified: Yes <input type="checkbox"/> No <input type="checkbox"/> If yes, identify the threat actor(s): _____ _____ _____ _____ _____ B. Has there been communication(s) from or with the threat actor that caused or claims to have caused the significant cyber security incident (answer even if the actor(s) has not been identified): Yes <input type="checkbox"/> No <input type="checkbox"/> If yes, describe the communications: _____ _____ _____ _____ _____									

FORM SCIR PART I Page 3	Covered Entity Name: _____	Official Use	Official Use Only
	Date: _____ SEC Filer No: _____		
8. Describe the actions taken or planned to respond to and recover from the significant cybersecurity incident: _____ _____ _____ _____			
9. Was any data stolen, altered, or accessed or used for any other unauthorized purpose: Yes <input type="checkbox"/> No <input type="checkbox"/> Unknown <input type="checkbox"/> If yes, describe the nature and scope of the data: _____ _____ _____ _____			
10. A. Was any personal information lost, stolen, modified, deleted, destroyed, or accessed without authorization as a result of the significant cybersecurity incident: Yes <input type="checkbox"/> No <input type="checkbox"/> Unknown <input type="checkbox"/> If yes, describe the nature and scope of the information: _____ _____ _____ _____			
B. i. If yes, has notification been provided to persons whose personal information was lost, stolen, modified, deleted, destroyed, or accessed without authorization: Yes <input type="checkbox"/> No <input type="checkbox"/> ii. If no, is notification planned: Yes <input type="checkbox"/> No <input type="checkbox"/>			

FORM SCIR PART I Page 4	Covered Entity Name: _____ Date: _____ SEC Filer No: _____	Official Use	Official Use Only						
11. Were any assets of the covered entity lost or stolen as a result of the significant cybersecurity incident: Yes <input type="checkbox"/> No <input type="checkbox"/> Unknown <input type="checkbox"/> If yes, describe the types of assets that were lost or stolen and include an approximate estimate of their value, if known: _____ _____ _____ _____									
12. A. Were any assets of the covered entity's customers, counterparties, members, registrants, or users lost or stolen as a result of the significant cybersecurity incident: Yes <input type="checkbox"/> No <input type="checkbox"/> Unknown <input type="checkbox"/> If yes, describe the types of assets that were lost or stolen and include an approximate estimate of their value, if known: _____ _____ _____ _____ B. i. If yes, has notification been provided to persons whose assets were lost or stolen: Yes <input type="checkbox"/> No <input type="checkbox"/> ii. If no, is notification planned: Yes <input type="checkbox"/> No <input type="checkbox"/>									
13. Has the significant cybersecurity incident been disclosed in accordance with 17 CFR 242.10: A. On EDGAR: Yes <input type="checkbox"/> No <input type="checkbox"/> If yes, disclosure date: <table border="1" style="display: inline-table; border-collapse: collapse;"><tr><td style="width: 30px;">DD</td><td style="width: 30px;">MM</td><td style="width: 30px;">YYYY</td></tr></table> B. On business Internet website: Yes <input type="checkbox"/> No <input type="checkbox"/> If yes, disclosure date: <table border="1" style="display: inline-table; border-collapse: collapse;"><tr><td style="width: 30px;">DD</td><td style="width: 30px;">MM</td><td style="width: 30px;">YYYY</td></tr></table> C. If applicable, to the covered entity's customers: Yes <input type="checkbox"/> No <input type="checkbox"/> If 12.A, 12.B, and/or 12C. are no, explain why the disclosures have not been made: _____ _____ _____ _____				DD	MM	YYYY	DD	MM	YYYY
DD	MM	YYYY							
DD	MM	YYYY							
14. A. Is the significant cybersecurity incident covered by an insurance policy of the covered entity: Yes <input type="checkbox"/> No <input type="checkbox"/> Unknown <input type="checkbox"/> B. If yes, has the insurance company been contacted: Yes <input type="checkbox"/> No <input type="checkbox"/>									
15. Provide any additional information or comments: _____ _____ _____ _____									

FORM SCIR PART II Page 1 (Execution Page)	CYBERSECURITY RISKS AND SIGNIFICANT CYBERSECURITY INCIDENTS Date: _____ SEC File No: _____	Official Use	Official Use Only
Failure to file Form SCIR as required by 17 CFR 242.10 would violate the Federal securities laws and may result in disciplinary, administrative, injunctive or criminal action.			
WARNING INTENTIONAL MISSTATEMENTS OR OMISSIONS OF FACTS MAY CONSTITUTE FEDERAL CRIMINAL VIOLATIONS. See 18 U.S.C. 1001 and 15 U.S.C. 78ff(a)			
1. Information about the covered entity:			
A. i. Full legal name: _____ ii. Business name if different than legal name: _____			
B. Covered Entity's UIC # (if any): _____ Covered Entity's CIK #: _____			
C. Main Address: (Do not use a P.O. Box)			
Number and Street 1: _____		Number and Street 2: _____	
City: _____	State: _____	Country: _____	Zip/Postal Code: _____
D. Type of Covered Entity (Check all that apply):			
Broker or dealer <input type="checkbox"/>		Clearing Agency <input type="checkbox"/>	Major Security-Based Swap Participant <input type="checkbox"/>
Municipal Securities Rulemaking Board <input type="checkbox"/>		National Securities Association <input type="checkbox"/>	National Securities Exchange <input type="checkbox"/>
Security-Based Swap Dealer <input type="checkbox"/>		Security-Based Swap Data Repository <input type="checkbox"/>	Transfer Agent <input type="checkbox"/>
EXECUTION: The undersigned certifies that this form was executed on behalf of, and with the authority of, the covered entity. The undersigned and covered entity represent that the information and statements contained herein are current, true and complete. The undersigned and covered entity further represent that to the extent any information previously submitted is not amended such information is current, true, and complete.			
_____ Date (MM/DD/YYYY)		_____ Full Legal Name of Covered Entity	
By: _____ Signature		_____ Name and Title of Person Signing on Covered Entity's behalf	
This page must always be completed in full.			
DO NOT WRITE BELOW THIS LINE – FOR OFFICIAL USE ONLY			

FORM SCIR PART II Page 2	Covered Entity Name: _____	Official Use	<small>Official Use Only</small>
	Date: _____ SEC File No: _____		
<p>2. "Cybersecurity risk" means financial, operational, legal, reputational, and other adverse consequences that could result from cybersecurity incidents, cybersecurity threats, and cybersecurity vulnerabilities. "Cybersecurity incident" means an unauthorized occurrence on or conducted through a covered entity's information systems that jeopardizes the confidentiality, integrity, or availability of the information systems or any information residing on those systems. "Cybersecurity threat" means any potential occurrence that may result in an unauthorized effort to affect adversely the confidentiality, integrity, or availability of a covered entity's information systems or any information residing on those systems. "Cybersecurity vulnerability" means a vulnerability in a covered entity's information systems, information system security procedures, or internal controls, including, for example, vulnerabilities in their design, configuration, maintenance, or implementation that, if exploited, could result in a cybersecurity incident.</p> <p>Provide a summary description of the cybersecurity risks that could materially affect the covered entity's business and operations and how the covered entity assesses, prioritizes, and addresses those cybersecurity risks.</p> <hr/> <hr/> <hr/> <hr/>			
<p>3. A "significant cybersecurity incident" means a cybersecurity incident, or a group of related cybersecurity incidents, that (1) significantly disrupts or degrades the ability of the covered entity to maintain critical operations; or (2) leads to the unauthorized access or use of the information or information systems of the covered entity, where the unauthorized access or use of such information or information systems results in or is reasonably likely to result in: (A) substantial harm to the covered entity; or (B) substantial harm to a customer, counterparty, member, registrant, or user of the covered entity, or to any other person that interacts with the covered entity.</p> <p>Has the covered entity experienced one or more significant cybersecurity incidents during the current or previous calendar year: Yes <input type="checkbox"/> No <input type="checkbox"/></p> <p>If yes, provide a summary description of each significant cybersecurity incident during that period. The description of each significant cybersecurity must include, at a minimum, the following information to the extent known:</p> <p>The person or persons affected; The date the incident was discovered and whether it is ongoing; Whether any data was stolen, altered, or accessed or used for any other authorized purpose; The effect of the incident on the covered entity's operations; and Whether the covered entity, or service provider, has remediated or is currently remediating the incident.</p> <hr/> <hr/> <hr/> <hr/> <hr/>			



FEDERAL REGISTER

Vol. 88

Wednesday,

No. 65

April 5, 2023

Part III

The President

Proclamation 10539—Arab American Heritage Month, 2023
Proclamation 10540—Care Workers Recognition Month, 2023
Proclamation 10541—Month of the Military Child, 2023
Proclamation 10542—National Cancer Control Month, 2023
Proclamation 10543—National Child Abuse Prevention Month, 2023
Proclamation 10544—National Donate Life Month, 2023
Proclamation 10545—National Sexual Assault Awareness and Prevention Month, 2023
Proclamation 10546—Second Chance Month, 2023
Proclamation 10547—National Public Health Week, 2023
Proclamation 10548—Education and Sharing Day, USA, 2023
Proclamation 10549—World Autism Awareness Day, 2023

Presidential Documents

Title 3—

Proclamation 10539 of March 31, 2023

The President

Arab American Heritage Month, 2023

By the President of the United States of America

A Proclamation

The Arab American story is the American story—one of diverse backgrounds and faiths, vibrant tradition, bold innovation, hard work, commitment to community, and stalwart patriotism, all coming together to accomplish something greater than any one of us. This month, we join together to celebrate the immeasurable contributions of Arab Americans to our Nation and recommit ourselves to the timeless work of making sure that all people have the opportunity to achieve the American Dream.

Ours is a Nation shaped by the immigrant's heart, and generations of brave and hopeful people from across all countries, including from the Arab world, have woven their unique heritages, customs, and talents into the tapestry of America. Today, the achievements of Arab Americans are reflected in the arts and sciences; in businesses and faith communities; in classrooms and hospitals; and in police stations, firehouses, and every branch of the military. Arab Americans are also proudly serving throughout my Administration, bringing a diversity of expertise that helps make this country stronger, more prosperous, and more just.

Sadly, we also recognize that, even as Arab Americans enrich our Nation, many continue to face prejudice, bigotry, and violence—a stain on our collective conscience. Hate must have no safe harbor in this country. We must affirm that sentiment again and again. That is why, on my first day in office, I issued the Proclamation on Ending Discriminatory Bans on Entry to The United States, which harmed the Arab American community. I also signed an Executive Order charging the Federal Government with advancing equity for historically underserved communities, including Arab Americans. I was proud to host a first-of-its-kind United We Stand Summit at the White House and announce new measures to help communities prevent and respond to hate-based threats, bullying, and harassment. I established a new interagency group to coordinate the Federal Government's efforts to fight antisemitism and Islamophobia, which impact Arab Americans. And my Administration is also exploring adding a new data category to the census for Middle Eastern and North African communities as part of our vital work to ensure that Arab Americans are seen, valued, consulted, and properly considered as new policy is made.

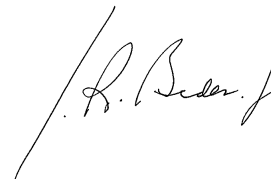
I have worked closely with our partners across the Middle East and North Africa to advance a common vision for the world as well as a more peaceful, prosperous, and integrated region. Together, we are strengthening our ability to address shared challenges, from regional security to climate change; fostering economic development and cooperation in science, technology, renewable energy, and space; and bringing greater peace and prosperity to all of our people.

The United States is the only Nation in the world founded on an idea—the idea that we are all created equal and deserve to be treated equally throughout our lives. As a Nation, we have never fully lived up to that promise, but we have never walked away from it either. This Arab American Heritage Month, let us all strive to honor our fundamental values and

advance equity and opportunity for all people, affirming once again that diversity is our country's greatest strength.

NOW, THEREFORE, I, JOSEPH R. BIDEN JR., President of the United States of America, by virtue of the authority vested in me by the Constitution and the laws of the United States, do hereby proclaim April 2023 as Arab American Heritage Month. I call upon all Americans to learn more about the history, culture, and achievements of Arab Americans and to observe this month with appropriate programs and activities.

IN WITNESS WHEREOF, I have hereunto set my hand this thirty-first day of March, in the year of our Lord two thousand twenty-three, and of the Independence of the United States of America the two hundred and forty-seventh.



Presidential Documents

Proclamation 10540 of March 31, 2023

Care Workers Recognition Month, 2023

By the President of the United States of America

A Proclamation

Across America, care workers help raise our children, assist seniors as they age with dignity, and support people with disabilities—giving families peace of mind and making it possible for millions of Americans to earn a paycheck while their loved ones are safe and secure. These unsung heroes strengthen our communities and form the backbone of our Nation’s economy. This month, we honor their extraordinary contributions and commit to supporting them with better pay, better benefits, and the recognition they have long deserved.

Despite all they give to this country, care workers—including child care workers, home care workers, and long-term care workers—are among the lowest-paid workers in America. Some juggle multiple jobs, and many leave the profession altogether in search of better options. The vast majority of care workers are women, and a disproportionate share are people of color, so this chronic underpayment deepens gender and racial wealth gaps. During the COVID–19 pandemic, many care workers were forced to put themselves and their families at risk, just to do their jobs. And the care workforce continues to recover slowly, making it hard for families to find care. This leads to hundreds of billions in lost wages each year and only heightens the obligation placed on the Nation’s more than 50 million family caregivers.

As many have said, care is the work that makes all other work possible. That is why my Administration invested over \$39 billion from our American Rescue Plan to help child care providers keep their doors open and to provide child care workers with higher pay, bonuses, and other benefits—reducing turnover and attracting new staff. To date, these efforts have helped 220,000 child care programs, which employ more than 1 million child care workers and have the capacity to serve 9.6 million children. At the height of the pandemic, we delivered financial relief to nearly 300,000 child care workers through our expanded earned income tax credit. We know we must do more, so my most recent budget proposes investing \$600 billion over 10 years to expand access to high-quality child care and free, high-quality preschool. This funding will allow States to increase pay for child care workers while helping the families of more than 16 million children afford child care.

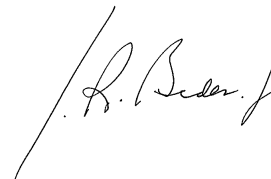
Meanwhile, we are promoting the use of apprenticeship programs and partnering with employers, unions, and others to recruit, train, and keep long-term care workers on the job while also helping them advance their careers as registered and licensed nurses. My Budget calls on the Congress to invest \$150 billion over the next decade to improve and expand Medicaid home- and community-based services—making it easier for seniors and people with disabilities to receive care in their own homes. This funding would improve the quality of jobs for home care workers and support family caregivers.

Our message this month to care workers across America is simple: The work you do matters. You are there for families when they need you most—providing comfort, strength, and compassion that inspire us all. Your devotion to the people and communities you serve represents the best of America’s

character, and we will always stand with you, ensuring you are seen, valued, and rewarded fairly for the work you do.

NOW, THEREFORE, I, JOSEPH R. BIDEN JR., President of the United States of America, by virtue of the authority vested in me by the Constitution and the laws of the United States, do hereby proclaim April 2023 as Care Workers Recognition Month. I call upon all Americans to celebrate the contributions of care workers to our Nation with appropriate ceremonies, activities, and programs.

IN WITNESS WHEREOF, I have hereunto set my hand this thirty-first day of March, in the year of our Lord two thousand twenty-three, and of the Independence of the United States of America the two hundred and forty-seventh.

A handwritten signature in black ink, appearing to read "Joe Biden", with a long, sweeping underline that extends to the left.

Presidential Documents

Proclamation 10541 of March 31, 2023

Month of the Military Child, 2023

By the President of the United States of America

A Proclamation

This month, we honor the over 2 million children of our service members and veterans, whose support and sacrifice help keep our military strong and our Nation secure. These young Americans already understand what it means to serve, shouldering the unique demands of military life with courage and tenacity.

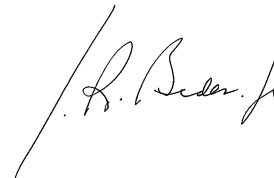
Whenever the First Lady and I meet with military children, we are amazed by their strength and selflessness. Most of these young patriots uproot their lives every few years—starting at new schools, making new friends, and learning new cultures and customs in different corners of the country and around the globe. They often celebrate birthdays and holidays with an empty seat at the dinner table. Many have marked graduations without one of their biggest fans in the crowd. So often, these children serve as Hidden Helpers, becoming caregivers for their wounded, ill, or injured loved ones—and far too many have grown up with the enduring grief of having lost a parent.

As a Nation, we have many obligations, but we have only one truly sacred obligation: to prepare our troops we send into harm's way and to care for them and their families while they are deployed and when they return home. Our military-connected children are at the heart of this sacred obligation. My Administration is stepping up to meet this obligation. We have expanded the Military Parental Leave Program, which enables service members to spend needed time with their families following a child's birth, adoption, or placement for long-term foster care. Through the Joining Forces initiative, the First Lady is leading our efforts to support military-connected children in their classrooms and help ease the burdens created by the highly mobile military lifestyle. We are also investing to provide their parents with access to affordable, quality child care.

The English poet John Milton once wrote, "They also serve who only stand and wait." Every day, military-connected children stand tall with pride for their parents and our Nation. They make sacrifices—big and small—so their parents can continue to serve and protect this country. These young people represent the very best of America, and we will always be grateful for their service to our Nation. May God bless our troops and their families, caregivers, and survivors.

NOW, THEREFORE, I, JOSEPH R. BIDEN JR., President of the United States of America, by virtue of the authority vested in me by the Constitution and laws of the United States, do hereby proclaim April 2023 as the Month of the Military Child. I call upon the people of the United States to honor the children of our service members and veterans with appropriate ceremonies and activities. I also encourage Americans everywhere to find ways to support military-connected children, including by wearing purple during the month of April in honor of their service.

IN WITNESS WHEREOF, I have hereunto set my hand this thirty-first day of March, in the year of our Lord two thousand twenty-three, and of the Independence of the United States of America the two hundred and forty-seventh.

A handwritten signature in black ink, appearing to read "Joe Biden", with a long, sweeping underline that extends to the left.

Presidential Documents

Proclamation 10542 of March 31, 2023

National Cancer Control Month, 2023

By the President of the United States of America

A Proclamation

Cancer has touched nearly every American family, and it remains the second leading cause of death in the United States. During National Cancer Control Month, we call on all Americans to join our movement to end cancer as we know it. By raising awareness of the risk factors, promoting life-saving regular screenings, investing in research, and expanding access to affordable treatment, we can give patients, survivors, and their families the hope and new beginnings they deserve.

We have made enormous progress in the half-century since our country first declared war on cancer. We have learned it is not a single disease but, in fact, over 200 different types of cancers caused by different genetic mutations. We have discovered life-saving prevention and early detection measures, new medicines, and innovative therapies, slashing the death rate by a third since 1991. But despite all that progress, cancer still claims the lives of over 600,000 Americans a year. And for many communities of color, the mortality rates are far worse, with Black Americans facing the highest mortality rate of any racial and ethnic group for all cancers combined and for most major cancers. Patients and their loved ones are still overwhelmed by a flood of unfamiliar information; worried about how they will pay for treatment; and awash in bewilderment, frustration, and fear. And those who have lost someone have often lost a piece of their soul.

I am more confident than ever, though, that we can change things. Last year, as part of the Unity Agenda that I outlined during my State of the Union Address, the First Lady and I reignited the Cancer Moonshot initiative that President Barack Obama first asked me to lead in 2016. We have set a new goal to cut America's cancer death rate by half in the next 25 years, turning more cancers from death sentences into treatable diseases and creating a more supportive experience for patients and families. As a first step, I established the Advanced Research Projects Agency for Health, securing \$2.5 billion in bipartisan funding from the Congress to develop breakthroughs in preventing, diagnosing, and treating cancer and other deadly diseases. This will pioneer partnerships to get those breakthroughs to the clinic. Additionally, I signed an Executive Order that will require biotechnology to be made in America, preserving access to lifesaving medications and making sure we lead the world in biotech innovation.

Improving treatment options is only part of the fight—we also need to make those treatments more affordable for everyone. To that end, the American Rescue Plan expanded the Affordable Care Act, which requires insurers to pay for cancer screenings and primary care visits and to cover cancer survivors and others who have preexisting conditions. We are working to make sure insurers cover patient navigation services, too, to help patients, caregivers, and families through screening, diagnosis, treatment, and survival. Meanwhile, the Inflation Reduction Act will cap out-of-pocket drug costs for seniors on Medicare at \$2,000 per year. This is a gamechanger for cancer patients in particular, whose medicines can currently cost seven times that. And the Honoring our PACT Act is ensuring that veterans exposed

to cancer-causing toxic substances during their military service get the health care and benefits that they have earned.

More than a third of all cancer cases are preventable, so my Administration is working to reduce people's exposure to risk factors. That starts with tackling the top cause of cancer deaths in this country: smoking. The Food and Drug Administration has proposed rules to ban menthol cigarettes and flavored cigars, which could prevent hundreds of thousands of deaths. For help quitting or avoiding smoking in the first place, visit [SmokeFree.gov](https://www.smokefree.gov), call 1-800-QUIT-NOW, or text QUITNOW to 333888.

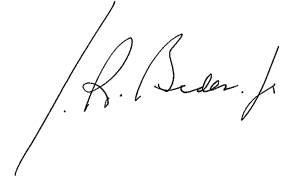
We are also making it easier for Americans to adopt healthy eating and exercise habits, which have been shown to lower cancer risk. Our national strategy to end hunger seeks to provide healthy, free school meals to millions of kids; boost Medicaid and Medicare coverage for things like nutrition and obesity counseling; and make fruits and vegetables more affordable for low-income families.

Because detecting cancer early can increase survival, we urge all Americans to catch up on routine screening appointments they may have missed during the pandemic and to encourage loved ones to do the same. In the last year, the Centers for Disease Control and Prevention issued more than \$200 million in grants to support cancer screening in every State, many United States territories, and Tribal Nations. The Department of Health and Human Services is helping community health centers improve access to early detection, too. To learn which screenings are right for you, talk to your health care provider, visit [cdc.gov/cancerscreeningorcancer.gov/screeningtests](https://www.cdc.gov/cancerscreeningorcancer.gov/screeningtests), or call 1-800-4-CANCER.

The fight against cancer is personal to so many families, including ours. It is one of the reasons I ran for President. And it is something big that we can all do together. Cancer does not care if you are Republican or Democrat—we need everyone in the game. We need the scientific and medical communities, bringing their boldest thinking. We need the private sector, testing new treatments and sharing more knowledge. We need people living with cancer, survivors, caregivers, and families, whose absolute courage this work is all about. For the lives we can save and those we have lost, let this be a truly American moment that rallies the country and the world together to end cancer as we know it and to cure some cancers for good.

NOW, THEREFORE, I, JOSEPH R. BIDEN JR., President of the United States of America, do hereby proclaim April 2023 as National Cancer Control Month. I encourage citizens, government agencies, private businesses, non-profit organizations, and other interested groups to join in activities that will increase awareness of what Americans can do to prevent, detect, treat, and control cancer.

IN WITNESS WHEREOF, I have hereunto set my hand this thirty-first day of March, in the year of our Lord two thousand twenty-three, and of the Independence of the United States of America the two hundred and forty-seventh.

A handwritten signature in black ink, appearing to read "Joe Biden", written in a cursive style.

Presidential Documents

Proclamation 10543 of March 31, 2023

National Child Abuse Prevention Month, 2023

By the President of the United States of America

A Proclamation

During National Child Abuse Prevention Month, we want every young person in the United States who has faced the fear and pain of abuse or neglect to know they are not alone. We see you and will always fight to protect your safety and well-being. We reaffirm our commitment to listening to children, standing with brave survivors, and reaching out across our communities to support families and to help others in need.

I was raised to believe that the greatest sin in life is the abuse of power, and the abuse of a woman or child is the worst of all. Yet millions of children of every race, religion, and background face neglect or physical, emotional, or sexual abuse in America every year. It can leave deep, lasting scars, making it harder to learn in school, to form trusting relationships, to build self-esteem, and to escape cycles of abuse long-term. It denies far too many children the promise of America and risks cutting them off from their dreams and undermining their ability to reach their full potential.

We have a moral obligation to protect every child in America and to help survivors heal. That is why, as a United States Senator, I wrote and passed the Violence Against Women Act, to help secure safety and justice for women and children impacted by domestic violence. We have fought ever since to keep building on that law—including with last year's bipartisan reauthorization, which increased support for prevention, trauma-informed services, and training for courts while also expanding recognition of Tribal courts' jurisdiction in cases involving non-Native perpetrators of child abuse. As President, I also signed the American Rescue Plan, investing an additional \$350 million to improve State child protective services and community-based child abuse prevention programs. The Department of Justice is providing resources to Children's Advocacy Centers across the country that support child abuse victims by supporting law enforcement efforts to investigate and prosecute child abuse and funding law enforcement task forces to combat online child exploitation. I also signed legislation eliminating the Federal statute of limitations for child sex abuse crimes so justice can still be done even after survivors become adults. And we are helping State and territorial health departments prevent sexual violence and provide trauma-informed training to support recovery among the 1 in 4 girls and 1 in 13 boys who will face sexual abuse before they turn 18.

To support our children, we are continuing our efforts to reduce child poverty across the board, including by fighting to restore the Child Tax Credit, which in 2021 helped slash child poverty to its lowest rate ever. We know that poverty can trigger interventions in which children are sometimes unnecessarily removed from their homes. My new budget requests \$10 billion to help keep families safely together and to better fund child abuse prevention and treatment services.

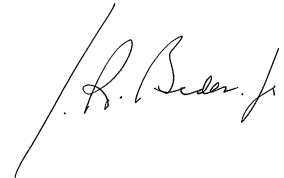
Meanwhile, a dangerous wave of cynical State investigations is targeting families just because they love and support their transgender children. These State campaigns are government overreach at its worst. From the Department of Justice to the Department of Health and Human Services, my Administration will keep working to make sure that politicians do not unlawfully

weaponize child protective services against loving families who simply want to support their kids and help them to be themselves.

It has been said that a Nation is judged by how we treat the most vulnerable among us. Nowhere is that truer than when it comes to protecting our children, making sure they grow up safe from harm and surrounded by love. That is on all of us. For more information on how to recognize and report child abuse or neglect, as well as on how to support loving families and safe communities, visit childwelfare.gov.

NOW, THEREFORE, I, JOSEPH R. BIDEN JR., President of the United States of America, by virtue of the authority vested in me by the Constitution and the laws of the United States, do hereby proclaim April 2023 as National Child Abuse Prevention Month. I call upon all Americans to observe this month by joining together as a Nation to promote the safety and well-being of all children and families and to recognize the child-welfare professionals and allies who work tirelessly to protect our children. Let us also honor the strength and resilience of survivors of child abuse.

IN WITNESS WHEREOF, I have hereunto set my hand this thirty-first day of March, in the year of our Lord two thousand twenty-three, and of the Independence of the United States of America the two hundred and forty-seventh.



Presidential Documents

Proclamation 10544 of March 31, 2023

National Donate Life Month, 2023

By the President of the United States of America

A Proclamation

More than 400,000 Americans in every corner of our country are alive today thanks to the tremendous generosity and courage of organ donors. During National Donate Life Month, we honor donors and their families who have turned pain into purpose by sharing the gift of life with loved ones in need or countless others whom they have never met. We encourage everyone to follow their lead and register as an organ, eye, tissue, or bone marrow donor, bringing hope and healing to so many others.

Last year, American doctors completed our Nation's one-millionth organ transplant, a tremendous milestone in the history of a procedure pioneered and honed in America. We are now performing transplants at a record pace, with higher success rates and increased lifespans for recipients. Still, every 10 minutes, someone new joins the waiting list—fighting organ failure or blood cancer, their futures hanging in the balance. More than 100,000 people, including 1,900 children, are currently on the waiting list. A majority of them are people of color, for whom it can sometimes be more difficult to find a good donor match. Seventeen Americans die every day while waiting for a transplant.

We each have the power to change that. Just one person can save up to 8 lives through organ donation after they die and improve another 75 lives through eye and tissue donation. Registering as a donor does not change the quality of care that you receive in your lifetime. It allows you to give countless others a second chance at life and your family to find peace amid grief while leaving an extraordinary legacy of compassion and dignity.

Each year, thousands of Americans choose to donate an organ while still living, a profoundly courageous act of connection and healing.

My Administration is working across the board to support organ donation and to make sure living donors and recipients have the affordable health care and prescription drug coverage they need before and after a transplant and throughout their lives. We have acted to extend Medicare coverage of vital drugs for kidney transplant patients. And just recently, we launched the Organ Procurement and Transplantation Network (OPTN) Modernization Initiative to better serve the needs of patients and families across the country. We have published data on organ donors, organ procurements, transplant waitlists, and transplant recipients. We will foster competition, working to promote the use of innovative technology and ensure the highest quality of care is provided to patients. We are committed to a modernized OPTN that is transparent, accountable, and equitable.

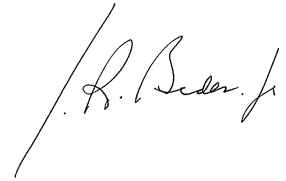
We have also launched the transformational Advanced Research Projects Agency for Health, securing \$2.5 billion for breakthroughs in the prevention, detection, and treatment of cancer and other deadly diseases, which could one day make many transplants unnecessary.

America is a great Nation because we are a good people—generous, decent, and fair. We look out for our neighbors and lend a hand to those in need. Few things demonstrate that more than the act of becoming an organ

donor. Any adult can register, regardless of age or medical history; in many States, doing so is as simple as checking a box when renewing your driver's license or signing up online. I encourage all Americans to visit organdonor.gov to learn more about organ, eye, and tissue donation or bloodstemcell.hrsa.gov for more information on donating bone marrow. We celebrate everyone who makes this deeply generous choice to give others the gift of life.

NOW, THEREFORE, I, JOSEPH R. BIDEN JR., President of the United States of America, by the authority vested in me by the Constitution and the laws of the United States, do hereby proclaim April 2023 as National Donate Life Month. I call on every person who can to share the gift of life and hope by becoming an organ, eye, tissue, or bone marrow donor. I also call on this Nation to observe National Pediatric Transplant Week from April 23 through April 29, a week dedicated to ending the pediatric transplant waiting list.

IN WITNESS WHEREOF, I have hereunto set my hand this thirty-first day of March, in the year of our Lord two thousand twenty-three, and of the Independence of the United States of America the two hundred and forty-seventh.



Presidential Documents

Proclamation 10545 of March 31, 2023

National Sexual Assault Awareness and Prevention Month, 2023

By the President of the United States of America

A Proclamation

Freedom from sexual assault is a basic human right. Yet tens of millions of Americans—our family and friends, colleagues, neighbors, and classmates—carry the trauma of sexual assault with them. National Sexual Assault Awareness and Prevention Month is an important time to speak out, stand with courageous survivors, and finally change the culture that has allowed sexual violence to exist for far too long.

Sexual violence affects all people, regardless of geography, race, age, ethnicity, gender, religion, sexual orientation, gender identity, or economic background. One in four women and 1 in 26 men have survived a rape or attempted rape. Abuse can happen anywhere—at work, at home, at school, in other public places, or online. It can lead to depression, anxiety, PTSD, and other physical and emotional wounds. We must keep fighting to make clear how important consent is and how sexual assault can be a crime. And we must help survivors access safety, justice, and healing.

That is why I wrote the landmark Violence Against Women Act (VAWA) 30 years ago, at a time when domestic violence and sexual assault were often swept under the rug. We changed that. VAWA has given us tools to prevent and prosecute sexual assault and provide support for survivors. It has helped to save and rebuild so many lives, and I have never quit working to strengthen the law, including expanding protections when VAWA was reauthorized in 2000, 2005, 2013, and most recently in 2022. These efforts have expanded support for survivors, especially for people of color, members of the LGBTQI+ community, and immigrants, and have broadened protections to cover online abuse, such as the non-consensual distribution of intimate images. We increased VAWA funding this past year by 20 percent to a historic \$700 million for 2023.

Today, we are doing more to help survivors in underserved communities and rural areas. We are working to reduce the backlog of untested rape kits as many survivors continue to wait for justice. We are improving trauma-informed training for law enforcement and making sure that adult survivors of child sexual abuse can get help, including legal help and support for healing. And we have ensured that Tribal courts have jurisdiction over non-Native perpetrators suspected of committing crimes of sexual assault, sex trafficking, and child abuse on Tribal lands. Additionally, through the American Rescue Plan, we have delivered \$1 billion in additional funding for rape crisis centers, culturally specific community support organizations, and other domestic violence and sexual assault services nationwide.

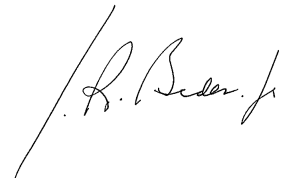
We have also reformed how the military investigates and prosecutes sexual assault, sexual harassment, and related crimes, including by shifting authority from commanders to independent prosecutors. I issued an Executive Order listing sexual harassment and the wrongful distribution of intimate images as offenses under the Uniform Code of Military Justice.

I launched a Federal task force to tackle the rise in online sexual harassment and abuse, recommending concrete steps for prevention, accountability, research, and support for survivors. And I signed laws ending forced arbitration and limiting the enforcement of non-disclosure agreements to ensure people who have experienced sexual assault and sexual harassment in the workplace can pursue justice.

While we have made progress addressing sexual violence over the years, there is still much work to do. As President, I have expanded funding for campus prevention efforts, building on the work I did as Vice President when we launched “It’s On Us”. I signed an Executive Order calling on the Department of Education to protect students from discrimination based on sex, including sex-based harassment and sexual violence. And I will continue to fight tirelessly to realize the promise of Title IX, which requires institutions to prevent and address sexual violence and harassment. I have called on young men in particular to speak up and stand against abuse—because the real test of character is having the guts to do the right thing. And I have been awed by the courage of countless survivors in every part of the country who have come forward to push for justice and have inspired many others to do the same. It is on us all to stand with them.

NOW, THEREFORE, I, JOSEPH R. BIDEN JR., President of the United States of America, by virtue of the authority vested in me by the Constitution and laws of the United States, do hereby proclaim April 2023 as National Sexual Assault Awareness and Prevention Month. I urge all Americans to support sexual assault survivors, including when survivors reach out and disclose abuse, and to strengthen our efforts to prevent this abuse in the first place.

IN WITNESS WHEREOF, I have hereunto set my hand this thirty-first day of March, in the year of our Lord two thousand twenty-three, and of the Independence of the United States of America the two hundred and forty-seventh.

A handwritten signature in black ink, appearing to read "Joe Biden", with a long, sweeping underline that extends to the left and then curves back under the signature.

Presidential Documents

Proclamation 10546 of March 31, 2023

Second Chance Month, 2023

By the President of the United States of America

A Proclamation

America has always been a land of second chances, founded on fresh starts, new possibilities, and the belief that every person deserves to be treated with dignity and respect. During Second Chance Month, we recommit to helping people forge the new beginnings they have earned and building a safer and more just society.

I believe in redemption—but for hundreds of thousands of Americans released from State and Federal prisons each year, or the nearly 80 million who have an arrest or conviction record, it is not always easy to come by. A criminal record can prevent them from landing a steady job, a safe place to live, quality health care, or the chance to go to back school. It can keep them from ever getting a loan to buy a home, start a business, or build a future. It can bar them from voting. As a result, three-quarters of formerly incarcerated people remain unemployed a year after their release—and joblessness is a top predictor of recidivism. We are not giving people a real second chance.

Our justice system should instead be based on the simple premise that once someone completes their sentence, they should have the chance to earn a living, build a life, and participate in our democracy as fellow citizens. Instead of giving people \$25 and a bus ticket when they are released, we have to help them address their underlying needs as they re-enter society. It will keep families whole, build stronger and safer communities, grow our economy, and reduce recidivism long-term.

To do that, we need education, job, and substance use programs, during and after incarceration. My Administration is, for example, investing nearly \$1 billion in job training, recovery, and reentry services. We are implementing changes to the Pell Grant program so people can earn a college degree while still in prison, jumpstarting new lives. Once they are released, we are helping them to find jobs rebuilding America through our historic infrastructure law; and we have expanded access to small business loans, so no one's past keeps them from building a better future.

There is much more to do. Last summer, I released my Safer America Plan, which calls on the Congress to invest \$15 billion more in mental health and substance use services, job training, affordable housing, and other resources to help people rebuild their lives. It also urges the Congress to end restrictions on people with criminal records receiving disability insurance, Supplemental Nutrition Assistance Program food assistance, or other Federal benefits that would help them get back on their feet.

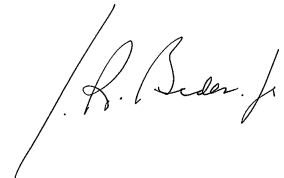
At the same time, we have to invest in preventing crime and breaking the cycle of recidivism. To that end, my Administration has put \$3 billion in American Rescue Plan funds toward mental health and substance use programs. We are allocating \$400 million this year to keep young people from becoming involved in the juvenile justice system. And my Safer America Plan would increase support for State and local crime prevention, including community violence intervention, which has been shown to reduce gun violence by up to 60 percent. We have also taken historic steps to end our Nation's failed approach to marijuana. Sending people to prison for

possession has upended too many lives for conduct that many States no longer prohibit. It has seen Black and Brown Americans disproportionately arrested, prosecuted, and convicted; and imposed unfair barriers to housing, employment, and education. Last fall, I announced a full pardon for Federal and DC simple possession offenses, while calling on other elected officials to do the same at the State and local levels where most marijuana prosecutions take place.

Meanwhile, we are working to reverse generations of disinvestment, rebuilding America's economy from the bottom up and middle out to leave no one behind. We have created a record 12 million jobs in the last 2 years and now have the near lowest unemployment rate in a half-century, putting good-paying work within everyone's reach, including people with past arrests or convictions. Our historic investments in infrastructure, manufacturing, and clean energy will help to close the racial wealth gap, investing in people and communities that have been overlooked for too long. That is what second chances look like, and every American should have an equal shot at one.

NOW, THEREFORE, I, JOSEPH R. BIDEN JR., President of the United States of America, by virtue of the authority vested in me by the Constitution and the laws of the United States, do hereby proclaim April 2023 as Second Chance Month. I call upon all government officials, educators, volunteers, and all the people of the United States to observe the month with appropriate programs, ceremonies, and activities.

IN WITNESS WHEREOF, I have hereunto set my hand this thirty-first day of March, in the year of our Lord two thousand twenty-three, and of the Independence of the United States of America the two hundred and forty-seventh.



Presidential Documents

Proclamation 10547 of March 31, 2023

National Public Health Week, 2023

By the President of the United States of America

A Proclamation

The field of public health is grounded in the fundamental truth that we are all in this together—that our health is connected and we are stronger as a Nation when we work together to lift everyone’s well-being. During National Public Health Week, we celebrate the life-saving work that our public health professionals do to keep Americans healthy and safe.

All of America has seen the importance of public health during the past 3 years. The pandemic shut down our businesses, closed our schools, and robbed us of so much, including the lives of over one million Americans. While the virus is not gone, we have made enormous progress, and it no longer controls our lives. More than 230 million Americans are fully vaccinated. COVID deaths are down more than 90 percent. Schools and businesses are open and thriving. And these gains are thanks in large part to the absolute courage and commitment of everyone who contributes to protecting our public health—including first responders and social workers, scientists and researchers, doctors and nurses, and so many others.

Public health professionals have been shaping our country for the better since long before COVID arose. From expanding access to immunizations and improving safety standards for food, traffic, and the workplace, to advocating for cleaner air and water, public health professionals have improved the lives of all Americans and made our country stronger, healthier, and more prosperous.

Looking ahead, there is so much more to do to end health disparities, keep advancing science, and improve the health and well-being of all Americans. That starts by making sure everyone has access to quality health care. Under my Administration, we have expanded coverage through the Affordable Care Act, making it cheaper and easier to sign up and saving millions of families \$800 a year. Through the American Rescue Plan, we invested \$7.6 billion in community health centers, and my latest budget would put us on a path to doubling the size of the Health Center Program, which funds care in underserved areas. We are also bringing down the cost of life-saving drugs like insulin and investing in next-generation breakthroughs to prevent, diagnose, and treat deadly diseases like cancer through the new Advanced Research Projects Agency for Health.

To take on the public health epidemic of gun violence, we passed the most significant gun safety law in three decades, which includes enhanced background checks for individuals under age 21, and funding for red flag laws that can help keep guns from people who are a danger to themselves and others. The law also makes historic investments in mental health, and it complements the launch of the 9–8–8 National Suicide & Crisis Lifeline and additional work to protect kids online. Additionally, I reauthorized the landmark Violence Against Women Act that I first wrote in 1990 and expanded protections for survivors of domestic violence. And we are fighting the opioid epidemic by cracking down on fentanyl trafficking; pushing for tougher penalties for suppliers; and expanding access to life-saving naloxone, treatment, and recovery services.

We have also made the biggest-ever investment in fighting the public health threat represented by the climate crisis. Our Justice40 Initiative works to ensure that 40 percent of our clean energy investments flow to disadvantaged communities that have so often borne the brunt, including the health consequences, of environmental damage. The Bipartisan Infrastructure Law is replacing poisonous lead pipes that go into 10 million homes and 400,000 schools and child care centers so that every child in America can turn on the faucet and drink clean water.

And we have released a national strategy to end hunger and reduce diet-related diseases like diabetes and obesity. The strategy provides millions of students with free, nutritious school meals and helps Americans exercise and make healthy choices in the foods they eat. We are also supporting people who want to quit smoking, and the Food and Drug Administration has proposed rules to ban menthol cigarettes and flavored cigars, which could save hundreds of thousands of lives.

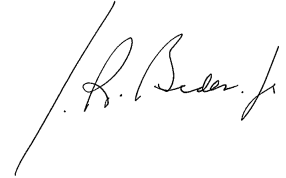
Since the Supreme Court's extreme decision to strip women of their fundamental right to choose, I have also taken urgent executive action to safeguard emergency care and protect patients' privacy. The Congress must act now to codify the protections of *Roe v. Wade* into law so women in every State have the right to make their own health care decisions. At the same time, my Administration is also working to end the maternal health crisis that leaves Black and Native American women up to three times more likely than white women to die during pregnancy.

These are all vital public health issues. Their range reminds us how connected our health is to the health of others. That is why the United States has continued to lead on global health challenges like HIV/AIDS, tuberculosis, and malaria, as well as COVID. Working with the G20 and other partners, we created the Pandemic Fund to strengthen global pandemic preparedness, prevention, and response. And at home, we invested over \$7 billion into strengthening the capacity of State and local public health departments to respond to future public health crises—including by launching the new Public Health AmeriCorps to train a strong, diverse public health workforce for the future.

As we look ahead, we have a choice to make. We can repeat the mistakes of the past that left us vulnerable to public health crises like COVID, or we can seize the opportunity to better prepare ourselves for the future and build a stronger public health system in every community nationwide. Let's choose to move forward, celebrating our dedicated public health professionals and making America more healthy, resilient, and just.

NOW, THEREFORE, I, JOSEPH R. BIDEN JR., President of the United States of America, by virtue of the authority vested in me by the Constitution and the laws of the United States, do hereby proclaim April 3 through April 9, 2023, as National Public Health Week. I call on all citizens, government agencies, private businesses, nonprofit organizations, and other groups to take action to improve the health of our Nation.

IN WITNESS WHEREOF, I have hereunto set my hand this thirty-first day of March, in the year of our Lord two thousand twenty-three, and of the Independence of the United States of America the two hundred and forty-seventh.

A handwritten signature in black ink, appearing to read "Joe Biden", written in a cursive style.

Presidential Documents

Proclamation 10548 of March 31, 2023

Education and Sharing Day, USA, 2023

By the President of the United States of America

A Proclamation

On Education and Sharing Day, we honor the memory of the Lubavitcher Rebbe, Rabbi Menachem Mendel Schneerson, who devoted his life to outreach and teaching—building bridges, challenging us to grow, and championing tolerance and learning.

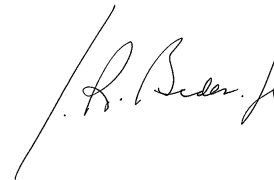
Forced to flee Nazi-occupied Europe during World War II, the Rebbe witnessed some of history's darkest moments. But his faith and a lifetime of study had already taught him that education is both the antidote to hate and the cornerstone of humanity as a whole. From Brooklyn, he turned pain into purpose and built a global movement devoted to education, fellowship, and healing. His work established schools and community institutions dedicated to helping people reach their full potential. He offered guidance to Presidents and celebrated the rich diversity of our Nation, advocating throughout for compassion and learning. Education, he once said, should not just be about training individuals to earn a living, but it should also be about making a better living for society as a whole. Instructors should not just teach; they should teach justice. Students should not only learn but also build character.

My Administration has stood firm in defending the core values that the Rebbe championed and that we all share as Americans—the idea that everyone is created equal and must be treated with dignity and respect throughout their lives. We are committed to stamping out intolerance, so nothing stops children from learning and no one is denied the promise of America. In this country, hate will never prevail.

The Rebbe told us, “We must translate pain into action and tears into growth.” That is what education makes possible. Children are the kite strings that hold our national ambitions aloft—everything America will be tomorrow depends on how we deliver for our young people today. So let us remember his teachings. Let us prepare our children to be tolerant, curious, and moral, ensuring that they lift up others as they rise.

NOW, THEREFORE, I, JOSEPH R. BIDEN JR., President of the United States of America, by virtue of the authority vested in me by the Constitution and the laws of the United States, do hereby proclaim April 2, 2023, as Education and Sharing Day, USA. I call upon all government officials, educators, volunteers, and all the people of the United States to observe this day with appropriate programs, ceremonies, and activities.

IN WITNESS WHEREOF, I have hereunto set my hand this thirty-first day of March, in the year of our Lord two thousand twenty-three, and of the Independence of the United States of America the two hundred and forty-seventh.

A handwritten signature in black ink, appearing to read "Joe Biden", is written in a cursive style. The signature is positioned to the right of the main text block.

Presidential Documents

Proclamation 10549 of March 31, 2023

World Autism Awareness Day, 2023

By the President of the United States of America

A Proclamation

There is no one way to be autistic—each individual with autism experiences it differently—but together, autistic people make industries, communities, and our Nation stronger. Today, we celebrate the achievements of neurodiverse people everywhere and champion the equal rights and dignity of all those living on the autism spectrum.

Here in the United States, more than 5.4 million adults are autistic, and 1 in every 44 children has been diagnosed with autism. Yet this developmental disability is still misunderstood. Autistic people continue to face obstacles when seeking employment, health care, education, and housing, and the immense contributions of people with autism are often overlooked. We owe it to our fellow Americans to address the disparities they face and to support autistic people with tools that facilitate clearer communication, increased productivity, and greater independence.

That is why my Administration is funding cutting-edge research to enable earlier autism diagnoses and to develop more resources to help neurodiverse people of all ages thrive. Recognizing that Autism Spectrum Disorder is categorized as a disability, my American Rescue Plan provided \$25 billion to States to make it easier for people with disabilities, including autism, to receive care at home. We also rolled out new tools and strategies for partner organizations to connect disabled Americans with stable housing while helping them pay rent, fight eviction, and prevent homelessness.

Last year, I was proud to reauthorize Kevin and Avonte's Law, which expands training for first responders and others giving care to people with autism. And in my recent State of the Union Address, I called on the Congress to increase its support for community living for people with disabilities.

My Administration is also boosting employment opportunities for autistic and other historically marginalized Americans. I was proud to sign an Executive Order advancing diversity, equity, inclusion, and accessibility in the Federal workforce, which will help create new jobs for Americans with autism and make space for their voices in the policy-making process.

We are helping State and local governments, employers, and nonprofits tap Federal funds to hire more Americans with disabilities like autism through competitive integrated employment practices. We are cracking down on employers who discriminate on the basis of disability, and we are fighting to end the unfair use of sub-minimum wages. I continue to urge States that have not yet expanded Medicaid coverage under the Affordable Care Act to do the right thing and provide health insurance to those currently locked out of Medicaid support that would otherwise be available to them from the Federal Government. Medicaid expansion would help many Americans with disabilities, including those with autism.

To support students with autism, the Department of Education is ensuring that public schools uphold their obligation to provide free and appropriate public education in the least restrictive environment to all students. My Administration has also issued new guidance to help schools avoid the

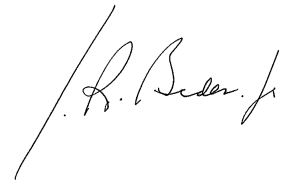
discriminatory use of discipline, which too often impacts autistic students, whose needs and behaviors are commonly misunderstood.

As we build a more inclusive, just, and equal Nation, we aim to lead by the power of our example. I reestablished the role of Special Advisor on International Disability Rights at the Department of State to prioritize disability rights in our policy discussions with foreign nations. The United States Agency for International Development is advancing disability inclusion as part of its democracy, climate, humanitarian, and peacebuilding activities. And as co-chair of the Global Action on Disability Network and a participant in the Global Disability Summit, the United States continues to promote the equal human rights of people with disabilities worldwide.

America is founded on the idea that all people are created equal and deserve to be treated equally throughout their lives. Today and always, let us strive to live up to this ideal. Let us embrace our diversity; empower each other to reach our full potential; and promote the basic decency, acceptance, and fairness we know is right.

NOW, THEREFORE, I, JOSEPH R. BIDEN JR., President of the United States of America, by virtue of the authority vested in me by the Constitution and the laws of the United States, do hereby proclaim April 2, 2023, as World Autism Awareness Day. I call upon all Americans to learn more about autism to improve early diagnosis, to learn more about the experiences of autistic people from autistic people, and to build more welcoming and inclusive communities to support people with autism.

IN WITNESS WHEREOF, I have hereunto set my hand this thirty-first day of March, in the year of our Lord two thousand twenty-three, and of the Independence of the United States of America the two hundred and forty-seventh.



Reader Aids

Federal Register

Vol. 88, No. 65

Wednesday, April 5, 2023

CUSTOMER SERVICE AND INFORMATION

Federal Register/Code of Federal Regulations	
General Information, indexes and other finding aids	202-741-6000
Laws	741-6000
Presidential Documents	
Executive orders and proclamations	741-6000
The United States Government Manual	741-6000
Other Services	
Electronic and on-line services (voice)	741-6020
Privacy Act Compilation	741-6050

ELECTRONIC RESEARCH

World Wide Web

Full text of the daily Federal Register, CFR and other publications is located at: www.govinfo.gov.

Federal Register information and research tools, including Public Inspection List and electronic text are located at: www.federalregister.gov.

E-mail

FEDREGTOC (Daily Federal Register Table of Contents Electronic Mailing List) is an open e-mail service that provides subscribers with a digital form of the Federal Register Table of Contents. The digital form of the Federal Register Table of Contents includes HTML and PDF links to the full text of each document.

To join or leave, go to <https://public.govdelivery.com/accounts/USGPOOFR/subscriber/new>, enter your email address, then follow the instructions to join, leave, or manage your subscription.

PENS (Public Law Electronic Notification Service) is an e-mail service that notifies subscribers of recently enacted laws.

To subscribe, go to <http://listserv.gsa.gov/archives/publaws-l.html> and select *Join or leave the list (or change settings)*; then follow the instructions.

FEDREGTOC and **PENS** are mailing lists only. We cannot respond to specific inquiries.

Reference questions. Send questions and comments about the Federal Register system to: fedreg.info@nara.gov

The Federal Register staff cannot interpret specific documents or regulations.

FEDERAL REGISTER PAGES AND DATE, APRIL

19547-19796.....	3
19797-20058.....	4
20059-20382.....	5

CFR PARTS AFFECTED DURING APRIL

At the end of each month the Office of the Federal Register publishes separately a List of CFR Sections Affected (LSA), which lists parts and sections affected by documents published since the revision date of each title.

3 CFR		32 CFR	
Proclamations:		199.....	19844
10537.....	19797	33 CFR	
10538.....	19799	100.....	19856, 19857
10539.....	20357	Proposed Rules:	
10540.....	20359	117.....	20082
10541.....	20361	165.....	19579, 20084
10542.....	20363	37 CFR	
10543.....	20367	1.....	19862
10544.....	20369	41.....	19862
10545.....	20371	38 CFR	
10546.....	20373	17.....	19862
10547.....	20375	Proposed Rules:	
10548.....	20379	46.....	19581
10549.....	20381	40 CFR	
10 CFR		180.....	19873
430.....	19801	Proposed Rules:	
14 CFR		52.....	19901, 20086
25.....	19547	141.....	20092
33.....	19801	142.....	20092
39.....	19811, 19815, 20059, 20062, 20065, 20067, 20070	42 CFR	
71.....	19817, 19819, 19820, 19821, 19822, 19823	Proposed Rules:	
97.....	20073, 20074	418.....	20022
Proposed Rules:		424.....	20022
71.....	19895	43 CFR	
15 CFR		1600.....	19583
922.....	19824	6100.....	19583
17 CFR		47 CFR	
Proposed Rules:		73.....	19549, 20076
232.....	20212	48 CFR	
240.....	20212	538.....	20077
242.....	20212	552.....	20077
249.....	20212	49 CFR	
21 CFR		Proposed Rules:	
Proposed Rules:		216.....	19730
1308.....	19896	231.....	19730
23 CFR		238.....	19730
Proposed Rules:		50 CFR	
661.....	19571	17.....	19549, 19880
28 CFR		622.....	20079
0.....	19830	648.....	19559
30 CFR		679.....	20080
Proposed Rules:		Proposed Rules:	
585.....	19578	648.....	20015
31 CFR			
591.....	19840, 19842		

LIST OF PUBLIC LAWS

Note: No public bills which have become law were received by the Office of the Federal Register for inclusion

in today's **List of Public Laws**.
Last List January 23, 2023

Public Laws Electronic Notification Service (PENS)

PENS is a free email notification service of newly

enacted public laws. To subscribe, go to <https://portalguard.gsa.gov/—layouts/PG/register.aspx>.

Note: This service is strictly for email notification of new laws. The text of laws is not available through this service. **PENS** cannot respond to specific inquiries sent to this address.