SECURITIES AND EXCHANGE COMMISSION

17 CFR Parts 230, 232, 239, 270, 274, 275, and 279

[Release Nos. 33–11028; 34–94197; IA–5956; IC–34497; File No. S7–04–22]

RIN 3235–AN08

Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies

AGENCY: Securities and Exchange Commission.

ACTION: Proposed rule.

SUMMARY: The Securities and Exchange Commission is proposing new rules under the Investment Advisers Act of 1940 (''Advisers Act'') and the Investment Company Act of 1940 (''Investment Company Act'') to require registered investment advisers (''advisers'') and investment companies (''funds'') to adopt and implement written cybersecurity policies and procedures reasonably designed to address cybersecurity risks. The Commission also is proposing a new rule and form under the Advisers Act to require advisers to report significant cybersecurity incidents affecting the adviser, or its fund or private fund clients, to the Commission. With respect to disclosure, the Commission is proposing amendments to various forms regarding the disclosure related to significant cybersecurity risks and cybersecurity incidents that affect advisers and funds and their clients and shareholders. Finally, we are proposing new recordkeeping requirements under the Advisers Act and Investment Company Act.

DATES: Comments should be received on or before April 11, 2022.

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 S7–04–22 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 S7–04–22. 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: Juliet Han, Senior Counsel; Thomas Strumpf, Senior Counsel; Christopher Staley, Branch Chief; or Melissa Gainor, Assistant Director, at (202) 551–6787, Investment Adviser Regulation Office, Division of Investment Management, (202) 551–6787 or *IArules@sec.gov;* Y. Rachel Kuo, Senior Counsel; Amanda Hollander Wagner, Branch Chief; or Brian McLaughlin Johnson, Assistant Director, Investment Company Regulation Office, Division of Investment Management, (202) 551–6792 or *IM-Rules@sec.gov;* David Joire, Senior Special Counsel, at (202) 551–6825, Chief Counsel's Office, Division of Investment Management, (202) 551–6825 or *IMOCC@sec.gov,* Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549–8549.

SUPPLEMENTARY INFORMATION: The Securities and Exchange Commission (''Commission'') is proposing for public comment 17 CFR 275.206(4)–9 (''proposed rule 206(4)–9'') and 17 CFR 275.204–6 (''proposed rule 204–6'') under the Advisers Act [15 U.S.C. 80b–1 *et seq.*]; 17 CFR 270.38a–2 (''proposed rule 38a–2'') under the Investment Company Act [15 U.S.C. 80a–1 *et seq.*]; and new Form ADV–C [referenced in 17 CFR 279.7] under the Advisers Act; amendments to 17 CFR 275.204–2 (''rule 204–2'') and 17 CFR 275.204–3 (''rule 204–3'') under the Advisers Act; amendments to Form ADV [referenced in 17 CFR 279.1] under the Advisers Act; amendments to Form N–1A [referenced in 17 CFR 274.11A], Form N–2 [referenced in 17 CFR 274.11a–1], Form N–3 [referenced in 17 CFR 274.11b, Form N–4 [referenced in 17 CFR 274.11c], Form N–6 [referenced in 17 CFR 274.11d], Form N–8B–2 [referenced in 17 CFR 274.12], and Form S–6 [referenced in 17 CFR 239.16] under the Investment Company Act and the Securities Act of 1933 (''Securities Act'') [15 U.S.C. 77a *et seq.*]; amendments to 17 CFR 232.11 (''rule 11 of Regulation S–T'') and 17 CFR 232.405 (''rule 405 of Regulation S–T'') under the Securities Exchange Act of 1934 (''Exchange Act'') [15 U.S.C. 78a *et seq.*]; amendments to 17 CFR 230.485 (''rule 485'') under the Securities Act; and amendments to 17 CFR 230.497 (''rule 497'') under the Securities Act.[1]

Table of Contents

I. Introduction
A. Adviser and Fund Cybersecurity Risks
B. Current Legal and Regulatory Framework
C. Overview of Rule Proposal
II. Discussion
A. Cybersecurity Risk Management Policies and Procedures
1. Required Elements
2. Annual Review and Required Written Reports
3. Fund Board Oversight
4. Recordkeeping
B. Reporting of Significant Cybersecurity Incidents to the Commission
1. Proposed Rule 204–6
2. Form ADV–C
C. Disclosure of Cybersecurity Risks and Incidents
1. Proposed Amendments to Form ADV Part 2A
2. Cybersecurity Risks and Incidents Disclosure
3. Requirement To Deliver Certain Interim Brochure Amendments to Existing Clients
4. Proposed Amendments To Fund Registration Statements
III. Economic Analysis
A. Introduction
B. Broad Economic Considerations
C. Baseline
1. Cybersecurity Risks and Practices
2. Regulation
3. Market Structure
D. Benefits and Costs of the Proposed Rule and Form Amendments

[1] Unless otherwise noted, when we refer to the Investment Company Act, we are referring to 15 U.S.C. 80a, and when we refer to rules under the Investment Company Act, we are referring to title 17, part 270 of the Code of Federal Regulations [17 CFR 270]. In addition, unless otherwise noted, when we refer to the Advisers Act, we are referring to 15 U.S.C. 80b, and when we refer to rules under the Advisers Act, we are referring to title 17, part 275 of the Code of Federal Regulations [17 CFR 275].

1. Cybersecurity Policies and Procedures
2. Disclosures of Cybersecurity Risks and Incidents
3. Regulatory Reporting of Cybersecurity Incidents
4. Recordkeeping
E. Effects on Efficiency, Competition, and Capital Formation
F. Alternatives Considered
1. Alternatives to the Proposed Policies and Procedures Requirement
2. Modify Requirements for Structuring Disclosure of Cybersecurity Risks and Incidents
3. Public Disclosure of Form ADV–C
IV. Paperwork Reduction Act Analysis
A. Introduction
B. Rule 206(4)–9
C. Rule 38a–2
D. Rule 204–2
E. Rule 204–6
F. Form ADV–C
G. Form ADV
H. Rule 204–3
I. Form N–1A
J. Form N–2
K. Form N–3
L. Form N–4
M. Form N–6
N. Form N–8B–2 and Form S–6
O. Investment Company Interactive Data
P. Request for Comment
V. Initial Regulatory Flexibility Act Analysis
A. Reason for and Objectives of the Proposed Action
B. Legal Basis
C. Small Entities Subject to the Rules and Rule Amendments
D. Projected Reporting, Recordkeeping and Other Compliance Requirements
E. Duplicative, Overlapping, or Conflicting Federal Rules
F. Significant Alternatives
G. Solicitation of Comments
VI. Consideration of Impact on the Economy
VII. Statutory Authority

I. Introduction

A. Adviser and Fund Cybersecurity Risks

Advisers and funds play an important role in our financial markets and increasingly depend on technology for critical business operations.[2] Advisers and funds are exposed to, and rely on, a broad array of interconnected systems and networks, both directly and through service providers such as custodians, brokers, dealers, pricing services, and other technology vendors. Advisers also increasingly use digital engagement tools and other technology to engage with clients and develop and provide investment advice.[3] As a result, they face numerous cybersecurity risks and may experience cybersecurity incidents that can cause, or be exacerbated by, critical system or process failures.[4]

At the same time, cyber threat actors have grown more sophisticated and may target advisers and funds, putting them at risk of suffering significant financial, operational, legal, and reputational harm.[5] Cybersecurity incidents affecting advisers and funds also can cause substantial harm to their clients and investors. For example, cybersecurity incidents caused by malicious software (also known as malware) can cause the loss of adviser, fund, or client data. Cybersecurity incidents can prevent an adviser or fund from executing its investment strategy or an adviser, fund, client, or investor from accessing an account, which can lead to financial losses for clients or investors. In addition, cybersecurity incidents can lead to the theft of intellectual property, confidential or proprietary information, or client assets.

An adviser or a fund may incur substantial remediation costs due to a cybersecurity incident.[6] It may need to reimburse clients for cybersecurity-related losses as well as implement expensive organizational or technological changes to reinforce its ability to respond to and recover from a cybersecurity incident. It may also see an increase in its insurance premiums. In addition, an adviser or fund may face increased litigation, regulatory, or other legal and financial risks or suffer reputational damage, and any of these outcomes could cause its clients or investors to lose confidence in their adviser or fund, or the financial markets more generally. Cybersecurity risk management is therefore a critical area of focus for advisers and funds, and many advisers and funds have taken steps to address cybersecurity risks.

The Commission and its staff have and continue to focus on cybersecurity risks to advisers and their clients, and funds and their investors.[7] We are concerned about the efficacy of adviser and fund practices industry-wide to address cybersecurity risks and incidents, and that less robust practices may not address investor protection concerns. We are also concerned about the effectiveness of disclosures to advisory clients and fund shareholders concerning cybersecurity risks and incidents. The staff has observed a number of practices with respect to firms addressing cybersecurity risk and has provided its observations on a number of occasions to assist firms in enhancing their cybersecurity preparedness.[8] Despite these efforts and in the face of ever-increasing cybersecurity risk, staff continues to observe that certain advisers and funds show a lack of cybersecurity preparedness, which puts clients and investors at risk. We believe that clients and investors would be better protected if advisers and funds were required to have policies and procedures that include specific elements to address cybersecurity risks.

[2] Unless otherwise noted, the term ''fund'' means a registered investment company or a closed-end company that has elected to be treated as a business development company under the Investment Company Act (''BDC'').

[3] Request for Information and Comments on Broker-Dealer and Investment Adviser Digital Engagement Practices, Related Tools and Methods, and Regulatory Considerations and Potential Approaches; Information and Comments on Investment Adviser Use of Technology to Develop and Provide Investment Advice, Investment Advisers Act Release No. 5833 (Aug. 27, 2021) [86 FR 49067 (Sept. 1, 2021)].

[4] *See, e.g.,* Financial Services Information Sharing and Analysis Center, Navigating Cyber 2021 (Mar. 2021), *available at https://www.fsisac.com/navigatingcyber2021-report* (detailing cyber threats that emerged in 2020 and predictions for 2021).

[5] *See, e.g.,* Federal Bureau of Investigation, *2020 Internet Crime Report* (Mar. 17, 2021), at 5, *available at https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf* (''FBI 2020 Internet Crime Report'') (noting the FBI's Internet Crime Complaint Center received more than 791,790 complaints in 2020); *see also* SEC, Office of Compliance, Inspections and Examinations (''OCIE'') (as of December 17, 2020, OCIE was renamed the Division of Examinations (''EXAMS''); SEC, EXAMS 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 SEC registrants); SEC, EXAMS 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 Credential Stuffing Risk Alert''). 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.

[6] *See, e.g.,* Ponemon Institute and IBM Security, *Cost of Data Breach Report 2021* (July 2021), *available at https://www.ibm.com/security/data-breach* (''Cost of Data Breach Report'') (noting the average cost of a data breach in the financial industry in the United States is $5.72 million); FBI 2020 Internet Crime Report, *supra* footnote 5, at 15 (noting that cybercrime victims lost approximately $4.2 billion in 2020).

[7] *See, e.g.,* Division of Investment Management Cybersecurity Guidance, IM Guidance Update No. 2015–02 (Apr. 2015), *available at https://www.sec.gov/investment/im-guidance-2015-02.pdf;* Division of Investment Management, Business Continuity Planning for Registered Investment Companies, IM Guidance Update No. 2016–04 (June 2016), *available at https://www.sec.gov/investment/im-guidance-2016-04.pdf.*

[8] *See, e.g.,* SEC, EXAMS, 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 Cybersecurity Initiative (Apr. 15, 2014), *available at https://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf;* EXAMS' 2015 Cybersecurity Examination Initiative (Sept. 15, 2015), *available at https://www.sec.gov/files/ocie-2015-cybersecurity-examination-initiative.pdf.*

Moreover, the staff has observed that while many advisers and funds already provide disclosure about cybersecurity risks, we are concerned that clients and investors may not be receiving sufficient cybersecurity-related information, particularly with respect to cybersecurity incidents, to assess the operational risk at a firm or the effects of an incident to help ensure they are making informed investment decisions. We therefore seek to improve cybersecurity-related disclosures by addressing cybersecurity more directly.

Finally, we believe that, in the face of ever-increasing cybersecurity risk, advisers and funds should report certain cybersecurity incidents to the Commission to assist in its oversight role. As further discussed below, this would allow the Commission and its staff to understand better the nature and extent of cybersecurity incidents occurring at advisers and funds, how firms respond to such incidents to protect clients and investors, and how cybersecurity incidents affect the financial markets more generally. We believe requiring advisers and funds to report the occurrence of significant cybersecurity incidents would bolster the efficiency and effectiveness of our efforts to protect investors, other market participants, and the financial markets in connection with cybersecurity incidents. Accordingly, we are proposing a set of comprehensive reforms to address cybersecurity risks for advisers and funds, enhance disclosure of information regarding cybersecurity risks and significant cybersecurity incidents, and require the reporting of significant cybersecurity incidents to the Commission.

B. Current Legal and Regulatory Framework

As fiduciaries, advisers are required to act in the best interest of their clients at all times.[9] Advisers owe their clients a duty of care and a duty of loyalty. An adviser's fiduciary obligation to its clients includes the obligation to take steps to protect client interests from being placed at risk because of the adviser's inability to provide advisory services.[10] These include steps to minimize operational and other risks that could lead to significant business disruptions or a loss or misuse of client information. Under this framework, advisers today consider a number of rules and regulations, which indirectly address cybersecurity. As discussed above, cybersecurity incidents can lead to significant business disruptions, including lapses in communication or the inability to place trades. In addition, these disruptions can lead to the loss of access to accounts or investments, potentially resulting in the loss or theft of data or assets. Thus, advisers should take steps to minimize cybersecurity risks in accordance with their fiduciary obligations.

Additionally, 17 CFR 275.206(4)–7 (''Advisers Act compliance rule'') requires advisers to consider their fiduciary and regulatory obligations and formalize policies and procedures reasonably designed to address them.[11] While the Advisers Act compliance rule does not enumerate specific elements that an adviser must include in its compliance program, an adviser generally should first identify conflicts of interest and other compliance factors creating risk exposure for the firm and its clients in light of the firm's particular operations and then design policies and procedures that address those risks.[12] Because cybersecurity incidents could create significant operational disruptions and losses to clients and investors, we understand that advisers often consider the cybersecurity risks created by their particular circumstances when developing their compliance policies and procedures under the Advisers Act compliance rule and tailor their policies and procedures to address those risks.

Similarly, 17 CFR 270.38a–1 (''Investment Company compliance rule'') requires funds to adopt and implement written policies and procedures reasonably designed to prevent violations of the Federal securities laws by the fund, including policies and procedures that provide for the oversight of compliance by each investment adviser, principal underwriter, administrator, and transfer agent of the fund (''named service providers'').[13] We understand that funds take into account the specific risks they face, often including any specific cybersecurity risks, when developing their compliance policies and procedures under the Investment Company compliance rule.

Other Commission rules require advisers and funds to consider cybersecurity. For example, advisers and funds subject to 17 CFR 248.1 through 248.31 (''Regulation S–P'') are required to, among other things, adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information.[14] These written policies and procedures must be reasonably designed to protect the security and confidentiality of customer records and information. They must also be reasonably designed to protect against any anticipated threats or hazards, unauthorized access to, or use of customer records or information that could result in substantial harm or inconvenience to any customer.[15]

Moreover, advisers and funds subject to 17 CFR 248.201 through 202 (''Regulation S–ID'') must develop and implement a written identity theft program.[16] A Regulation S–ID program must include reasonable policies and procedures to identify and detect relevant red flags, as well as respond appropriately to red flags so as to prevent and mitigate identity theft.

[9] *SEC* v. *Capital Gains Research Bureau, Inc.,* 375 U.S. 180, 194 (1963); *see also* Commission Interpretation Regarding Standard of Conduct for Investment Advisers, Investment Advisers Act Release No. 5248 (June 5, 2019) [84 FR 33669 (July 12, 2019)], at 6–8.

[10] *See* Compliance Programs of Investment Companies and Investment Advisers, Investment Advisers Act Release No. 2204 (Dec. 17, 2003) [68 FR 74714 (Dec. 24, 2003)], at n.22 (''Compliance Program Release'') (noting this fiduciary obligation in the context of business continuity plans).

[11] The Advisers Act compliance rule requires an adviser that is registered, or required to be registered, with the Commission to: (1) Adopt and implement written policies and procedures reasonably designed to prevent violations of the Advisers Act by the adviser and its supervised persons; (2) designate a chief compliance officer (''CCO'') responsible for administering the policies and procedures; and (3) review the adequacy of the policies and procedures and the effectiveness of their implementation at least annually.

[12] *See* Compliance Program Release, *supra* footnote 10, at n.22 and accompanying text. The Commission included business continuity, safeguards for the privacy of client records and information, as well as the accuracy of disclosures made to investors, clients and regulators in a list of general areas it believes, at a minimum, an adviser's compliance program should address to the extent they are relevant to the adviser. *Id.*

[13] The Investment Company compliance rule also requires the fund to: (1) Designate a CCO responsible for administering the policies and procedures, subject to certain requirements, including providing the fund's board with an annual report; and (2) review the adequacy of the policies and procedures and the effectiveness of their implementation at least annually.

[14] *See* Privacy of Consumer Financial Information (Regulation S–P), Investment Advisers Act Release No. 1883 (June 22, 2000) [65 FR 40334 (June 29, 2000)] (''Regulation S–P Release''); *see also* Disposal of Consumer Report Information, Investment Advisers Act Release No. 2332 (Dec. 2, 2004) [69 FR 71322 (Dec. 8, 2004)] (''Disposal of Consumer Report Information Release'') (requiring written policies and procedures under Regulation S–P); Compliance Program Release, *supra* footnote 10, at n.21 and accompanying text (stating expectation that policies and procedures would address safeguards for the privacy protection of client records and information and noting the applicability of Regulation S–P).

[15] 17 CFR 248.30. Regulation S–P also establishes general requirements and restrictions on, as well as exceptions to, the ability of financial institutions to disclose nonpublic personal information about customers to nonaffiliated third parties.

[16] *See* Identity Theft Red Flags Rules, Investment Advisers Act Release No. 3582 (Apr. 10, 2013) [78 FR 23638 (Apr. 19, 2013)] (''Identity Theft Release'').

Regulation S–ID programs must also be reviewed periodically to ensure that changes in the identity theft risk landscape are reflected and provide for the continued administration of the program, including staff training and appropriate and effective oversight of service providers.[17] In addition, because fraudulent activity could result from cybersecurity or data breaches from insiders, such as advisory or fund personnel, advisers and funds often take precautions concerning information security specifically related to insiders.[18]

C. Overview of Rule Proposal

While some funds and advisers have implemented cybersecurity programs under the existing regulatory framework, there are no Commission rules that specifically require firms to adopt and implement comprehensive cybersecurity programs. Based on our staff's examinations of advisers and funds, we are concerned that some funds and advisers that are registered with us have not implemented reasonably designed cybersecurity programs. As a result, these firms' clients and investors may be at greater risk of harm than those of funds and advisers that have in place appropriate plans to address cybersecurity risks.

To address these concerns, we are proposing rules 206(4)–9 under the Advisers Act and 38a–2 under the Investment Company Act, which would require advisers and funds that are registered or required to be registered with us to implement cybersecurity policies and procedures addressing a number of elements.[19] Under the proposed rules, such an adviser's or fund's cybersecurity policies and procedures generally should be tailored based on its business operations, including its complexity, and attendant cybersecurity risks. Further, the proposed rules would require advisers and funds, at least annually, to review and evaluate the design and effectiveness of their cybersecurity policies and procedures, which would allow them to update them in the face of ever-changing cyber threats and technologies. We believe that advisers and funds should be required to adopt and implement policies and procedures that address a number of elements to increase the likelihood that they are prepared to face a cybersecurity incident (whether that threat comes from an outside actor or the firm's personnel), and that investors and other market participants are protected from a cybersecurity incident that could significantly affect a firm's operations and lead to significant harm to clients and investors.

To address cybersecurity more directly, we also are proposing amendments to adviser and fund disclosure requirements to provide current and prospective advisory clients and fund shareholders with improved information regarding cybersecurity risks and cybersecurity incidents. In particular, we propose amendments to Form ADV for advisers and Forms N–1A, N–2, N–3, N–4, N–6, N–8B–2, and S–6 for funds. We believe these proposed cybersecurity disclosure requirements would enhance investor protection by requiring that cybersecurity risk or incident-related information is available to increase understanding in these areas and help ensure that investors and clients can make informed investment decisions.

In addition, we are proposing to require advisers to report significant cybersecurity incidents affecting the adviser, or its fund or private fund clients, to the Commission on a confidential basis.[20] These reports would bolster the efficiency and effectiveness of our efforts to protect investors in connection with cybersecurity incidents. This reporting would not only help the Commission monitor and evaluate the effects of a cybersecurity incident on an adviser and its clients or a fund and its investors, but also assess the potential systemic risks affecting financial markets more broadly.

Taken together, these reforms are designed to promote a more comprehensive framework to address cybersecurity risks for advisers and funds, thereby reducing the risk that advisers and funds would be not be able to maintain critical operational capability when confronted with a significant cybersecurity incident. These reforms also are designed to give clients and investors better information with which to make investment decisions, and to give the Commission better information with which to conduct comprehensive monitoring and oversight of ever-evolving cybersecurity risks and incidents affecting advisers and funds.

II. Discussion

A. Cybersecurity Risk Management Policies and Procedures

The Commission is proposing rule 206(4)–9 under the Advisers Act and 38a–2 under the Investment Company Act (collectively, ''proposed cybersecurity risk management rules'').[21] The proposed cybersecurity risk management rules would require all advisers and funds to adopt and implement cybersecurity policies and procedures containing certain elements. Advisers and funds of every type and size rely on technology systems and networks and face increasing cybersecurity risks. The rules would therefore require all of these advisers and funds to consider and mitigate cybersecurity risk.[22]

As discussed below, while the proposed cybersecurity risk management rules would require all such advisers and funds to implement cybersecurity hygiene and protection measures, we recognize that there is not a one-size-fits-all approach to addressing cybersecurity risks. As a result, the proposed cybersecurity risk management rules would allow firms to tailor their cybersecurity policies and procedures to fit the nature and scope of their business and address their individual cybersecurity risks.

We request comment on the entities subject to the proposed rules:

1. Should we exempt certain types of advisers or funds from these proposed

[17] *See also* Appendix A to Subpart C of 17 CFR part 248 (setting out Commission guidelines for consideration when implementing an identity theft program).

[18] *See, e.g.,* 17 CFR 270.17j–1; 17 CFR 275.204A–1; *see also generally* Personal Investment Activities of Investment Company Personnel, Investment Company Act Release No. 23958 (Aug. 24, 1999) [64 FR 46821 (Aug. 27, 1999)] (stating that rule 17j–1 prohibits fraudulent, deceptive or manipulative acts by fund personnel in connection with their personal transactions in securities held or to be acquired by the fund); Investment Adviser Codes of Ethics, Investment Advisers Act Release No. 2256 (July 2, 2004) [69 FR 41696 (July 9, 2004)] (stating that rule 204A–1 will benefit advisers by renewing their attention to their fiduciary and other legal obligations, and by increasing their vigilance against inappropriate behavior by employees).

[19] When discussing the requirements proposed in this release, our use of the terms funds and advisers refers to funds and advisers that are registered or required to be registered with the Commission.

[20] *See* 15 U.S.C. 80b–2(a)(29) (defining a ''private fund'' as ''an issuer that would be an investment company, as defined in section 3 of the Investment Company Act of 1940, but for section 3(c)(1) or 3(c)(7) of that Act'').

[21] Section 206(4) of the Advisers Act permits the Commission to define, and prescribe means reasonably designed to prevent, such acts, practices and courses of business conduct as are fraudulent, deceptive or manipulative under the Advisers Act, and to adopt rules reasonably designed to prevent fraud. We are proposing rule 206(4)–9 as a means reasonably designed to prevent fraud. Section 38(a) of the Investment Company Act authorizes the Commission to ''make . . . such rules and regulations . . . as are necessary or appropriate to the exercise of the powers conferred upon the Commission elsewhere in [the Investment Company Act].''

[22] Proposed rule 206(4)–9 would apply to advisers to separately managed accounts and pooled investment vehicles, both private and offered to the public. Proposed rule 38a–2 would apply to mutual funds, exchange-traded funds (''ETFs''), unit investment trusts, registered closed-end funds, and BDCs.

cybersecurity risk management rules? If so, which ones, and why? For example, is there a subset of funds or advisers with operations so limited or staffs so small that the adoption of cybersecurity risk management programs is not beneficial?

2. Should we scale the proposed requirements based on the size of the adviser or fund? If so, which of the elements described below should not be required for smaller advisers or funds? How would we define such smaller advisers or funds? For example, should we define such advisers and funds based on the thresholds that the Commission uses for purposes of the Regulatory Flexibility Act? Would using different thresholds based on assets under management, such as $150 million or $200 million, be appropriate? Would another threshold be more suitable, such as one based on an adviser's or fund's limited operations, staffing, revenues or management?

1. Required Elements of Advisers' and Funds' Policies and Procedures

The proposed cybersecurity risk management rules would require advisers and funds to adopt and implement written policies and procedures that are reasonably designed to address cybersecurity risks. We believe that these policies and procedures would help address operational and other risks that could harm advisory clients and fund investors or lead to the unauthorized access to or use of adviser or fund information.[23] The proposed cybersecurity risk management rules enumerate certain general elements that advisers and funds would be required to address in their cybersecurity policies and procedures.[24] They also contain a number of defined terms that apply across the proposed cybersecurity risk management rules as well as the other rule and form amendments we are proposing.[25]

The general elements are designed to enumerate core areas that firms must address when adopting, implementing, reassessing and updating their cybersecurity policies and procedures. We recognize, however, that given the number and varying characteristics (*e.g.,* size, business, and sophistication) of advisers and funds, firms need the ability to tailor their cybersecurity policies and procedures based on their individual facts and circumstances. The proposed cybersecurity risk management rules therefore give advisers and funds the flexibility to address the general elements based on the particular cybersecurity risks posed by each adviser's or fund's operations and business practices. In addition, because cybersecurity threats are constantly evolving and measures to address those threats continue to advance, this approach would allow an adviser's or fund's cybersecurity policies and procedures to evolve accordingly as firms reassess their cybersecurity risks in accordance with the proposed cybersecurity risk management rules.

The proposed cybersecurity risk management rules also would provide flexibility for the adviser and fund to determine the person or group of people who implement and oversee the effectiveness of its cybersecurity policies and procedures. Wide-ranging areas of expertise could be needed to manage cybersecurity risk. We understand that cybersecurity may be the responsibility of many individuals within an organization, and expertise may be provided both internally and by third-party experts. Within an adviser or fund organization, various officers or employees may be involved in implementing a cybersecurity program, including those who specialize in technology, risk, compliance, and legal matters. Some advisers and funds may be a part of a larger company structure that shares common cybersecurity and information technology (''IT'') personnel, resources, systems, and infrastructure. Advisers and funds may also utilize third-party cybersecurity experts that provide varying perspectives and are well-positioned to understand and assist in managing risks. Multiple perspectives may assist in building a stronger cybersecurity program, and also would allow firms to add expertise as needed in the rapidly changing cybersecurity environment. We believe that this approach allows advisers and funds of differing sizes, organizational structures, and investment strategies to tailor their cybersecurity programs effectively to their operations.

Under the proposed cybersecurity risk management rules, an adviser or fund may choose to administer its cybersecurity policies and procedures using in-house resources with appropriate knowledge and expertise. The proposed framework also does not preclude an adviser or fund from using a third party's cybersecurity risk management services, subject to appropriate oversight. Similarly, subject to appropriate oversight, a fund's adviser or sub-adviser could administer any of the functions of the fund's required policies and procedures.[26] Whether the administrators of an adviser's or fund's cybersecurity policies and procedures are in-house or a third party, reasonably designed policies and procedures must empower these administrators to make decisions and escalate issues to senior officers as necessary for the administrator to carry out the role effectively (*e.g.,* the policies and procedures could include an explicit escalation provision to the adviser's or fund's senior officers). Reasonably designed cybersecurity policies and procedures generally should specify which groups, positions, or individuals, whether in-house or third-party, are responsible for implementing and administering the policies and procedures, including specifying those responsible for communicating incidents internally and

[23] After gaining access to an adviser's or a fund's information systems, an attacker could use this access to steal, disclose, delete, destroy, or modify adviser or fund information, as well as steal client or investor assets.

[24] Funds and advisers may wish to consult a number of resources in connection with these elements. *See, e.g.,* National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity,* Version 1.1 (Apr. 16, 2018), *available at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf* (''NIST Framework''); Cybersecurity and Infrastructure Security Agency (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.*

[25] The proposed defined terms for advisers and funds are the same in most instances, except where necessary to take into account relevant differences in each of the proposed cybersecurity risk management rules. For example, the majority of differences between proposed rules 206(4)–9 and 38a–2 are that the rule applicable to advisers includes the word ''adviser'' in a number of terms (*e.g.,* ''adviser information systems'' and ''adviser information'') whereas the rule applicable to funds includes the word ''fund'' (*e.g.,* ''fund information systems'' and ''fund information.'') in a number of terms. We understand that there are different definitions for a number of common terms in the realm of cybersecurity, and we propose terms derived from a number established sources. *See* Presidential Policy Directive—United States Cyber Incident Coordination (July 26, 2016) (''PPD–41''); 6 U.S.C. 1501 (2021); 44 U.S.C. 3502 (2021); 44 U.S.C. 3552 (2021); *see also* National Institute of Standards and Technology (NIST), Computer Security Resource Center Glossary (last visited Feb. 2, 2022), *available at https://csrc.nist.gov/glossary* (''NIST Glossary''). We believe the proposed terms are sufficiently precise and aligned with each other for advisers and funds to understand and utilize in connection with the proposed rules. Using common terms and similar definitions is intended to facilitate compliance and reduce regulatory burdens.

[26] A sub-adviser that is delegated advisory services by an adviser is subject to its own cybersecurity obligations under the proposed risk management rules. Delegating any or all cybersecurity-related activities does not exempt an adviser or fund from its oversight responsibilities.

making decisions with respect to reporting to the Commission and disclosing to clients and investors certain incidents.

We believe that this approach would help ensure that advisers and funds adopt and implement cybersecurity policies and procedures that are effective in mitigating cybersecurity risk without being overly burdensome or costly to implement. Moreover, we believe the proposed cybersecurity risk management rules would benefit advisory clients and fund investors because advisers and funds would be better prepared to confront a cybersecurity incident if (and when) it occurs.[27] The proposed rules also would help to ensure that advisers and funds focus their efforts and resources on mitigating the cybersecurity risks associated with their operations and business practices.[28]

a. Risk Assessment

The first step in designing effective cybersecurity policies and procedures is assessing and understanding the cybersecurity risks facing an adviser or a fund.[29] As an element of an adviser's or fund's reasonable policies and procedures, the proposed cybersecurity risk management rules would require advisers and funds periodically to assess, categorize, prioritize, and draft written documentation of, the cybersecurity risks associated with their information systems and the information residing therein.[30] The proposed cybersecurity risk management rules would require advisers and funds, when conducting this risk assessment, to:

(i) Categorize and prioritize cybersecurity risks based on an inventory of the components of their information systems, the information residing therein, and the potential effect of a cybersecurity incident on the advisers and funds; and

(ii) Identify their service providers that receive, maintain or process adviser or fund information, or that are permitted to access their information systems, including the information residing therein, and identify the cybersecurity risks associated with the use of these service providers.[31]

The proposed rules would also require written documentation of any risk assessment. Generally, this risk assessment should inform senior officers at the adviser or the fund of the risks specific to the firm and support responses to cybersecurity risks by identifying cybersecurity threats to information systems that, if compromised, could result in significant cybersecurity incidents.[32] In general, an adviser or fund's cybersecurity program should be reasonably designed to ensure its operational capability, including resiliency and capacity of information systems, when confronted with a cybersecurity incident, whether at the adviser or at a service provider that may access adviser or fund information.

An adviser or fund generally should assess, categorize, and prioritize the cybersecurity risks created by its information systems and information residing therein in light of the firm's particular operations.[33] For example, advisers may be subject to different risks as a result of international operations, insider threats, or remote or traveling employees. Only after assessing, analyzing, categorizing, and prioritizing its risks can an adviser or fund develop and implement cybersecurity policies and procedures designed to mitigate those risks. The proposed cybersecurity risk management rules would also require advisers and funds to reassess and re-prioritize their cybersecurity risks periodically as changes that affect these risks occur. Due to the ongoing and emerging nature of cybersecurity threats, and the proposed requirement discussed below that advisers and funds review their cybersecurity policies and procedures no less frequently than annually, we are not proposing that such a reassessment occur at specified intervals.[34] Instead, advisers and funds should reassess their cybersecurity risks as they arise to reflect internal changes, such as changes to its business, online presence, or client web access, or external changes, such as changes in the evolving technology and cybersecurity threat landscape, and inform senior officers of the adviser or fund of any material changes to the risk assessment. In assessing ongoing and emerging cybersecurity threats, advisers and funds generally should monitor and consider updates and guidance from private sector and governmental resources, such as the Financial Services Information Sharing and Analysis Center (''FS–ISAC'') and the

[27] We propose to define ''cybersecurity incident'' as ''an unauthorized occurrence on or conducted through [an adviser's or a fund's] information systems that jeopardizes the confidentiality, integrity, or availability of [an adviser's or a fund's] information systems or any [adviser or fund] information residing therein.'' *See* proposed rules 206(4)–9 and 38a–2. This proposed term is derived from the 44 U.S.C. 3552, which is incorporated into PPD–41 (defining ''cyber incident''), and included in the NIST Glossary (defining ''incident''). We believe this term is sufficiently understood and broad enough to encompass incidents that could adversely affect an adviser's or fund's information systems or information residing therein, such as gaining access without authorization or by exceeding authorized access to such systems and information that could lead, for example, to the modification or destruction of systems and information.

[28] We propose to define ''cybersecurity risk'' as the ''financial, operational, legal, reputational, and other adverse consequences that could stem from cybersecurity incidents, threats, and vulnerabilities.'' *See* proposed rules 206(4)–9 and 38a–2. This proposed term is designed to capture risks that an adviser or fund faces when confronted with incidents, threats and vulnerabilities, and we believe is generally well understood in connection with integrating cybersecurity into enterprise risk management. *See generally* NIST Framework, *supra* footnote 24.

[29] Risk assessments are included as an element in many cybersecurity frameworks. *See, e.g.,* NIST Framework, *supra* footnote 24.

[30] *See* proposed rules 206(4)–9(a)(1) and 38a–2(a)(1). ''Adviser information systems'' is proposed to be defined as ''information resources owned or used by the adviser, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of adviser information to maintain or support the adviser's operations.'' *See* proposed rule 206(4)–9; *see also* proposed rule 38a–2 (defining ''fund information systems''). The definitions of these terms are designed to be broad enough to encompass all the electronic information resources owned or used by an adviser or a fund.

[31] ''Adviser information'' is proposed to be defined as ''any electronic information related to the adviser's business, including personal information, received, maintained, created, or processed by the adviser.'' The term ''personal information'' is proposed to be defined as: ''(1) any information that can be used, alone or in conjunction with any other information, to identify an individual, such as name, date of birth, place of birth, telephone number, street address, mother's maiden name, Social Security number, driver's license number, electronic mail address, account number, account password, biometric records or other non-public authentication information; or (2) Any other non-public information regarding a client's account.'' *See* proposed rule 206(4)–9; *see also* proposed rule 38a–2 (the term ''personal information'' in proposed rule 38a–2 does not include the second prong of the same term contained in proposed rule 206(4)–9). The definitions of ''personal information'' for advisers and funds are derived from a number of established sources and aim to capture a broad array of personal information that can reside on an adviser's or a fund's information systems. *See e.g.,* Regulation S–ID, *supra* footnote 16 (defining ''identifying information''); NIST Glossary, *supra* footnote 24 (defining ''personal information'' and ''personally identifiable information'').

[32] ''Cybersecurity threat'' is proposed to be defined as ''any potential occurrence that may result in an unauthorized effort to adversely affect the confidentiality, integrity or availability of [an adviser's or a fund's] information systems or any [adviser or fund] information residing therein.'' *See* proposed rules 206(4)–9 and 38a–2.

[33] Some firms use an enterprise governance, risk management and compliance (''EGRC'') system to manage cybersecurity risk and compliance by creating policies, procedures, and internal controls that assist in identifying cybersecurity risks related to particular systems.

[34] *See* discussion in section II.A.2 below (advisers and funds must review their cybersecurity policies and procedures no less frequently than annually, including preparing and reviewing a written report that is designed to address cybersecurity risk assessments, among other items).

Department of Homeland Security's CISA.[35]

Because many advisers and funds are exposed to cybersecurity risks through the technology of their service providers, a risk assessment also must identify service providers that receive, maintain, or process adviser or fund information, or that are permitted to access their information systems, including the information residing therein and the cybersecurity risks they present.[36] For example, advisers may use service providers who provide trade order management systems that allow the adviser to automate all or some of the adviser's trading, and advisers should consider any cybersecurity risks presented by these services. In identifying cybersecurity risks, an adviser or fund should consider the service provider's cybersecurity practices, including whether any systems used have the resiliency and capacity to process transactions in an accurate, timely and efficient manner, and their capability to protect information and systems (including response and recovery procedures in response to any incidents and any escalation protocols contained therein).

Generally, an adviser or fund should take into account whether a cybersecurity incident at a service provider could lead to the unauthorized access or use of adviser or fund information or technology or process failures. For an adviser, such unauthorized access or use or failure could disrupt portfolio management, trade execution, or other aspects of its operations. For example, an adviser may retain a cloud service provider for maintaining required books and records. If all of the adviser's books and records were concentrated at this cloud service provider and a cybersecurity incident were to occur at the cloud service provider—or any service provider maintaining the adviser's books and records—there could potentially be detrimental data loss affecting the ability of the adviser to provide services and comply with regulatory obligations. Accordingly, as part of identifying the cybersecurity risks associated with using this cloud service provider, the adviser 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.

For a fund, similar unauthorized access or use or failure could affect the valuation of portfolio securities or the processing of shareholder transactions, which could significantly disrupt the fund's operations. For example, a fund may rely on service providers to calculate the fund's net asset value (''NAV''). The inability of an administrator, pricing vendor, or accounting system to calculate a fund's NAV due to a cybersecurity incident would force a fund to consider alternatives. As part of its cybersecurity program and its oversight of service providers, a fund that relies on any service provider for calculating NAV generally should assess the potential cybersecurity risks presented by that service provider and develop procedures to respond to and mitigate disruptions, including by identifying alternative processes or vendors to calculate the fund's NAV.[37] Accordingly, the fund's risk assessment generally should involve inquiring about that service provider's business continuity and disaster recovery protocols with respect to a cybersecurity incident.

b. User Security and Access

As an element of an adviser's or fund's reasonably designed policies and procedures, the proposed cybersecurity risk management rules would require controls designed to minimize user-related risks and prevent the unauthorized access to information and systems.[38] Their policies and procedures must include:

(1) Requiring standards of behavior for individuals authorized to access adviser or fund information systems and any adviser or fund information residing therein, such as an acceptable use policy;

(2) Identifying and authenticating individual users, including 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, replacement, and revocation of passwords or methods of authentication;

(4) Restricting access to specific adviser or fund information systems or components thereof and adviser or fund information residing therein solely to individuals requiring access to such systems and information as is necessary for them to perform their responsibilities and functions on behalf of the adviser or fund; and

(5) Securing remote access technologies used to interface with adviser or fund information systems.

The proposed cybersecurity risk management rules would require advisers and funds, as part of their cybersecurity programs, to address user access controls to restrict system and data access to authorized users.[39] Such controls are necessary to prevent and detect unauthorized access to systems or client or investor data or information. In addition, as remote access and teleworking have become increasingly common, we believe that having such measures is a necessary component of robust and comprehensive cybersecurity policies and procedures.

In designing and implementing user access controls, advisers and funds generally should develop a clear understanding of the need for access to systems, data, functions, and/or accounts, including identifying which users have legitimate needs to access particularly critical or sensitive systems, data, functions, or accounts. For example, a portfolio manager may have privileged access to trading systems that permit him or her to enter trades, while a compliance personnel's access may be limited to reviewing or approving, but not entering, trades.

Access to systems and data can be controlled through a variety of means, including, but not limited to, 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 sensitive information and network resources. Effective controls would also generally include user security and access measures that are regularly monitored not only to provide access to authorized users, but also to remove access for users that are no longer authorized, whether due to removal from a project or termination of employment.

As part of its user access controls, an adviser or fund should also consider what measures are necessary for clients

[35] Information about FS–ISAC is available at *https://www.fsisac.com.* Information about CISA is available at *https://www.cisa.gov.*

[36] Oversight of third-party service provider or vendor risk is a component of many cybersecurity frameworks. *See, e.g.,* NIST Framework, *supra* footnote 24 (discussing supply chain risks associated with products and services an organization uses).

[37] *See generally* Good Faith Determinations of Fair Value, Investment Company Release No. 34128 (Dec. 3, 2020) [86 FR 748 (Jan. 06, 2021)], at text accompanying nn.94–95 (determining fair value in good faith requires the oversight and evaluation of any pricing services used, including approval, monitoring, and evaluation).

[38] *See* proposed rules 206(4)–9(a)(2) and 38a–2(a)(2).

[39] Advisers and funds generally should consider their potential obligations under Regulation S–P and Regulation S–ID to implement certain access controls with respect to protecting client or investor information.

and investors that have access to information systems and information residing on the systems—not only user access controls for its own personnel. For example, an adviser or fund may implement measures that monitor for unauthorized login attempts and account lockouts, and the handling of customer requests, including for user name and password changes. Similarly, well-designed user access controls should assess the need to authenticate or investigate any unusual customer requests (*e.g.,* wire transfer or withdraw requests).

In developing these policies and procedures, an adviser or fund also should take into account the types of technology through which its users access adviser or fund information systems. For example, mobile devices (whether firm-issued or personal devices) that allow employees to access sensitive data and systems may create additional and unique vulnerabilities, including when such devices are used internationally. An adviser or fund may consider limiting mobile or other devices approved for remote access to those issued by the firm or enrolled through a mobile device manager.[40]

In addition, an adviser or fund should consider its practices with respect to securing remote network access and teleworking to define its network perimeter. Advisers and funds generally should implement detection security capabilities that can identify threats on a network's endpoints. For example, they may utilize 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. Advisers and funds should also consider cybersecurity best practices in remote or telework locations. For example, if adviser or fund personnel work remotely at home or in a co-working space, additional cybersecurity risks, such as unsecured or less secure Wi-Fi, may be present, resulting in sensitive information being seen, gathered or stolen by unauthorized persons. Accordingly, firms should consider having policies and procedures for using any mobile or other devices approved for remote access, and implementing security measures and training on device policies and effective security practices.

[40] Advisers and funds 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 such methods may provide less security than other non-SMS based multi-factor authentication methods.

c. Information Protection

As an element of an adviser's or fund's reasonably designed policies and procedures, the proposed cybersecurity risk management rules would require advisers and funds to monitor information systems and protect information from unauthorized access or use, based on a periodic assessment of their information systems and the information that resides on the systems.[41] Such assessment should take into account:

(1) The sensitivity level and importance of adviser or fund information to its business operations;

(2) Whether any adviser or fund information is personal information;

(3) Where and how adviser or fund information is accessed, stored and transmitted, including the monitoring of adviser or fund information in transmission;

(4) Adviser or fund information systems access controls and malware protection; and

(5) The potential effect of a cybersecurity incident involving adviser or fund information on the adviser or fund and its clients or shareholders, including the ability for the adviser to continue to provide investment advice or the fund to continue providing services.

Advisers and funds generally should use the information obtained from this assessment to determine what methods to implement to prevent the unauthorized access or use of such data. For example, an adviser or fund could utilize processes such as encryption, network segmentation, and access controls to ensure that only authorized users have access to sensitive data or information or critical systems.

An adviser or fund could also implement measures reasonably designed to identify suspicious behavior that 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. Such a program may include rules to identify and block the transmission of sensitive data (*e.g.,* account numbers, Social Security numbers, trade information, and source code) from leaving the organization. The program could also include testing of systems, including penetration tests. An adviser or fund could also 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 methods for preventing the unauthorized use of data may differ depending on circumstances specific to an adviser or fund, such as the systems used, the relationship with service providers, or level of access granted to employees or contractors. Appropriate methods would also generally be expected to evolve with changes in technology and the increased sophistication of cybersecurity attacks.

[41] Proposed rules 206(4)–9(a)(3) and 38a–2(a)(3).

In addition, as part of an adviser's or fund's reasonably designed cybersecurity policies and procedures, an adviser or fund would be required to oversee any service providers that receive, maintain, or process adviser or fund information, or are otherwise permitted to access their information systems and any information residing therein. Advisers and funds would be required to document that the adviser or fund is requiring such service providers, pursuant to a written contract, to implement and maintain appropriate measures, including measures similar to the elements advisers and fund must address in their own cybersecurity policies and procedures, designed to protect adviser and fund information and systems. Such policies and procedures generally should also include other oversight measures, such as due diligence procedures or periodic contract review processes, that allow funds and advisers 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 fund and adviser information and systems (*e.g.,* notifying the adviser or fund of cybersecurity incidents that adversely affect an adviser's or fund's information, systems, or operations). Given the significant role played by service providers, we believe this proposed requirement would assist advisers and funds, when considering whether to hire or retain service providers, in assessing whether they are capable of appropriately protecting important information and systems.

d. Threat and Vulnerability Management

As an element of an adviser's or fund's reasonably designed policies and procedures, the proposed cybersecurity risk management rules would require advisers and funds to detect, mitigate, and remediate cybersecurity threats and vulnerabilities with respect to adviser or

fund information and systems.[42] Cybersecurity threats may result in unauthorized access to an adviser's or fund's information systems or any information residing therein that could lead to adverse consequences. Cybersecurity vulnerabilities present weaknesses in adviser or fund information systems that attackers may exploit. Because advisers and funds depend on information systems to process, store, and transmit sensitive information and to conduct business functions, it is essential for advisers and funds to manage cybersecurity threats and vulnerabilities effectively.

Detecting, mitigating, and remediating threats and vulnerabilities is essential to preventing cyber incidents before they occur. Advisers and funds generally should seek to detect cybersecurity threats and vulnerabilities through ongoing monitoring (*e.g.,* comprehensive examinations and risk management processes). Ongoing monitoring of vulnerabilities could include, 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. Advisers and funds generally should also monitor industry and government sources for new threat and vulnerability information that may assist them in detecting cybersecurity threats and vulnerabilities.[43]

In general, once a threat or vulnerability is identified, advisers and funds should consider how to mitigate and remediate the threat or vulnerability, with a view towards minimizing the window of opportunity for attackers to exploit vulnerable hardware and software. Methods for mitigating and remediating threats and vulnerabilities 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.[44] An adviser or a fund should adopt policies and procedures that establish accountability for handling vulnerability reports, and processes for intake, assignment, escalation, remediation, and remediation testing. For example, an adviser or fund may use a vulnerability tracking system that includes severity ratings, and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities.

Advisers and funds should also consider role-specific cybersecurity threat and vulnerability and response training. 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. Advisers and funds that do not proactively address threats and discovered vulnerabilities face an increased likelihood of having their information systems, and the adviser or fund information residing therein, compromised.

e. Cybersecurity Incident Response and Recovery

As an element of an adviser's or fund's reasonable policies and procedures, the proposed cybersecurity risk management rules would require advisers and funds to have measures to detect, respond to, and recover from a cybersecurity incident.[45] These include policies and procedures that are reasonably designed to ensure:

(1) Continued operations of the fund or adviser;

(2) The protection of adviser information systems and the fund or adviser information residing therein;

(3) External and internal cybersecurity incident information sharing and communications; and

(4) Reporting of significant cybersecurity incidents to the Commission.[46]

Finally, the proposed rules would require advisers and funds to prepare written documentation of any cybersecurity incident, including their response and recovery from such an incident.

Cybersecurity incidents can lead to significant business disruptions, including losing the ability to communicate or the ability to access accounts or investments. These incidents also can lead to the unauthorized access or use of adviser or fund information. Having policies and procedures reasonably designed to respond to cybersecurity incidents can help mitigate these significant business disruptions. A cybersecurity program with a clear incident response plan designed to ensure continued operational capability, and the protection of, and access to, sensitive information and data, even if an adviser or fund loses access to its systems, would assist in mitigating the effects of a cybersecurity incident. Advisers and funds, therefore, may wish to consider maintaining physical copies of their incident response plans—and other cybersecurity policies and procedures—to help ensure they can be accessed and implemented during the times they may be needed most.

We believe it is critical for advisers and funds to focus on operational capability, including resiliency and capacity of information systems, so that they can continue to provide services to their clients and investors when facing disruptions resulting from cybersecurity incidents. The ability to recover critical systems or technologies, including those provided by service providers, in a timeframe that meets business requirements, is important to mitigate the consequences of cybersecurity incidents. An adviser or fund may consider implementing safeguards, such as backing up data, which can help facilitate a prompt recovery to allow an adviser or fund to resume operations following a cybersecurity incident that leads to the unauthorized access or use of adviser or fund information.[47]

An incident response plan should also designate adviser or fund personnel to perform specific roles in the case of a cybersecurity incident. This would 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, an incident response plan should generally have a clear escalation protocol to ensure that an adviser's and fund's

[42] Proposed rules 206(4)–9(a)(4) and 38a–2(a)(4). *See* proposed definition of ''cybersecurity threat,'' *supra* footnote 32. ''Cybersecurity vulnerability'' is proposed to be defined as ''a vulnerability in [an adviser's or a fund's] information systems, information system security procedures, or internal controls, including vulnerabilities in their design, maintenance, or implementation that, if exploited, could result in a cybersecurity incident.''

[43] *See supra* footnote 35 and accompanying text; *see also, e.g.,* CISA, National Cyber Awareness System—Alerts, *available at https://us-cert.cisa.gov/ncas/alerts* (last visited Feb. 2, 2022) (providing information about current security issues, vulnerabilities, and exploits).

[44] Advisers and funds should also 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).

[45] Proposed rules 206(4)–9(a)(5) and 38a–2(a)(5).

[46] Incident and response recovery are common elements of many cybersecurity frameworks. *See, e.g.,* NIST Framework, *supra* footnote 24 (setting out incident response and recovery functions and categories, such as planning, improvements (*e.g.,* lessons learned), and communication, in connection with an organization's risk management processes).

[47] Because having easily accessible, accurate backup data could be critical when responding to and recovering from a cybersecurity incident, advisers and funds may wish to consider storing sensitive backup data in immutable, multi-tiered online and offline storage systems.

senior officers, including appropriate legal and compliance personnel, and a fund's board (as applicable) receive necessary information regarding cybersecurity incidents on a timely basis.

Moreover, under proposed rule 204–6 and amendments to Form ADV Part 2A, as well as amendments to funds' disclosure requirements, advisers and funds would have to report any significant cybersecurity incidents to the Commission and make appropriate disclosures to their clients and investors.[48] Accordingly, advisers and funds must include provisions in their policies and procedures designed to ensure their compliance with their reporting and disclosure obligations as part of their cybersecurity incident response.[49]

Advisers and funds should also consider testing their incident response plans to assess their efficacy and to determine whether any changes are necessary, for example, through tabletop or full-scale exercises. As part of the annual review of their policies and procedures, advisers and funds are required to review and assess the design and effectiveness of the policies and procedures and should generally consider amendments to correct any identified weaknesses in their design or effectiveness.[50]

We request comment on the proposed cybersecurity risk management rules:

3. Are the proposed elements of the cybersecurity policies and procedures appropriate? Should we modify or delete any of the proposed elements? Why or why not? For example, should advisers and funds be required, as proposed, to conduct a risk assessment as part of their cybersecurity policies and procedures? Should we require that a risk assessment include specific components (*e.g.,* identification and documentation of vulnerabilities and threats, identification of the business effect of threats and likelihood of incidents occurring, identification and prioritization of responses), or require written documentation for risk assessments? Should the rules require policies and procedures related to user security and access, as well as information protection?

4. Should there be additional or more specific requirements for who would implement an adviser's or fund's cybersecurity program? For example, should we require an adviser or fund to specify an individual, such as a chief information security officer, or group of individuals as responsible for implementing the program or parts thereof? Why or why not? If so, should such an individual or group of individuals be required to have certain qualifications or experience related to cybersecurity, and if so, what type of qualifications or experience should be required?

5. The Investment Company Act compliance rule prohibits the fund's officers, directors, employees, adviser, principal underwriter, or any person acting under the direction of these persons, from directly or indirectly taking any action to coerce, manipulate, mislead or fraudulently influence the fund's chief compliance officer in the performance of her responsibilities under the rule in order to protect the chief compliance officer from undue influence by those seeking to conceal non-compliance with the Federal securities laws. Should we adopt a similar prohibition for those administering a fund's or adviser's cybersecurity policies and procedures? Why or why not?

6. Would advisers and funds expect to use sub-advisers or other third parties to administer their cybersecurity programs? If so, to what extent and in what manner? Should there be additional or specific requirements for advisers and funds that delegate cybersecurity management responsibilities to a sub-adviser or third party? If so, what requirements and why?

7. Should we include any other cybersecurity program administration requirements? If so, what? For example, should we include a requirement for training staff responsible for day-to-day management of the program? If we require such training, should that involve setting minimum qualifications for staff responsible for carrying out the requirements of the program? Why or why not?

8. Are the proposed rules' definitions appropriate and clear? If not, how could these definitions be clarified within the context of the proposed rules? Should any be modified or eliminated? Are any of them proposed terms too broad or too narrow? Are there other terms that we should define?

9. What are best practices that commenters have developed or are aware of with respect to the types of measures that must be implemented as part of the proposed cybersecurity risk management rules or, alternatively, are there any measures that commenters have found to be ineffective or relatively less effective?

10. What user measures do advisers currently have for using mobile devices or other ways to access adviser or fund information systems remotely? Should we require advisers and funds to implement specific measures to secure remote access technologies?

11. Do advisers and funds currently conduct periodic assessments of their information systems to monitor and protect information from unauthorized use? If so, how often do advisers and funds conduct such assessments? Should the proposed rules specify a minimum assessment frequency, and if so, what should that frequency be?

12. Other than what is required to be reported under proposed rule 204–6, should we require any specific measures within an adviser's policies and procedures with respect to cybersecurity incident response and recovery?

13. Should we require that advisers and funds respond to cybersecurity incidents within a specific timeframe? If so, what would be an appropriate timeframe?

14. Should we require advisers and funds to assess the compliance of all service providers that receive, maintain, or process adviser or fund information, or are otherwise permitted to access adviser or fund information systems and any adviser or fund information residing therein, with these proposed cybersecurity risk management rules? Should we expand or narrow this set of service providers? For example, with respect to funds, should this requirement only apply to ''named service providers'' as discussed above?

15. How do advisers and funds currently consider cybersecurity risks when choosing third-party service providers? What due diligence with respect to cybersecurity is involved in selecting a service provider?

16. How do advisers and funds reduce the risk of a cybersecurity incident transferring from the service provider (or a fourth party (*i.e.,* a service provider used by one of an adviser's or fund's service providers)) to the adviser today?

17. Should we require advisers' and funds' cybersecurity policies and procedures to require oversight of certain service providers, including that such service providers implement and maintain appropriate measures designed to protect a fund's or an adviser's

[48] *See* proposed rule 204–6; *see also infra* sections II.B and C.

[49] Although an adviser's or a fund's initial focus may be on protecting its clients and investors, it may also 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. 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 also* FBI, What We Investigate, Cyber Crime, *available at https://www.fbi.gov/investigate/cyber* (last visited Feb. 2, 2022).

[50] *See* proposed rules 206(4)–9(b) and 38a–2(b).

information and information systems pursuant to written contract? Do advisers and funds currently include specific cybersecurity and data protection provisions in their agreements with service providers? If so, what provisions are the most important? Do they address potential cybersecurity risks that could result from a cybersecurity incident occurring at a fourth party? Should any contractual provisions be specifically required as part of these rules? Should this requirement apply to a more limited subset of service providers? If so, which service providers? For example, should we require funds to include such provisions in their agreements with advisers that would be subject to proposed rule 206(4)–9? Are there other ways we should require protective actions by service providers?

18. Do advisers or funds currently consider their or their service providers' insurance policies, if any, when responding to cybersecurity incidents? Why or why not?

19. Are advisers and funds currently able to obtain information from or about their service providers' cybersecurity practices (*e.g.,* policies, procedures, and controls) to effectively assess them? What, if any, challenges do advisers and funds currently have in obtaining such information? Are certain advisers or funds (*e.g.,* smaller or larger firms) more easily able to obtain such information?

2. Annual Review and Required Written Reports

The proposed cybersecurity risk management rules would require advisers and funds to review their cybersecurity policies and procedures no less frequently than annually.[51] Advisers and funds must, at least annually: (1) Review and assess the design and effectiveness of the cybersecurity policies and procedures, including whether they reflect changes in cybersecurity risk over the time period covered by the review; and (2) prepare a written report. The report would, at a minimum, describe the annual review, assessment, and any control tests performed, explain the results thereof, document any cybersecurity incident that occurred since the date of the last report, and discuss any material changes to the policies and procedures since the date of the last report.

The annual review requirement is designed to require advisers and funds to evaluate whether their cybersecurity policies and procedures continue to work as designed and whether changes are needed to assure their continued effectiveness, including oversight of any delegated responsibilities. The written report should be prepared or overseen by the persons who administer the adviser's or fund's cybersecurity policies and procedures and should consider any risk assessments performed by the adviser or fund. We recognize that a cybersecurity expert may provide needed expertise and perspective to the annual review, but additional adviser or fund personnel generally should also participate to provide their organizational perspective, as well as ensure accountability and appropriate resources.

We request comment on the proposed requirements for a review and assessment of the policies and procedures and a related written report:

20. Should there be additional, fewer, or more specific requirements for the annual review or written report? Why or why not?

21. Is the proposed requirement for advisers and funds to review their cybersecurity policies and procedures at least annually appropriate? Is this minimum review period too long or too short? Why or why not?

22. Should the annual review include whether the cybersecurity policies and procedures reflect changes in cybersecurity risk over the time period covered by the review? Why or why not?

23. Should management, a cybersecurity officer, or a centralized committee be designated to conduct the annual review and prepare the report? Would additional specificity promote accountability and adequate resources? Should relevant expertise be required? Why or why not?

24. Would the proposed annual review raise any particular challenges for smaller or different types of advisers or funds? If so, what could we do to help mitigate these challenges?

25. Are there any conflicts of interest if the same adviser or fund officers implement the cybersecurity program and also conduct the annual review? How can those conflicts be mitigated or eliminated? Should advisers and funds be required to have their cybersecurity policies and procedures periodically audited by an independent third party to assess their design and effectiveness? Why or why not? If so, are there particular cybersecurity-focused audits or assessments that should be required, and should any such audits or assessments be required to be performed by particular professionals (*e.g.,* certified public accountants)? Would there be any challenges in obtaining such audits, particularly for smaller advisers or funds?

3. Fund Board Oversight

Proposed rule 38a–2 would require a fund's board of directors, including a majority of its independent directors, initially to approve the fund's cybersecurity policies and procedures, as well as to review the written report on cybersecurity incidents and material changes to the fund's cybersecurity policies and procedures that, as described above, would be required to be prepared at least annually.[52] These requirements are designed both to facilitate the board's oversight of the fund's cybersecurity program and provide accountability for the administration of the program. These requirements also would be consistent with a board's duty to oversee other aspects of the management and operations of a fund.[53] Board oversight should not be a passive activity, and the requirements for the board to initially approve the fund's cybersecurity policies and procedures and thereafter to review the required written reports are designed to assist directors in understanding a fund's cybersecurity risk management policies and procedures, as well as the risks they are designed to address.

A fund's independent directors play an important role in overseeing fund activities.[54] We believe this should include reviewing and initially approving a fund's cybersecurity policies and procedures to help ensure that the fund's adviser has committed sufficient resources to the activity. Directors may satisfy their obligation with respect to the initial approval by reviewing summaries of the cybersecurity program prepared by persons who administer the fund's

[51] Proposed rules 206(4)–9(b) and 38a–2(b). As discussed below, the proposed rules would require funds' boards of directors to review funds' required written reports. *See infra* section II.A.3.

[52] Proposed rule 38a–2(c). The board may satisfy its obligation to approve a fund's cybersecurity policies and procedures by reviewing summaries of those policies and procedures. This is similar to how directors may satisfy their obligations under rule 38a–1. *See* Compliance Program Release, *supra* footnote 10, at n.33.

[53] *See, e.g.,* rule 38a–1 under the Investment Company Act; Compliance Program Release, *supra* footnote 10, at n.31.

[54] Fund directors are commonly referred to as ''independent directors'' if they are not ''interested persons'' of the fund. The term ''interested person'' is defined in section 2(a)(19) of the Investment Company Act [15 U.S.C. 80a–2(a)(19)]. If the fund is a unit investment trust, the fund's principal underwriter or depositor must approve the policies and procedures. Proposed rule 38a–2(d). Fund boards, including a majority of independent directors, approve fund advisory contracts, among other oversight functions. *See* Section 15(c) of the Investment Company Act [15 U.S.C. 80a–15(c)]. *See also* rule 38a–1 under the Investment Company Act.

cybersecurity policies and procedures. Any documentation provided to the board with respect to the initial approval should generally serve to familiarize directors with the salient features of the program and provide them with an understanding of the operation and administration of the program. In considering whether to approve the policies and procedures, a board may wish to consider the fund's exposure to cybersecurity risks, including those of its service providers, as appropriate, and any recent threats and incidents to which the fund may have been subject.

The required written reports also would provide fund directors with information necessary to ask questions and seek relevant information regarding the effectiveness of the program and its implementation, and whether the fund has adequate resources with respect to cybersecurity matters, including access to cybersecurity expertise. We anticipate that a fund's board's review of the written reports would naturally involve inquiries about cybersecurity risks arising from the program and any incidents that have occurred.

Boards should also consider what level of oversight of the fund's service providers is appropriate with respect to cybersecurity based on the fund's operations. For example, a board may review the service provider contract and risk assessment (or summaries thereof) of any service providers that receive, maintain or process fund information, or that are permitted to access their information systems, including the information residing therein and the cybersecurity risks they present, in the required written reports. Generally, the board should follow up regarding any questions on the contracts or weaknesses found in the risk assessments as well as the steps the fund has taken to address the fund's overall cybersecurity risks, including as those risks may change over time.

We request comment on the proposed initial board approval of the fund's cybersecurity policies and procedures, as well as the proposed requirement for the board to review the written reports that would be prepared at least annually under the proposed rules:

26. Should the Commission require a fund's board, including a majority of its independent directors, initially to approve the cybersecurity policies and procedures, as proposed? As an alternative, should the Commission require approval by the board, but not specify that this approval also must include approval by a majority of the fund's directors who are not interested persons of the fund? Why or why not?

27. As part of their oversight function, should fund boards also be required to approve the cybersecurity policies and procedures of certain of the fund's service providers (*e.g.,* its investment adviser, principal underwriter, administrator, and transfer agent)? Why or why not? If so, which service providers should be included and why?

28. Should a fund's board, or some designee such as a sub-committee or cybersecurity expert, have oversight over the fund's risk assessments of service providers? Why or why not?

29. Should the Commission require boards to base their approval of cybersecurity policies and procedures on any particular finding, for example, that that they are reasonably designed to prevent violations of the Federal securities laws or reasonably designed to address the fund's cybersecurity risks? Why or why not?

30. Does the release provide adequate guidance to funds' boards regarding their initial approval of the cybersecurity policies and procedures? Why or why not? Should the Commission provide any additional guidance in this regard? If so, what guidance would assist boards in their approval process? For example, should the Commission provide additional guidance on documentation provided to the board with respect to the initial approval?

31. Is the proposed requirement for fund boards to review the required written reports appropriate? The proposed rules would require these reports to be prepared at least annually, and a fund's board would be required to review each such report that is prepared. Should the Commission instead require periodic reviews of a report on the fund's cybersecurity risk management policies and procedures, or specify a shorter or longer frequency for review of such a report? Why or why not?

32. Should the Commission require boards to approve any material changes to the fund's cybersecurity policies and procedures instead of reviewing a written report that discusses such changes? Why or why not?

4. Recordkeeping

As part of the proposed cybersecurity risk management rules, we are proposing new recordkeeping requirements under the Advisers Act and Investment Company Act. Advisers Act rule 204–2, the books and records rule, sets forth requirements for maintaining, making, and retaining books and records relating to an adviser's investment advisory business. We are proposing to amend this rule to require advisers to maintain: (1) A copy of their cybersecurity policies and procedures formulated pursuant to proposed rule 206(4)–9 that are in effect, or at any time within the past five years were in effect; (2) a copy of the adviser's written report documenting the annual review of its cybersecurity policies and procedures pursuant to proposed rule 206(4)–9 in the last five years; (3) a copy of any Form ADV–C filed by the adviser under rule 204–6 in the last five years; (4) records documenting the occurrence of any cybersecurity incident, including any records related to any response and recovery from such an incident, in the last five years; and (5) records documenting an adviser's cybersecurity risk assessment in the last five years.[55] Records documenting the occurrence of a cybersecurity incident may include event or incident logs, as well as longer descriptions depending on the nature and scope of the incident. These proposed amendments would help facilitate the Commission's inspection and enforcement capabilities.

Similarly, proposed rule 38a–2 under the Investment Company Act would require that a fund maintain: (1) A copy of its cybersecurity policies and procedures that are in effect, or at any time within the last five years were in effect; (2) copies of written reports provided to its board; (3) records documenting the fund's annual review of its cybersecurity policies and procedures; (4) any report of a significant fund cybersecurity incident provided to the Commission by its adviser; (5) records documenting the occurrence of any cybersecurity incident, including any records related to any response and recovery from such an incident; and (6) records documenting the fund's cybersecurity risk assessment.[56] These records would have to be maintained for five years, the first two years in an easily accessible place.[57]

We request comments on the proposed recordkeeping requirements:

33. Are the records that we propose to require advisers and funds to keep relating to the proposed cybersecurity risk management rules appropriate? Why or why not? Should advisers and

[55] *See* proposed rule 204–2(a)(17)(i), (iv) through (vii).

[56] *See* proposed rule 38a–2(e). If the fund is a unit investment trust, copies of materials provided to its principal underwriter or depositor should be maintained for at least five years after the end of the fiscal year in which the documents were provided.

[57] *See* proposed rule 38a–2(e). A copy of the fund's policies and procedures that are in effect, or were at any time within the past five years in effect, must be kept in an easily accessible place for five years. *See* proposed rule 38a–2(e)(1).

funds have to keep any additional or fewer records, and if so, what records?

34. Do advisers or funds have concerns it will be difficult to retain any of documents? Could this place an undue burden on smaller advisers or funds?

B. Reporting of Significant Cybersecurity Incidents to the Commission

We are proposing a new reporting rule requirement and related proposed Form ADV–C. Advisers would be required to report significant cybersecurity incidents to the Commission, including on behalf of a client that is a registered investment company or business development company, or a private fund (referred to in this release as ''covered clients'') that experiences a significant cybersecurity incident. Specifically, under proposed rule 204–6, any adviser registered or required to be registered with the Commission as an investment adviser would be required to submit proposed Form ADV–C promptly, but in no event more than 48 hours, after having a reasonable basis to conclude that a significant adviser cybersecurity incident or a significant fund cybersecurity incident had occurred or is occurring.[58] Form ADV–C would include both general and specific questions related to the significant cybersecurity incident, such as the nature and scope of the incident as well as whether any disclosure has been made to any clients and/or investors.[59] Proposed rule 204–6 would also require advisers to amend any previously filed Form ADV–C promptly, but in no event more than 48 hours, after information reported on the form becomes materially inaccurate; if new material information about a previously reported incident is discovered; and after resolving a previously reported incident or closing an internal investigation pertaining to a previously disclosed incident.

This reporting would help us in our efforts to protect investors in connection with cybersecurity incidents by providing prompt notice of these incidents. We believe this proposed reporting would allow the Commission and its staff to understand the nature and extent of a particular cybersecurity incident and the firm's response to the incident. As stated above, this reporting would not only help the Commission monitor and evaluate the effects of the cybersecurity incident on an adviser and its clients or a fund and its investors, but also assess the potential systemic risks affecting financial markets more broadly. For example, these reports could assist the Commission in identifying patterns and trends across registrants, including widespread cybersecurity incidents affecting multiple advisers and funds.

1. Proposed Rule 204–6

Proposed rule 204–6 would require investment advisers to report on Form ADV–C within 48 hours after having a reasonable basis to conclude that a significant adviser cybersecurity incident or a significant fund cybersecurity incident occurred or is occurring. The rule would define a significant adviser cybersecurity incident as a cybersecurity incident, or a group of related incidents, that significantly disrupts or degrades the adviser's ability, or the ability of a private fund client of the adviser, to maintain critical operations, or leads to the unauthorized access or use of adviser information, where the unauthorized access or use of such information results in: (1) Substantial harm to the adviser, or (2) substantial harm to a client, or an investor in a private fund, whose information was accessed.[60]

The first prong of the definition of significant adviser cybersecurity incident includes a cybersecurity incident, or a group of related cybersecurity incidents, that significantly disrupts or degrades the adviser's ability, or the ability of a private fund client of the adviser, to maintain critical operations. If an adviser were unable to maintain critical operations, such as the ability to implement its investment strategy, process or record transactions, or communicate with clients, there is potential for substantial loss to both the adviser and its clients. For example, if an adviser's internal computer systems, including its websites or email function, are shut down due to malware, it could have a significant effect on the ability for the adviser to continue to provide advisory services and for the adviser's clients to access their investments or communication with the adviser. In such a situation, it is possible that the adviser's employees would not be able to access the computer systems they need to make trades or manage a client's portfolio, and advisory clients may not be able to access their accounts through the adviser's web page or other channels that were affected by the malware.[61] Depending on the type of malware, this could lock up advisory client records, among other things, and affect an adviser's decision-making and investments for days, or even weeks. This in turn could potentially affect the market, particularly if other advisers are similarly targeted with the same malware. Reporting to the Commission the occurrence of such an incident, we believe, could help the Commission monitor and evaluate the effects of the event on an adviser or fund and its clients and investors, and the broader financial markets. For example, reporting by a large adviser or a series of advisers of similar occurrences could signal a market-wide event requiring Commission attention and, if necessary, coordination with other governmental agencies.

Under the proposed rules, a significant adviser cybersecurity incident would also include significant cybersecurity incidents affecting private fund clients of an adviser. Given that a cybersecurity incident that significantly disrupts or degrades the ability of a private fund to maintain its critical operations could potentially cause similar substantial losses to the adviser and private fund investors, and that private funds play a significant role in the financial industry, we believe that such incidents should be reported as well.

The second prong of the definition of a significant adviser cybersecurity incident would include a cybersecurity incident that leads to unauthorized access or use of adviser information, where the unauthorized access or use of such information results in: (1) Substantial harm to the adviser, or (2) substantial harm to a client, or an investor in a private fund, whose information was accessed.[62] Substantial harm to an adviser as the result of a cybersecurity incident in which adviser information is compromised could include, among other things, significant monetary loss or theft of intellectual

[58] *See* proposed rules 204–6 and 38a–2.

[59] *See* proposed Form ADV–C.

[60] *See* proposed rule 204–6(b); *see also* proposed rule 206(4)–9. This proposed definition is substantially similar to the proposed definition of ''significant fund cybersecurity incident'' for funds. We view critical operations as including investment, trading, reporting, and risk management of an adviser or fund as well as operating in accordance with the Federal securities laws.

[61] Account access could also be affected by denial of service (''DoS'') attacks that disrupt customer access for extended periods of time. We understand that DoS attacks are often accompanied by ransom demands to stop any attack and/or are used as a diversionary measure to exfiltrate (or remove) information or probe further into business networks.

[62] Proposed rule 204–6(b). There may be times where an incident meets both prongs. For example, a breach of an adviser's internal computer systems may affect the adviser's ability to maintain critical operations as well as result in substantial harm to the adviser, its clients, or investors in private fund clients of the adviser.

property. Substantial harm to a client or an investor in a private fund as the result of a cybersecurity incident in which adviser information is compromised could include, among other things, significant monetary loss or the theft of personally identifiable or proprietary information.[63] After gaining access to an adviser's or a fund's systems, an attacker could use this access to disclose, modify, delete or destroy adviser, fund, or client data, as well as steal intellectual property and client assets. Any of these actions could result in substantial harm to the adviser and/or to the client.

In addition to reporting significant cybersecurity incidents for itself and its private fund clients, an adviser would also have to report significant fund cybersecurity incidents on Form ADV–C for its registered fund and BDC clients. Similar to a significant adviser cybersecurity incident, a significant fund cybersecurity incident has two prongs, that it: (1) Significantly disrupts or degrades the fund's ability to maintain critical operations, or (2) leads to the unauthorized access or use of fund information, which results in substantial harm to the fund, or to the investor whose information was accessed.[64] Significant fund cybersecurity incidents may include cyber intruders interfering with a fund's ability to redeem investors, calculate NAV or otherwise conduct its business. Other significant fund cybersecurity incidents may involve the theft of fund information, such as non-public portfolio holdings, or personally identifiable information of the fund's employees, directors or shareholders.

In order to assist the adviser in reporting a significant fund cybersecurity incident, a fund's cybersecurity policies and procedures must address the proposed notification requirement to the Commission on Form ADV–C. Generally, these provisions of the policies and procedures should address communications between the person(s) who administer the fund's cybersecurity policies and procedures and the adviser about cybersecurity incidents, including those affecting the fund's service providers.

An adviser would have to report within 48 hours after having a reasonable basis to conclude that any significant adviser or fund cybersecurity incident has occurred or is occurring with respect to itself or any of its clients that are covered clients.[65] In other words, an adviser must report within 48 hours after having a reasonable basis to conclude that an incident has occurred or is occurring, and not after definitively concluding that an incident has occurred or is occurring. The 48-hour period would give an adviser time to confirm its preliminary analysis, and prepare the report while still providing the Commission with timely notice about the incident.

We are also requiring that advisers amend a previously filed Form ADV–C promptly, but in no event more than 48 hours, in connection with certain incidents. Advisers would be required to update the Commission by filing an amended Form ADV–C if any previously reported information about a significant cybersecurity incident becomes materially inaccurate or if the adviser discovers new material information related to an incident.[66] We are also proposing to require advisers to file a final Form ADV–C amendment after the resolution of any significant cybersecurity incident or after closing any internal investigation related to a previously disclosed incident.[67] We believe requiring advisers to amend Form ADV–C in these circumstances would help to ensure the Commission has accurate and timely information with respect to significant adviser and fund cybersecurity incidents to allocate resources better when evaluating and responding to these incidents. While advisers and funds have other incentives to investigate and remediate significant cybersecurity incidents, we believe these ongoing reporting obligations would further encourage advisers and funds to take the steps necessary to do so completely. Moreover, based on our experience with other regulatory filings, we believe it is likely that an adviser could regularly engage in a productive dialogue with applicable Commission staff after the reporting of an incident and the filing of any amendments to Form ADV–C, and, as part of that dialogue, could provide Commission staff with any additional information as necessary, depending on the facts and circumstances of the incident and the progress in resolving it.

We request comments on the proposed reporting rule 204–6 and the reporting thresholds.

35. Should we require advisers to report significant cybersecurity incidents of the adviser and covered clients with the Commission? Why or why not? Alternatively, should we exclude incidents that affect private fund clients of an adviser? Should we exclude registered funds and BDCs as covered clients? If so, should we require them to report to the Commission in another manner? How should the Commission address funds that are internally managed? Should we require a separate reporting requirement under the Investment Company Act for such funds? If so, should it be substantially similar to the proposed reporting requirements under rule 204–6?

36. Should we require advisers to report on significant cybersecurity incidents of other pooled investment vehicle clients? For example, should we require advisers to report on significant cybersecurity incidents of pooled investment vehicles that rely on the exemption from the definition of ''investment company'' in section 3(c)(5)(C) of that Act?[68]

37. Who should be responsible for having a reasonable basis to conclude that there has been a significant adviser cybersecurity incident or significant fund cybersecurity incident or that one is occurring? Should the Commission require a person or role be designated to be the one responsible for gathering relevant information about the incident and having a reasonable basis to conclude that such an incident occurred?

38. At what point would one conclude that there has been a significant adviser cybersecurity incident or significant fund cybersecurity incident? Would it be after some reasonable period of assessment or some other point?

39. Are the proposed definitions of significant adviser cybersecurity incident and significant fund cybersecurity incident appropriate and clear? If not, how could they be made clearer? Should the term critical operations be defined for advisers and funds, and if so what adviser and fund

[63] When considering their obligations under these proposed reporting and risk management requirements, advisers and funds should also keep in mind their obligations with respect to safeguarding client information, such as those required by Regulation S–P and under an adviser's fiduciary duty.

[64] *See* proposed rules 204–6(b) and 38a–2.

[65] We believe that an adviser would generally gather relevant information and perform an initial analysis to assess whether to reasonably conclude that a cybersecurity incident has occurred or is occurring and follow its own internal communication and escalation protocols concerning such an incident before providing notification of any significant cybersecurity incident to the Commission.

[66] *See* proposed rule 204–6(a)(2)(i) and (ii).

[67] *See* proposed rule 204–6(a)(2)(iii).

[68] Section 3(c)(5)(C) of the Investment Company Act provides an exclusion from the definition of investment company for any person who is not engaged in the business of issuing redeemable securities, face-amount certificates of the installment type or periodic payment plan certificates, and who is primarily engaged in the business of purchasing or otherwise acquiring mortgages and other liens on and interests in real estate.

operations should be considered critical? For example, should critical operations include the investment, trading, valuation, reporting, and risk management of the adviser or fund as well as the operation of the adviser or fund in accordance with the Federal securities laws? Alternatively, should there be a quantitative threshold at which operations must be impaired by a cybersecurity incident before an adviser's or fund's obligation to report is triggered (for example, maintaining operations at minimally 80% of current levels on any function)? If so, what should that threshold be and how should an adviser or fund measure its operational capacity to determine whether that threshold has been crossed?

40. Is the proposed ''substantial harm'' threshold under the definition of significant adviser and fund cybersecurity incident appropriate? Should we also include ''inconvenience'' as a threshold with respect to shareholders, clients and investors? In other words, should we also require reporting if the unauthorized access or use of such information results in substantial harm or inconvenience to a shareholder, client, or an investor in a private fund, whose information was accessed?

41. Do commenters believe requiring the report 48 hours after having a reasonable basis to conclude that there has been a significant adviser cybersecurity incident or significant fund cybersecurity incident or that one is occurring is appropriate? If not, is it too long or too short? Should we require a specific time frame at all? Do commenters believe that ''a reasonable basis'' is a clear standard? If not, what other standard should we use?

42. Should we provide for one or more exceptions to the reporting of significant cybersecurity incidents, for example for smaller advisers or funds? Are there ways, other than the filing of Form ADV–C, we should require advisers to notify the Commission regarding significant cybersecurity incidents?

43. The Commission recently proposed current reporting requirements that would require large hedge fund advisers to file a current report on Form PF within one business day of the occurrence of a reporting events at a qualifying hedge fund that they advise.[69] The proposed reporting events include a significant disruption or degradation of the reporting fund's key operations, which could include a significant cybersecurity incident. If the amendments to Form PF are adopted, should the Commission provide an exception to the Form ADV–C filing requirements when an adviser has reported the incident as a current report on Form PF? Alternatively, should the Commission provide an exception to the Form PF current reporting requirements if the adviser filed a Form ADV–C in connection with the reporting event?

44. Should advisers be required to provide the Commission with ongoing reporting about significant cybersecurity incidents? If so, are the proposed requirements to amend Form ADV–C promptly, but in no event more than within 48 hours, sufficient for such reporting? Is this timeframe appropriate? Should we require a shorter or longer timeframe? Is the materiality threshold for ongoing reports appropriate? Should we require another mechanism be used for ongoing reporting? For example, should advisers instead be required to provide periodic reports about significant cybersecurity incidents that are ongoing? If so, how often should such reports be required (*e.g.,* every 30 days) and what information should advisers be required to provide?

2. Form ADV–C

The Commission is proposing a new Form ADV–C to require an adviser to provide information regarding a significant cybersecurity incident in a structured format through a series of check-the-box and fill-in-the-blank questions. We believe that collecting information in a structured format would enhance our staff's ability to carry out our risk-based examination program and other risk assessment and monitoring activities effectively. By enhancing comparability across multiple filers, the structured format would also assist our staff in assessing trends in cybersecurity incidents across the industry and accordingly better protect investors from any patterned cybersecurity threats.

The proposed rule would require Form ADV–C to be filed electronically with the Commission through the Investment Adviser Registration Depository (''IARD'') platform. We considered proposing other electronic filing platforms, either maintained by the Commission or by a third-party contractor. However, we believe that there would likely be efficiencies realized if the IARD platform is expanded for this purpose, such as the possible interconnectivity of Form ADV filings and Form ADV–C filings, and possible ease of filing with one password. Moreover, the IARD platform is a familiar filing system for advisers.

Proposed Form ADV–C would require advisers to report certain information regarding a significant cybersecurity incident in order to allow the Commission and its staff to understand the nature and extent of the cybersecurity incident and the adviser's response to the incident.

Items 1 through 4 request the following information about the adviser: (1) Investment Advisers Act SEC File Number; (2) full name of investment adviser; (3) name under which business is conducted; (4) address of principal place of business; and (5) contact information for an individual with respect to the significant cybersecurity incident being reported: (name, title, address if different from above, phone, email address). These items are designed to provide the Commission with basic identifying information regarding the adviser. We anticipate that the IARD system will pre-populate this information, other than the contact information for the individual whom should be contacted for additional information about the incident being reported.

Items 6 through 9 would elicit whether the adviser is reporting a significant adviser cybersecurity incident or a significant fund cybersecurity incident (or both), the approximate date the incident occurred, the approximate date the incident was discovered, and whether the incident is ongoing. This information would provide the Commission with important background information regarding the incident. This information would also inform the Commission if the incident presents an ongoing threat and assist the Commission in prioritizing its outreach to advisers following multiple Form ADV–C filings in the same time period.

Item 10 would require the adviser to disclose whether law enforcement or a government agency has been notified about the cybersecurity incident. In assessing the risk to the broader financial market, it may be important for the Commission to coordinate with other governmental authorities. Therefore, this disclosure would inform the Commission whether an adviser or fund has already notified local and Federal law enforcement authorities, such as the FBI, or a local or Federal government agency, such as the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, about an incident.

Items 11 through 15 would require the adviser to provide the Commission with substantive information about the

[69] *See* Amendments to Form PF to Require Current Reporting and Amend Reporting Requirements for Large Private Equity Advisers and Large Liquidity Fund Advisers, Investment Advisers Act Release No. 5950 (Jan. 26, 2022).

nature and scope of the incident being reported, including any actions and planned actions to recover from the incident; whether any data was stolen altered, or accessed or used for any other unauthorized purpose; and whether the significant cybersecurity incident has been disclosed to the adviser's clients and/or to investors. When describing the nature and scope of the incident being reported, advisers generally should describe whether, and if so how, the incident has affected its critical operations, including which systems or services have been affected, and whether the incident being reported was the result of a cybersecurity incident that occurred at a service provider. Further, to the extent an adviser reports a significant cybersecurity incident that resulted from a cybersecurity incident that occurred at a service provider, generally the adviser also should describe the services provided to the adviser or funds it advises by the provider that experienced the incident and how any degradation in those services have affected the adviser's—or its registered and private fund clients'—operations. This information should provide the Commission with sufficient detail regarding the incident to understand its potential effects and whether the adviser can continue to provide services to its clients and investors. The information would also help the Commission determine whether the incident merits further analysis by the Commission and its staff and/or whether the Commission and its staff should collect additional information from the adviser.

Item 16 would require the adviser to disclose whether the cybersecurity incident is covered under a cybersecurity insurance policy. This information would assist the Commission in understanding the potential effect that incident could have on an adviser's clients. This information would also be helpful in evaluating the adviser's response to the incident given that cybersecurity insurance may require an adviser to take certain actions during and after a cybersecurity incident.

After realizing a cybersecurity incident has occurred, an adviser may need time to determine the scope and effect of the incident to provide meaningful responses to these questions. We recognize that the adviser may be working diligently to investigate and resolve the cybersecurity incident at the time it would be required to report to the Commission under the proposed rule. We believe, however, that advisers should have sufficient information to respond to the proposed questions by the time the filing is due to the Commission. Advisers should only share information about what is known at the time of filing.

Section 210(a) of the Advisers Act requires information in Form ADV–C to be publicly disclosed, unless we find that public disclosure is neither necessary nor appropriate in the public interest or for the protection of investors.[70] Form ADV–C would elicit certain information regarding cybersecurity incidents, the public disclosure of which, we believe, could adversely affect advisers (and advisory clients) and funds (and their investors). For example, public disclosure may harm an adviser's or fund's ability to mitigate or remediate the cybersecurity incident, especially if the incident is ongoing. Keeping information related to a cybersecurity incident confidential may serve to guard against the premature release of sensitive information, while still allowing the Commission to have early notice of the cybersecurity incident.[71] Accordingly, our preliminary view is that Form ADV–C should be confidential given that public disclosure is neither necessary nor appropriate in the public interest or for the protection of investors.[72]

We request comment on all aspects of Form ADV–C, including the following items.

45. Is IARD the appropriate system for investment advisers to file Form ADV–C with the Commission? Instead of expanding the IARD system to receive Form ADV–C filings, should the Commission utilize some other system, such as the Electronic Data Gathering, Analysis, and Retrieval System (EDGAR)? If so, please explain. What would be the comparative advantages and disadvantages and costs and benefits of utilizing a system other than IARD? What other issues, if any, should the Commission consider in connection with electronic filing?

46. Should we include any additional items or eliminate any of the items that we have proposed to include in Form ADV–C? For example, should advisers be required to disclose any technical information (*e.g.,* about specific information systems, particular vulnerabilities exploited, or methods of exploitation) about significant cybersecurity incidents? Should we modify any of the proposed items? If so, how and why?

47. Should Form ADV–C be confidential, as proposed? Alternatively, should we require public disclosure of some or all of the information included in Form ADV–C?

C. Disclosure of Cybersecurity Risks and Incidents

We are also proposing amendments to certain forms used by advisers and funds to require the disclosure of cybersecurity risks and incidents to their investors and other market participants. In particular, we propose amendments to Form ADV Part 2A for advisers and Forms N–1A, N–2, N–3, N–4, N–6, N–8B–2, and S–6 for funds. While many advisers and funds already provide disclosure about cybersecurity risks, we are updating current reporting and disclosure requirements to address cybersecurity risks and incidents more directly. These proposed amendments are designed to enhance investor protection by ensuring cybersecurity risk or incident-related information is available to increase understanding and insight into an adviser's or fund's cybersecurity history and risks. These proposed reporting and disclosure amendments, together with the proposed cybersecurity risk management rules, may also increase accountability of advisers and funds on cybersecurity issues. The proposed disclosure changes would also give the Commission and staff greater insight into cybersecurity risks affecting advisers and funds. This information would enhance the Commission's ability to oversee compliance with the proposed cybersecurity risk management rules, and to gain understanding about the specifics of the

[70] Section 210(a) of the Advisers Act states that ''[t]he information contained in any . . . report or amendment thereto filed with the Commission pursuant to any provision of this title shall be made available to the public, unless and except insofar as the Commission, by rules and regulations upon its own motion, or by order upon application, finds that public disclosure is neither necessary nor appropriate in the public interest or for the protection of investors.''

[71] Further, as discussed in greater detail below, we are proposing amendments to Form ADV Part 2A and certain fund registration forms that would require advisers and funds to publicly disclose significant cybersecurity incidents. Therefore, clients and investors would have access to information regarding cybersecurity incidents that they may find material, albeit on a different timeline. Further, as discussed in more detail below, the disclosure requirements we are proposing are designed to provide clients and investors with clear and meaningful disclosure regarding cybersecurity incidents in a narrative, plain-English format, while the information we are proposing to require adviser disclose on Form ADV–C may be less useful to clients and investors, given its more granular nature and the fact that it may be incomplete due to the expediency in which it must be reported.

[72] Although the Commission does not intend to make Form ADV–C filings public, the Commission or Commission staff could issue analyses and reports that are based on aggregated, non-identifying Form ADV–C data, which would otherwise be nonpublic.

policies and procedures that funds adopted under the rules.

1. Proposed Amendments to Form ADV Part 2A

We are proposing amendments to Form ADV Part 2A that are designed to provide clients and prospective clients with information regarding cybersecurity risks and incidents that could materially affect the advisory relationship. We believe the proposed amendments would improve the ability of clients and prospective clients to evaluate and understand relevant cybersecurity risks and incidents that advisers face and their potential effect on the advisers' services.

2. Cybersecurity Risks and Incidents Disclosure

The proposed amendments would add a new Item 20 entitled ''Cybersecurity Risks and Incidents'' to Form ADV's narrative brochure, or Part 2A. The brochure, which is publicly available and the primary client-facing disclosure document, contains information about the investment adviser's business practices, fees, risks, conflicts of interest, and disciplinary events. We believe the narrative format of the brochure would allow advisers to present clear and meaningful cybersecurity disclosure to their clients and prospective clients.

Advisers would be required to, in plain English, describe cybersecurity risks that could materially affect the advisory services they offer and how they assess, prioritize, and address cybersecurity risks created by the nature and scope of their business. A cybersecurity risk, regardless of whether it has led to a significant cybersecurity incident, would be material to an adviser's advisory relationship with its clients if there is a substantial likelihood that a reasonable client would consider the information important based on the total mix of facts and information.[73] 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 has disrupted) the adviser's ability to provide services, including the duration of such a disruption; (2) could result (or has resulted) in the loss of adviser or client data, including the nature and importance of the data and the circumstances and duration in which it was compromised; and/or (3) could harm (or has harmed) clients (*e.g.,* inability to access investments, illiquidity, or exposure of confidential or sensitive personal or business information).

The proposed amendments would also require advisers to describe any cybersecurity incidents that occurred within the last two fiscal years that have significantly disrupted or degraded the adviser's ability to maintain critical operations, or that have led to the unauthorized access or use of adviser information, resulting in substantial harm to the adviser or its clients.[74] When describing these incidents in their brochures, advisers would be required to identify the entity or entities affected, when the incidents were discovered and whether they are ongoing, whether any data was stolen, altered, or accessed or used for any other unauthorized purpose, the effect of the incident on the adviser's operations, and whether the adviser, or service provider has remediated or is currently remediating the incident. This information would allow investors to make more informed decisions when deciding whether to engage or stay with an adviser.

3. Requirement To Deliver Certain Interim Brochure Amendments to Existing Clients

17 CFR 275.204–3(b) (rule 204–3(b) under the Advisers Act) does not require advisers to deliver interim brochure amendments to existing clients unless the amendment includes certain disciplinary information in response to Item 9 Part 2A or Item 3 of Part 2B.[75] We are proposing an amendment to rule 204–3(b) that would also require an adviser to deliver interim brochure amendments to existing clients promptly if the adviser adds disclosure of a cybersecurity incident to its brochure or materially revises information already disclosed in its brochure about such an incident. Given the potential effect that significant cybersecurity incidents could have on an adviser's clients—such as exposing their personal or other confidential information or resulting in losses in their accounts—time is of the essence, and we believe that requiring an adviser to promptly deliver the brochure amendment would enhance investor protection by enabling clients to take protective or remedial measures to the extent appropriate. Accordingly, the timing of the brochure amendment delivery should take into account the exigent nature of cybersecurity incidents which would generally militate toward swift delivery to clients. We also believe that requiring advisers to deliver the brochure amendment to existing clients following the occurrence of a new significant cybersecurity incident would assist investors in determining whether their engagement of that particular adviser remains appropriate and consistent with their investment objectives.

We seek comment on the Commission's proposed amendments to Form ADV Part 2A:

48. Will the proposed cybersecurity disclosures in Item 20 of Form ADV Part 2A be helpful for clients and investors? Are there additional cybersecurity disclosures we should consider adding to Item 20? Should we modify or delete any of the proposed cybersecurity disclosures?

49. Does the definition of significant adviser cybersecurity incident allow advisers to inform investors of cybersecurity risks arising from the incident while protecting the adviser and its clients from threat actors who might use that information for the current or future attacks? Does this definition allow for disclosures relevant to investors without providing so much information as to be desensitizing? Why or why not?

50. Do the required disclosures provide investors with prompt access to important information that they need in connection with the decision to engage, or continue to engage, an adviser? Why or why not?

51. We propose to require advisers to update their cybersecurity disclosures in Item 20 promptly to the extent the disclosures become materially inaccurate. Do commenters agree that the lack of disclosure regarding certain cybersecurity risks and cybersecurity incidents would render an adviser's brochure materially inaccurate? Should we only require advisers to update their cybersecurity disclosures on an annual basis (rather than an ongoing basis, as proposed)?

52. We propose to require advisers to deliver brochure amendments to

[73] *See, e.g.,* Amendments to Form ADV, Investment Advisers Act Release No. 3060 (July 28, 2010) [75 FR 49233 (Aug.12, 2010)], at n.35 (citing *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)).

[74] We believe disclosure covering this look-back period would provide investors a short history of cybersecurity incidents affecting the adviser while not overburdening the adviser with a longer disclosure period. Further, this lookback period would foster consistency between adviser and fund disclosures regarding significant cybersecurity incidents.

[75] Even if an adviser is not required to deliver a brochure to an existing client, as a fiduciary the adviser may still be required to provide clients with similar information. If an adviser is not required to deliver an existing client a brochure, the adviser may make any required disclosures to that client by delivery of the brochure or through some other means. *See* Instruction 1 of Instructions for Part 2A of Form ADV: Preparing Your Firm Brochure.

existing clients if the adviser adds disclosure of an event, or materially revises information already disclosed about an event, that involves a cybersecurity incident in response to proposed Item 20. Is this delivery requirement appropriate? Why or why not? Are there other delivery or client-notification requirements that we should consider for advisers when updates to their cyber security disclosures are made?

53. Should advisers also be specifically required to disclose if there has *not* been a significant cybersecurity incident in its last two fiscal years? Would this disclosure assist investors in their investment decision-making? Why or why not?

54. Should the rule include a requirement to disclose whether a significant adviser cybersecurity incident is currently affecting the adviser? Why or why not? Is the look-back period of two fiscal years appropriate? Why or why not?

4. Proposed Amendments To Fund Registration Statements

Like advisers, funds would also be required to provide prospective and current investors with disclosure about significant cybersecurity incidents under our proposal. We are proposing amendments to funds' registration forms that would require a description of any significant fund cybersecurity incident that has occurred in its last two fiscal years, and that funds must tag the new information that would be included using a structured data language (specifically, Inline eXtensible Business Reporting Language or ''Inline XBRL'').[76] The proposed disclosure amendments would require that a fund disclose to investors in its registration statement whether a significant fund cybersecurity incident has or is currently affecting the fund or its service providers.[77]

Specifically, the proposed amendments would require a description of each significant fund cybersecurity incident, including the following information to the extent known: the entity or entities affected; when the incident was discovered and whether it is ongoing; whether any data was stolen, altered, or accessed or used for any other unauthorized purpose; the effect of the incident on the fund's operations; and whether the fund or service provider has remediated or is currently remediating the incident. The requirements for disclosure describing the incident would be similar to the information that new Form ADV–C requires, which we believe would increase compliance efficiencies for funds and their advisers.

The fund would be required to disclose any significant fund cybersecurity incident that has occurred during its last two fiscal years. We believe disclosure covering this look-back period would provide investors a short history of cybersecurity incidents affecting the fund while not overburdening the fund with a longer disclosure period.[78] We believe providing a description of a significant fund cybersecurity incident would improve the ability of shareholders and prospective shareholders to evaluate and understand relevant cybersecurity risks and incidents that a fund faces and their potential effect on the fund's operations.

In addition to providing investors with information on significant fund cybersecurity incidents, funds should consider cybersecurity risks when preparing risk disclosures in fund registration statements under the Investment Company Act and the Securities Act. Funds are currently required to disclose ''principal risks'' of investing in the fund, and if a fund determines that a cybersecurity risk is a principal risk of investing in the fund, the fund should reflect this information in its prospectus.[79] For example, a fund that has experienced a number of significant fund cybersecurity incidents in a short period of time may need to disclose heightened cybersecurity risk as a principal risk of investing in the fund. This information would allow investors to make more informed decisions when deciding whether to invest in a fund.

Funds are required to update their prospectuses so that they do not contain an untrue statement of a material fact (or omit a material fact necessary to make the disclosure not misleading).[80] To make timely disclosures of cybersecurity risks and significant fund cybersecurity incidents, a fund would amend its prospectus by filing a supplement with the Commission.[81] In addition, funds should generally include in their annual reports to shareholders a discussion of cybersecurity risks and significant fund cybersecurity incidents, to the extent that these were factors that materially affected performance of the fund over the past fiscal year.[82]

We are proposing to require all funds to tag this information about significant fund cybersecurity incidents in a structured, machine-readable data language.[83] Specifically, we are proposing to require funds to tag the disclosures in Inline XBRL in accordance with rule 405 of Regulation S–T and the EDGAR Filer Manual.[84]

[76] We are proposing amendments to Form N–1A, Form N–2, Form N–3, Form N–4, Form N–6, Form N–8B–2, and Form S–6.

[77] The proposed disclosure amendments would also require funds to disclose significant fund cybersecurity incidents affecting insurance companies (for separate accounts that are management investment companies that offer variable annuity contracts registered on Form N–3) and depositors (for separate accounts that are unit investment trusts that offer variable annuity contracts on Form N–4; unit investment trusts that offer variable life insurance contracts on Form N–6; and unit investment trusts other than separate accounts that are currently issuing securities, including unit investment trusts that are issuers of periodic payment plan certificates and unit investment trusts of which a management investment company is the sponsor or depositor on Form N–8b-2 or Form S–6).

[78] The two-year period is consistent with other items in Form N–1A (for example, Item 16(e) (description of the fund's portfolio turnover), Item 17(b)(6) through (9) (management of the fund), and Item 31 (business and other connections of investment adviser). We are proposing a corresponding period for the disclosures in Part 2A of Form ADV.

[79] *See* Form N–1A, Item 4(b)(1) (narrative risk disclosure), Item 9(c) (risks), and Item 16(b) (investment strategies and risks); Form N–2, Item 8(3) (risk factors); Form N–3, Item 5 (principal risks of investing in the contract) and Item 22 (investment objectives and risks); Form N–4, Item 5 (principal risks of investing in the contract) and Item 20 (non-principal risks of investing in the contract); Form N–6, Item 5 (principal risks of investing in the contract) and Item 21 (non-principal risks of investing in the contract). UITs filing on Form N–8B–2 must disclose instead information concerning the operations of the trust (Form N–8B–2, Items 14–24).

[80] *See generally* 17 CFR 230.497 [rule 497 under the Securities Act]; section 12(a)(2) of the Securities Act (providing a civil remedy if a prospectus includes an untrue statement of a material fact or omits to state a fact necessary in order to make the statements, in the light of the circumstances under which they were made, not misleading); 17 CFR 230.408 [rule 408 under the Securities Act] (requiring registrants to include, in addition to the information expressly required to be included in a registration statement, such further material information, if any, as may be necessary to make the required statements, in the light of the circumstances under which they are made, not misleading).

[81] *See* 17 CFR 230.497 (open-end funds); 17 CFR 230.424 (closed-end funds).

[82] *See, e.g.,* Disclosure of Mutual Fund Performance and Portfolio Managers, Investment Company Act Release No. 19382 (Apr. 6, 1993) [58 FR 21927 (Apr. 26, 1993)], at n.15 (noting that management's discussion of fund performance requires funds to ''explain what happened during the previous fiscal year and why it happened'').

[83] Many funds are already required to tag certain registration statement disclosure items using Inline XBRL; however, UITs that register on Form N–8B–2 and file post-effective amendments on Form S–6 are not currently subject to any tagging requirements. The costs of these requirements for funds that are currently subject to tagging requirements and those that newly would be required to tag certain disclosure items are discussed in the Economic Analysis. *See* section III.D.2 *infra.*

[84] This proposed tagging requirement would be implemented by including cross-references to rule 405 of Regulation S–T in each fund registration

Continued

The proposed requirements would include block text tagging of narrative information about significant fund cybersecurity incidents, as well as detail tagging of any quantitative values disclosed within the narrative disclosures.

Many funds are already required to tag certain registration statement disclosure items using Inline XBRL.[85] Requiring Inline XBRL tagging of significant fund cybersecurity incidents for all funds would benefit investors, other market participants, and the Commission by making the disclosures more readily available and easily accessible for aggregation, comparison, filtering, and other analysis, as compared to requiring a non-machine readable data language such as ASCII or HTML. This would enable automated extraction and analysis of granular data on significant fund cybersecurity incidents, such as the date the incident was discovered, allowing investors and other market participants to more efficiently perform large-scale analysis and comparison across funds and time periods. An Inline XBRL requirement would facilitate other analytical benefits, such as more easily extracting/searching disclosures about significant fund cybersecurity incidents, performing targeted assessments (rather than having to manually run searches for these disclosures through entire documents), and automatically comparing these disclosures against prior periods. We believe requiring structured data for significant fund cybersecurity incidents for all funds would make cybersecurity disclosure more readily available, accessible, and comparable for investors, other market participants, and the Commission.

We seek comment on the Commission's proposed amendments to fund registration statement disclosure requirements:

55. Should there be a prospectus disclosure requirement of significant fund cybersecurity incidents for *all* registered funds? If some types of funds should be exempt, have different disclosure requirements, or not be subject to the proposed structured data requirement, which and why?

56. Will the proposed cybersecurity disclosures be helpful for shareholders and potential shareholders? Are there additional cybersecurity disclosures we should add? Should we modify or delete any of the proposed cybersecurity disclosures?

57. Does the definition of significant fund cybersecurity incident allow funds to inform investors of cybersecurity risks arising from the incident while protecting the fund from threat actors who might use that information for the current or future attacks? Does this definition allow for disclosures relevant to investors without providing so much information as to be desensitizing? Why or why not?

58. Should the rule include a requirement to disclose whether a significant fund cybersecurity incident is currently affecting the fund as proposed? Why or why not? How often should cybersecurity disclosure be updated? Is the lookback period of two fiscal years appropriate? Why or why not?

59. Should the rule include an instruction about significant fund cybersecurity incidents that may have occurred in the fund's last two fiscal years but was discovered later? Why or why not? Should the Commission provide more specific guidance or requirements on when a fund should update its disclosure to provide information about a significant fund cybersecurity incident? Should the timing or information about a significant cybersecurity incident for updated disclosure match the prompt reporting requirement for advisers on Form ADV–C? Why or why not?

60. Are there other delivery or shareholder-notification requirements that we should consider for funds when updates to their cybersecurity disclosures are made? For example, should there be an alternate website disclosure regime, similar to how proxy voting records may be disclosed, for cybersecurity incidents? Why or why not? Or alternatively or additionally, should information about significant fund cybersecurity incidents be included in funds' annual reports to shareholders, filed on Form N–CSR, or reported on Form N–CEN?

61. Should funds also be specifically required to disclose if there has *not* been a significant cybersecurity incident in its last two fiscal years? Would this disclosure assist investors in their investment decision-making? Why or why not?

62. Should the Commission provide more specific guidance or requirements on when and what cybersecurity risk funds should disclose, including when cybersecurity risk would be considered a principal risk factor? Why or why not?

63. Should we require all funds to tag significant fund cybersecurity incidents in Inline XBRL, as proposed? Why or why not?

64. Should we require funds to use a different structured data language to tag significant fund cybersecurity incident disclosures? If so, what structured data language should we require?

III. Economic Analysis

A. Introduction

The Commission is mindful of the economic effects, including the costs and benefits, of the proposed rules and amendments. Section 3(f) of the Exchange Act, section 2(c) of the Investment Company Act, and section 202(c) of the Advisers Act provide that when engaging in rulemaking that requires us to consider or determine whether an action is necessary or appropriate in or consistent with the public interest, to also consider, in addition to the protection of investors, whether the action will promote efficiency, competition, and capital formation. Section 23(a)(2) of the Exchange Act also requires us to consider the effect that the rules would have on competition, and prohibits us from adopting any rule that would impose a burden on competition not necessary or appropriate in furtherance of the Exchange Act. The analysis below addresses the likely economic effects of the proposed amendments, including the anticipated and estimated benefits and costs of the amendments and their likely effects on efficiency, competition, and capital formation. The Commission also discusses the potential economic effects of certain alternatives to the approaches taken in this proposal.

form (and, as applicable, updating references to those fund registration forms in rule 11 and rule 405), by revising rule 405(b) of Regulation S–T to include the proposed significant fund cybersecurity incident disclosures, and by proposing conforming amendments to rule 485 and rule 497 under the Securities Act.

Pursuant to rule 301 of Regulation S–T, the EDGAR Filer Manual is incorporated by reference into the Commission's rules. In conjunction with the EDGAR Filer Manual, Regulation S–T governs the electronic submission of documents filed with the Commission. Rule 405 of Regulation S–T specifically governs the scope and manner of disclosure tagging requirements for operating companies and investment companies, including the requirement in rule 405(a)(3) to use Inline XBRL as the specific structured data language to use for tagging the disclosures.

[85] The Commission has adopted rules requiring funds registering on Forms N–1A, N–2, N–3, N–4, and N–6 to submit data using Inline XBRL. *See* Interactive Data to Improve Financial Reporting, Release No. 33–9002 (Jan. 30, 2009) [74 FR 6776 (Feb. 10, 2009)] as corrected by Release No. 33–9002A (Apr. 1, 2009) [74 FR 15666 (Apr. 7, 2009)]; Inline XBRL Filing of Tagged Data, Release No. 33–10514 (June 28, 2018) [83 FR 40846 (Aug. 16, 2018)]; Updated Disclosure Requirements and Summary Prospectus for Variable Annuity and Variable Life Insurance Contracts, Investment Company Act Release No. 33814 (Mar. 11, 2020) [85 FR 25964 (May 1, 2020)] (''Variable Contract Summary Prospectus Adopting Release''); Securities Offering Reform for Closed-End Investment Companies, Release No. 33–10771 (Apr. 8, 2020) [85 FR 33290 (June 1, 2020)]; Filing Fee Disclosure and Payment Methods Modernization, Release No. 33–10997 (Oct. 13, 2021) [86 FR 70166 (Dec. 9, 2021)].

The proposed rules and amendments would provide a more specific and comprehensive framework for advisers and funds to address, report on, and disclose cybersecurity-related risks and incidents. They would directly affect advisers and funds through changes in their obligations related to cybersecurity risks. They would also directly affect investment advisers' and funds' current and prospective clients and investors. In addition, the proposed rules may affect third-party service providers to advisers and funds.

We anticipate that the main economic benefits of the proposed rules and amendments would be to enhance certain advisers' and funds' cybersecurity preparedness and thereby reduce related risks to clients and investors, to improve clients' and investors' information about advisers' and funds' cybersecurity exposures, and to enhance the Commission's ability to assess systemic risks and its oversight of advisers and funds. We expect the main economic costs of the proposed rules and amendments to be compliance costs [86] borne by investment advisers and funds—costs likely to be passed on to their respective clients and investors. We do not anticipate that these costs and benefits will be material in the aggregate, although they may have significant effects on individual advisers, funds, and their respective clients and investors.

We expect that the proposed rules and amendments would have a more significant effect on smaller advisers and smaller fund families as well as their clients and investors. Such differential impacts would likely have some effect on competition in the adviser and fund management markets, although the direction of this effect is ambiguous.[87] In addition to providing clients and investors with additional cybersecurity-related information about advisers and funds, we expect the proposed amendments to increase investors' confidence in the operational resiliency of advisers and funds and safety of their investments held through those firms. In so doing, we expect that the proposed amendments would improve economic efficiency and enhance capital formation.

Many of the benefits and costs discussed below are difficult to quantify. For example, the effectiveness of cybersecurity hygiene measures taken as a result of the proposed amendments on the probability of a cybersecurity incident and on the expected cost of such an incident, including remediation costs, is subject to numerous assumptions and unknowns, and is thus impracticable to quantify. Also, in some cases, data needed to quantify these economic effects are not currently available. For example, the Commission does not have reliable data on the incidence of cybersecurity incidents for advisers and funds. While we have attempted to quantify economic effects where possible, much 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 a quantification of the proposal's economic effects.

B. Broad Economic Considerations

While advisers and funds have private incentives to maintain some level of cybersecurity hygiene, market failures can lead the privately optimal level to be inadequate from the perspective of overall economic efficiency: Such market failures provide the economic rationale for regulatory intervention in advisers' and funds' cybersecurity practices. At the core of these market failures is asymmetric information about cybersecurity preparations and incidents as well as negative externalities to these incidents. Asymmetric information contributes to two main inefficiencies: First, because the production of cybersecurity defenses must constantly evolve, an adviser's or fund's inability to observe cyberattacks on its competitors inhibits the efficacy of its own cybersecurity preparations. Second, for a client or investor, the inability to observe an adviser's or fund's effort in cybersecurity preparation gives rise to a principal-agent problem that can contribute to an adviser or fund exerting too little effort (*i.e.,* underinvesting or underspending) on cybersecurity preparations. Moreover, because there can be substantial negative externalities related to cybersecurity incidents, advisers' and funds' private incentives to exert effort on cybersecurity preparations are likely to be lower than optimal from a societal standpoint.

In the production of cybersecurity defenses, the main input is information. In particular, information about prior attacks and their degree of success is immensely valuable in mounting effective countermeasures.[88] However, firms are naturally reluctant to share such information freely: Doing so can assist future attackers as well as lead to loss of customers, reputational harm, litigation, or regulatory scrutiny.[89] Moreover, because disclosure of such information creates a positive information externality [90]—the benefits of which accrue to society at large and which cannot be fully captured by the firm making the disclosure—an inefficient market equilibrium is likely to arise. In this market equilibrium, too little information about cybersecurity incidents is disclosed, leading to inefficiently low levels of cybersecurity defense production.[91]

Asymmetric information also contributes to a principal-agent problem. The relationship between an adviser and its client or a fund and its investor is one where the principal (the client or fund investor) relies on an agent (the investment adviser or fund complex and its management) to perform services on the principal's behalf.[92] Because principals and their agents do 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.[93] Although private contracts between principals and agents aim to minimize such costs, they are limited in their ability to do so; this limitation provides one rationale for regulatory intervention.[94]

[86] Throughout this economic analysis, ''compliance costs'' refers to the direct and indirect costs resulting from material changes to affected registrants' business practices that may be required to comply with the proposed regulations (*e.g.,* conducting cybersecurity analysis of deployed systems, replacing outdated insecure computer software, hiring staff to implement cybersecurity improvements, renegotiating contracts with service providers, exposing aspects of secret business practices through mandated disclosures). As used here, ''compliance costs'' excludes certain administrative costs of the proposed regulations (*e.g.,* filling out and filing required forms, conducting legal reviews of mandated disclosures) subject to the Paperwork Reduction Act. These administrative costs are discussed in detail in the Paperwork Reduction Act analysis in section IV.

[87] Both costs and benefits would have differential effects. *See infra* section III.E.

[88] *See* Peter W. Singer and Allan Friedman, Cybersecurity: What Everyone Needs to Know. *Oxford University Press* 222 (2014).

[89] *See, e.g., Federal Trade Commission* v. *Equifax, Inc.* (2019), *available at https://www.ftc.gov/enforcement/cases-proceedings/172-3203/equifax-inc.*

[90] However, disclosure of this information to parties that do not obey the law creates significant negative externalities as it can facilitate attacks against those who employ similar business methods and IT systems. *See infra* section III.D.2.b (discussing the potential costs of excessive disclosure).

[91] This problem has long been recognized by policymakers leading to various efforts aimed at encouraging voluntary information sharing across firms. *See infra* section III.C.1.

[92] *See* Michael C. Jensen and William H. Meckling, Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure, 3 *Journal of Financial Economics,* 305–360 (1976) (''Jensen and Meckling'').

[93] *Id.*

[94] Such limitations can arise from un-observability or un-verifiability of actions,

Continued

In the context of cybersecurity, the principal-agent problem is one of underspending in cybersecurity—agents exerting insufficient effort toward protecting the personal information, investments, or funds of the principals from being stolen or otherwise compromised. For example, in a recent survey of financial firms, 58% of the respondents self-reported ''underspending'' on cybersecurity.[95] Several factors can contribute to this underspending. Agents (*i.e.,* advisers and funds) may not be able to credibly signal to their principals (*i.e.,* clients or investors) that they are better at addressing cybersecurity risks than their peers, reducing their incentives to bear such costs.[96] At the same time, agents who do not bear the full cost of a cybersecurity failure (*e.g.,* losses of their customers' information or assets) will prefer to avoid bearing costs—such as elaborate cybersecurity practices—the benefits of which accrue in large part to principals (*i.e.,* clients and investors).

Agents' reputation motives—the fear of market-imposed loss of future profits—should generally work against the tendency for agents to underinvest in cybersecurity measures. However, for smaller agents—who do not enjoy economies of scale or scope, and generally have less valuable brands—the cost of implementing robust cybersecurity measures will be relatively high, while their reputation motives will be more limited. Thus, smaller agents can be expected to be especially prone to underinvestment.

Even in the absence of agency problems, advisers and funds may still underinvest in cybersecurity due to negative externalities or moral hazard. In the context of cybersecurity, negative externalities arise because a disruption to the operation or financial condition of one financial entity can have significant negative repercussions on the financial system broadly.[97] For example, a cybersecurity incident at a large money market fund that affects its ability to process redemptions could disrupt the fund's shareholders' ability to access cash needed to satisfy other obligations, potentially leading those shareholders to default, which, in turn, could trigger further defaults by those shareholders' creditors. Alternatively, a cybersecurity incident may adversely affect market confidence and curtail economic activity through a confidence channel.[98] As such costs would not be internalized by advisers and funds, advisers and funds would be expected to underinvest in measures aimed at avoiding such costs. In addition, advisers and funds may also underinvest in their cybersecurity measures due to moral hazard from expectations of government support.[99] For example, a large fund may realize that it is an attractive target for sophisticated state actors aiming to disrupt the U.S. financial system. Protection against such ''advanced persistent threats'' [100] from sophisticated actors is costly.[101] A belief that such an attack would be met with government support could lead to moral hazard where the fund underinvests in defenses aimed at countering this threat.

The proposed amendments could mitigate these problems in several ways. First, establishing explicit requirements for cybersecurity policies and procedures could help ensure that investment advisers and funds devote a certain minimum amount of effort toward cybersecurity readiness. Second, the proposed disclosure and regulatory reporting requirements could help alleviate the information asymmetry problems by providing current and prospective investors and clients, third parties (*e.g.,* fund rating services), and regulators with more information about funds' and advisers' cybersecurity exposure. The publicly disclosed information could in turn be used by investors, clients, and third parties to screen and monitor funds and investment advisers, while the confidential regulatory reports could be used by regulators to inform industry and law enforcement about ongoing threats. Finally, by reducing uncertainty about the effectiveness of funds' and investment advisers' cybersecurity measures, the proposed amendments could help level the competitive playing field for funds and advisers by simplifying prospective investors' and clients' decision making.[102] By addressing important market imperfections, the proposed amendments could mitigate underinvestment in cybersecurity and improve the adviser and fund industry's ability to produce effective cybersecurity defenses through better information sharing, which could in turn lead to improved economic efficiency.

The effectiveness of the proposed amendments at mitigating the aforementioned problems would depend on several factors. It would depend on the extent to which the proposed amendments materially affect registrants' policies and procedures and disclosures. Insofar as the new requirements affect registrants' policies and procedures, the effectiveness of the proposed amendments would also depend on the extent to which the actions they induce alleviate cybersecurity underinvestment. The effectiveness of the proposed amendments would also depend on the extent to which the proposed disclosure requirements provide useful

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 (1) *American Economic Review,* 265–94 (Mar. 2009) (discussing a relatively modern treatment of these issues) (''Tirole'').

[95] Institute of International Finance, *IIF/McKinsey Cyber Resilience Survey* (Mar. 2020), *available at https://www.iif.com/Portals/0/Files/content/cyber_resilience_survey_3.20.2020_print.pdf* 2020) (''IIF/McKinsey Report''). A total of 27 companies participated in the survey, with 23 having a global footprint. Approximately half of respondents were European or U.S. Globally Systemically Important Banks (G–SIBs).

[96] *See* Sanford J. Grossman, The Informational Role of Warranties and Private Disclosure about Product Quality, 24 (3) *The Journal of Law and Economics* 461–83 (Dec. 1981); *see also* Michael Spence, Competitive and Optimal Responses to Signals: An Analysis of Efficiency and Distribution, 7 (3) *Journal of Economic Theory* 296–332 (Mar. 1, 1974); G.A. Akerlof, The Market for ''Lemons'': Quality Uncertainty and the Market Mechanism, 84 (3) *The Quarterly Journal of Economics* 488–500 (Aug. 1970).

[97] *See* Anil K. Kashyap and Anne Wetherilt, Some Principles for Regulating Cyber Risk, *AEA Papers and Proceedings* 109, 482–487 (May 2019).

[98] *Id.*

[99] 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,* King (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 University Press* (2010). *See also* Viral V. Acharya, Deniz Anginer, and A. Joseph Warburton, The End of Market Discipline? Investor Expectations of Implicit Government Guarantees, *SSRN Scholarly Paper. Rochester, NY: Social Science Research Network* (May 1, 2016).

[100] Advanced persistent threat (APT) 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), Usenix LISA 09 (Nov. 4, 2009), *available at https://www.usenix.org/legacy/events/lisa09/tech/slides/daly.pdf.*

[101] *See* Nikos Virvilis, and Dimitris Gritzalis, The Big Four—What We Did Wrong in Advanced Persistent Threat Detection? *2013 International Conference on Availability, Reliability and Security,* 248–54 (2013).

[102] By analogy, in the absence of rigorous airline safety regulation, shopping for airline tickets would be considerably more complex as one would need to consider not only each airline's price and level of service, but also the adequacy of each airline's maintenance regime, the age of its fleet, and the training of its pilots.

information to investors, clients, third parties, and regulators.[103]

C. Baseline

The market risks and practices, regulation, and market structure relevant to the affected parties in place today form the baseline for our economic analysis. The parties directly affected by the proposed amendments are advisers that are registered or required to be registered with the Commission and funds. In addition, the proposed amendments would indirectly affect current and prospective clients of such advisers (including private funds) and investors in such funds as well as certain service providers to advisers and funds. Finally, these amendments could also affect issuers of financial assets whose access to and cost of capital could change because of the proposed amendments' effects on the asset management markets.

1. Cybersecurity Risks and Practices

With the widespread adoption of internet-based products and services over the last two decades, all businesses have had to address issues of cybersecurity. For financial services firms, the stakes are particularly high—it is where the money is. Cybersecurity threat intelligence surveys consistently find the financial sector to be one of—if not the most—attacked industry,[104] and remediation costs for such incidents can be substantial.[105] The financial services sector has also been at the forefront of digitization and now represents one the most digitally mature sectors of the economy.[106] Not surprisingly, it is also one of the biggest spenders on cybersecurity measures: A recent survey found that non-bank financial firms spent an average of approximately 0.5% of revenues—or $2,348/employee—on cybersecurity.[107]

The ubiquity and rising costs of cybercrime[108] along with firm's increasingly costly efforts to prevent it[109] has created a boom in the cybersecurity industry[110] and led to the development of a numerous technologies, standards, and industry noted ''best practices'' aimed at mitigating cybersecurity threats. Many of these developments— multi-factor authentication, HTTPS, and user-access control—are so widely deployed as to be in common parlance. Among practitioners (chief technology officers, chief information officers, chief security officers (''CISOs'') and their staffs), best practice frameworks such as Carnegie Mellon University's Cyber Resilience Review,[111] the NIST Framework,[112] and similar offerings from cybersecurity consultants and product vendors are now frequently employed to assess and address institutional cybersecurity preparedness. Such frameworks cover the gamut of cybersecurity, including: IT 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, company boards and executive management teams have been paying more attention to many of these areas.[113]

While spending on cybersecurity measures in the financial services industry is considerable, it may nonetheless be inadequate—even in the estimation of financial firms themselves: According to one recent survey, 58% of financial firms self-reported ''underspending'' on cybersecurity measures.[114] And while adoption of cybersecurity best practices has been accelerating overall, many firms continue to lag in their adoption.[115] While surveys of financial services firms are suggestive, the true extent of advisers' and funds' underspending—and of failing to adopt industry-accepted cybersecurity ''best practices''—is impracticable to quantify.[116]

Similarly, it is impracticable to quantify the adequacy of advisers' and funds' information sharing arrangements.[117] 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.[118] The FS–ISAC provides financial firms with such a forum.[119] However, observers have questioned the efficacy of these information-sharing partnerships,[120] while the U.S. Government has continued in attempts to further such efforts. For example, President Obama's 2015 Executive Order, ''Promoting Private Sector Cybersecurity Information Sharing'' aimed ''to encourage the voluntary formation of [information sharing organizations], to establish mechanisms to continually improve the capabilities and functions of these organizations, and to better allow these organizations to partner with the Federal Government on a voluntary basis.''[121] Although the Commission does not have data on the extent of advisers' and funds' 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 information about cybersecurity threats voluntarily, with larger firms being

[103] Similar arguments have been put forward with respect to disclosure's utility in predicting adviser fraud. *See, e.g.,* Stephen Dimmock and William Gerken, Predicting Fraud by Investment Managers, 105 (1) *Journal of Financial Economics,* 153–173 (2012).

[104] *See, e.g.,* IBM, *X-Force Threat Intelligence Index 2021* (2021), *available at https://www.ibm.com/security/data-breach/threat-intelligence.*

[105] *See, e.g., supra* footnote 6 (Cost of Data Breach Report) and accompanying text (noting the average cost of a data breach in the financial industry in the United States is $5.72 million).

[106] *See* BCG Global, *Digital Maturity Is Paying Off* (Nov. 6, 2020), *available at https://www.bcg.com/publications/2018/digital-maturity-is-paying-off.*

[107] Deloitte LLP, *Reshaping the Cybersecurity Landscape, Deloitte Insights* (accessed Nov. 10, 2021), *available at https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html* (''Reshaping the Cybersecurity Landscape'').

[108] *See supra* footnote 5 (FBI 2020 Internet Crime Report, noting that cybercrime victims lost approximately $4.2 billion in 2020).

[109] *See* Office of Financial Research, *Annual Report to Congress* (2021), *available at https://www.financialresearch.gov/annual-reports/files/OFR-Annual-Report-2021.pdf.*

[110] VentureBeat, *The Cybersecurity Industry Is Burning—But VCs Don't Care* (Sept. 2, 2021)), *available at https://venturebeat.com/2021/09/02/the-cybersecurity-industry-is-burning-and-vcs-dont-care/* (''VentureBeat'').

[111] U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, *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.*

[112] *See supra* footnote 24.

[113] *See* Reshaping the Cybersecurity Landscape, *supra* footnote 107.

[114] *See* IIF/McKinsey Report, *supra* footnote 95.

[115] *See* VentureBeat, *supra* footnote 110.

[116] As noted in section III.B, the quality of cybersecurity measures is difficult to quantify. Moreover, the cybersecurity measures being employed by registrants are not generally observable. Consequently, it is not practicable to estimate the adequacy of measures currently being employed by registrants.

[117] The Commission does not currently collect data from registrants regarding the presence of such arrangements. We are also not aware of any third-party data providers that tabulate this information.

[118] *See* President Decision Directive/NSC–63, Critical Infrastructure Protection (May 22, 1998); Presidential Decision Directive 63 on 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.*

[119] More information about the FS–ISAC is available at *https://www.fsisac.com.*

[120] Denise E. Zheng and James A. Lewis, Cyber Threat Information Sharing, *Center for Strategic and International Studies* 62 (2015).

[121] *See* Executive Order 13691, Promoting Private Sector Cybersecurity Information Sharing (Feb. 13, 2015).

more likely to do so.[122] Other surveys paint a similar picture; a recent survey of financial firms found that while recognition of the value of information-sharing arrangements is widespread, a majority of firms report hesitance to participate due to regulatory restrictions or privacy concerns.[123]

2. Regulation

As discussed in greater detail in section I.B above, although existing rules and regulations do not impose explicit cybersecurity requirements on advisers and funds, advisers' duties as fiduciaries, as well as several existing rules and regulations applicable to advisers and funds indirectly implicate cybersecurity. As fiduciaries, advisers are required to act in the best interest of their clients at all times.[124] This fiduciary obligation includes taking steps to minimize cybersecurity risks that could lead to significant business disruptions or a loss or misuse of client data.[125] Additionally, the Advisers Act compliance rule requires advisers to consider their fiduciary and regulatory obligations and formulate policies and procedures to address them.[126] While the Advisers Act compliance rule does not enumerate specific cybersecurity elements that an adviser must include in its compliance program,[127] the Commission has previously stated that advisers should consider factors creating risk exposure for the firm and its clients and design policies and procedures that address those risks.[128] As the potential for a cybersecurity incident to create significant operational disruptions is well understood at this point, we understand that larger advisers with significant IT infrastructures are assessing cybersecurity risks when developing their compliance policies and procedures.[129]

One potential risk for an adviser's client stemming from the cybersecurity threats faced by the adviser, is that a cybersecurity incident at the adviser could lead to the client's information[130] being compromised or the loss of the client's assets. Nominally, the risk of outright loss should be limited for assets subject to 17 CFR 275.206(4)–2 (the ''Custody Rule''),[131] which are—by effect of said rule—generally held by ''qualified custodians.'' Qualified custodians are typically large financial institutions.[132] Such financial institutions generally enjoy significant economies of scale, have large franchise (and reputation) values, and are subject to numerous additional regulatory requirements.[133] For these reasons, cybersecurity protections provided by qualified custodians may be well-developed, and could help mitigate the risk of outright loss of client funds and securities in advisers' custody.[134]

Although protection provided by qualified custodians can mitigate risk to certain client assets to some extent, they cannot replace cybersecurity hygiene at the adviser level. As an adviser's ''custody'' of client assets implies a degree of control over those assets, compromise of adviser's systems—or the adviser's service providers' systems—could lead to unauthorized actions being taken with respect to those assets—including assets maintained with qualified custodians. Moreover, as observed by Commission staff, advisers may fail to realize that they have ''custody'' of client funds and securities, and may not place these assets with a qualified custodian.[135] Such problems can occur when, for example, an adviser holds login credentials to clients' accounts or when the adviser or a related person of the adviser serves as trustee of, or has been granted power of attorney for, client accounts.[136]

The Investment Company Act compliance rule requires a fund to adopt and implement written policies and procedures reasonably designed to prevent violations of the Federal securities laws by the fund and named service providers.[137] We believe that operating a fund today generally requires considerable IT sophistication, especially in the case of open-end funds.[138] Therefore, we believe that all but the smallest funds likely take into account cybersecurity risks when developing their compliance policies and procedures under the Investment Company Act compliance rule.

A number of other Commission rules also implicate cybersecurity. Regulation S–P requires advisers and funds to adopt written policies and procedures that address protection of customer records and information, which likely would include reasonably designed cybersecurity policies and procedures.[139] In addition, advisers and

[122] FINRA, *Report on Cybersecurity Practices* (Feb. 2015), *available at https://www.finra.org/sites/default/files/2020-07/2015-report-on-cybersecurity-practices.pdf.* Survey respondents included large investment banks, clearing firms, online brokerages, high-frequency traders, and independent dealers. Thus, the results should be taken as suggestive of practices that may be in place at advisers and funds.

[123] *See* Reshaping the Cybersecurity Landscape, *supra* footnote 107. Survey respondents consisted of CISOs (or equivalent) of 53 members of the FS–ISAC. Of the respondents, twenty-four reported being in the retail/corporate banking sector, twenty reported being in the consumer/financial services (non-banking) sector, and seventeen 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.

[124] *See supra* footnote 9.

[125] *See supra* section I.B (discussing fiduciary obligations).

[126] *See supra* section I.B (discussing Advisers Act compliance rule).

[127] According to the rule, an adviser should identify conflicts of interest and other compliance factors creating risk exposure for the firm and its clients in light of the firm's particular operations. *See supra* footnote 10 and accompanying text.

[128] *See* Compliance Program Release, *supra* footnote 10, at n.22 and accompanying text.

[129] *See, e.g.,* Chuck Seets, Jamie Smith, and Steve Klemash, What Companies Are Disclosing About Cybersecurity Risk and Oversight, *The Harvard Law School Forum on Corporate Governance* (blog), (Aug. 25, 2020), *available at https://corpgov.law.harvard.edu/2020/08/25/what-companies-are-disclosing-about-cybersecurity-risk-and-oversight/* (finding that 100 percent of Fortune 100 companies list cybersecurity as a risk factor in 2020 SEC disclosures, and 93 percent referenced efforts to mitigate such risks).

[130] Advisers may possess a wide range of potentially sensitive information relating to their clients, including personally identifiable information, portfolio composition, transaction histories, and confidential correspondence.

[131] The Custody Rule applies only to client funds and securities. 17 CFR 275.206(4)–2. In practice, staff has observed that many advisers treat all assets in the same way.

[132] 17 CFR 275.206(4)–2(a) and (d). A qualified custodian can be a bank, broker-dealer, futures commission merchant, or certain foreign financial institutions. The qualified custodian maintains client's funds and securities in a separate account for each client. Alternatively, the adviser's clients' funds and securities can be held in an account under the adviser's name as agent or trustee for the clients.

[133] *See, e.g., Interagency Guidelines Establishing Information Security Standards,* 12 CFR 225 Appendix F; *see also* Information Technology Risk Examination (''InTREx'') Program, *FDIC Financial Institution Letter* FIL–43–2016 (June 30, 2016).

[134] *See id.* The qualified custodian industry is dominated by large U.S. banking entities which are subject to various regulations, guidance, and examinations relating to cybersecurity.

[135] *See* SEC, EXAMS Risk Alert, Significant Deficiencies Involving Adviser Custody and Safety of Client Assets, (Mar. 4, 2013), *available at https://www.sec.gov/about/offices/ocie/custody-risk-alert.pdf.*

[136] *Id.*

[137] 17 CFR 270.38a–1. The Investment Company Act compliance rule also requires the fund to: (1) Designate a CCO responsible for administering the policies and procedures, subject to certain requirements, including providing the fund's board with an annual report; and (2) review the adequacy of the policies and procedures and the effectiveness of their implementation at least annually.

[138] The logistics of dealing with daily redemption requests, producing daily NAVs, and complying with the Commission's N–PORT filing requirements and liquidity rule (rule 22e–4 under the Investment Company Act) are not feasible without significant investments in IT infrastructure. *See, e.g.,* Investment Company Reporting Modernization, Investment Company Act Release No. 32314 (Oct. 13, 2016) [81 FR 81870 (Nov. 18, 2016)], at 360.

[139] *See* Regulation S–P Release, *supra* footnote 14; *see also* Disposal of Consumer Report Information Release, *supra* footnote 14 (requiring written policies and procedures under Regulation S–P). *See* Compliance Program Release, *supra* footnote 10 (stating expectation that policies and procedures would address safeguards for the privacy protection of client records and information and noting the applicability of Regulation S–P).

funds subject to Regulation S–ID must develop and implement a written identity theft program that includes policies and procedures to identify and detect relevant red flags.[140] Compliance with one or both of the aforementioned requirements requires certain reasonably designed cybersecurity policies and procedures to be in place.[141]

Some affected registrants may also be subject to other regulators' rules implicating cybersecurity. We understand that private funds may be subject to the Federal Trade Commission's recently amended 16 CFR 314.1 through 16 CFR 314.5 (Standards for Safeguarding Customer Information (''FTC Safeguards Rule'')) that contains a number of modifications to the existing rule with respect to data security requirements to protect customer financial information.[142] To the extent that a private fund subject to the FTC Safeguards Rule is managed by an adviser that is registered with the Commission, our proposed rule would result in some overlapping regulatory requirements.[143] As recently amended, the FTC Safeguards Rule generally requires financial institutions to develop, implement, and maintain a comprehensive information security program that consists of the administrative, technical, and physical safeguards the financial institution uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.[144] The key provision of the rule is the requirement to design and implement a comprehensive information security program with safeguards for access controls, data inventory and classification, encryption, secure development practices, authentication, information disposal procedures, change management, testing, and incident response.[145] It also requires written periodic risk assessments, and that the safeguards' be designed so as to address risks identified through such assessments.[146] In addition, it requires financial institutions to take reasonable steps to select and retain service providers capable of maintaining appropriate safeguards for customer information and require those service providers by contract to implement and maintain such safeguards.[147] Although narrower in scope than the rules being proposed here [148] and generally more prescriptive,[149] the FTC Safeguards Rule provisions are congruent with the requirements for cybersecurity policies and procedures,[150] annual review,[151] and board oversight being proposed here.[152] The FTC Safeguards Rule does not currently include disclosure, regulatory reporting, or recordkeeping requirements.[153]

3. Market Structure

Advisers that would be subject to the proposed rules provide a variety of services to their clients, including: Financial planning advice, portfolio management, pension consulting, selecting other advisers, publication of periodicals and newsletters, security rating and pricing, market timing, and educational seminars.[154] Although advisers can expose clients to cybersecurity threats through any of these activities, the potential for harm can vary widely across advisers. A cybersecurity breach at an adviser that only offers advice on wealth allocation strategies may not have a significant negative effect on its clients: Such adviser may not hold much client information beyond address, payment details, and the client's overall financial condition. On the other hand, a breach at an adviser that performs portfolio management services exposes clients to much greater risk: Such an adviser will not only hold client personally identifiable information and records, but also typically have some degree of control over client assets. In addition, even a brief disruption to the services offered by advisers performing portfolio management services (*e.g.,* a ransomware attack) could have large negative repercussions on the adviser's clients (*e.g.,* inability to access funds and securities).

Based on Form ADV filings up to October 31, 2021, there were 14,774 advisers with a total of $113 trillion in assets under management.[155] Practically all (97%) of the advisers reported providing portfolio management services to their clients.[156] Over half (55%) reported having custody [157] of clients' cash or securities either directly or through a related person with client funds in custody totaling $39 trillion.[158]

BILLING CODE 8011–01–P

[140] *See* Identity Theft Release, *supra* footnote 16.

[141] The scope of the Regulation S–ID differs from Regulation S–P. Regulation S–P applies to the protection of customer records and information by advisers and funds, whereas Regulation S–ID applies to funds and advisers that meet the definition of ''financial institution'' or ''creditor'' that offers or maintains ''covered accounts.'' *See* Regulation S–P Release, *supra* footnote 14; *see also* Identity Theft Release, *supra* footnote 16 ( ).

[142] *See* Federal Trade Commission, *Standards for Safeguarding Customer Information* (Oct. 27, 2021) [86 FR 70272 (Dec. 9, 2021)]. Although the amended rule became formally effective on January 10, 2022, a number of detailed measures must generally be adopted by December 9, 2022. *Id.*

[143] The Gramm Leach Bliley Act (''GLBA'') delegates the authority to create privacy and security standards to specified financial regulators. Public Law 106–102, 113 Stat. 1338, §§ 501–527 (1999) (codified at 15 U.S.C. 6801 *et seq.*). The GLBA gives the FTC the regulatory authority for financial institutions that are not subject to the jurisdiction of any other regulator under that Act. *Id.* (defining ''financial institution'' to mean ''any institution the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act of 1956'').

[144] 16 CFR 314.2(c).

[145] 16 CFR 314.4(c), (d), and (h). These ''safeguard'' elements of the FTC rule are effectively more prescriptive versions of the User Security and Access, Information Protection, and Cybersecurity Incident Response and Recovery elements being proposed here. *See supra* sections II.A.1.b, II.A.1.c, and II.A.1.e.

[146] 16 CFR 314.4(b), (c). These elements of the FTC rule are analogous to the Risk Assessment and Threat and Vulnerability Management elements being proposed here. *See supra* sections II.A.1.a and II.A.1.d.

[147] 16 CFR 314.4(d). Similar to the rules being proposed here, the FTC Safeguards Rule requires oversight of third-party service providers. *See* proposed rules 38a–2(a)(3)(ii) and 206(4)–9(a)(3)(ii).

[148] The scope of the FTC Safeguards Rule is limited to protecting customer information. 16 CFR 314.3(a).

[149] The FTC Safeguards Rule imposes various technical requirements such as the use of encryption and multi-factor authentication. 16 CFR 314.4(c)(3) and (c)(5).

[150] *See supra* footnotes 145 and 146.

[151] *See* proposed rule 38a–2(b) and 16 CFR 314.4(i); *see also supra* section II.A.2.

[152] *See* proposed rule 38a–2(c) and 16 CFR 314.4(i); *see also supra* section II.A.3.

[153] The FTC, however, issued a supplemental notice of proposed rulemaking requesting comment on further amending the Safeguards Rule to require regulatory reporting of certain security events. *See* FTC, Standards for Safeguarding Customer Information (Oct. 27, 2021) [86 FR 70062 (Dec. 9, 2021)].

[154] *See* Form ADV.

[155] Broadly, regulatory assets under management is the current value of assets in securities portfolios for which the adviser provides continuous and regular supervisory or management services. *See* Form ADV, Item 5F.

[156] Form ADV, Items 5G(2–5) (as of Oct. 4, 2021).

[157] Here, ''custody'' means ''holding, directly or indirectly, client funds or securities, or having any authority to obtain possession of them.'' An adviser also has ''custody'' if ''a related person holds, directly or indirectly, client funds or securities, or has any authority to obtain possession of them, in connection with advisory services [the adviser] provide[s] to clients.'' *See* 17 CFR 275.206(4)–2(d)(2).

[158] Form ADV, Items 9A and 9B (as of Oct. 4, 2021).

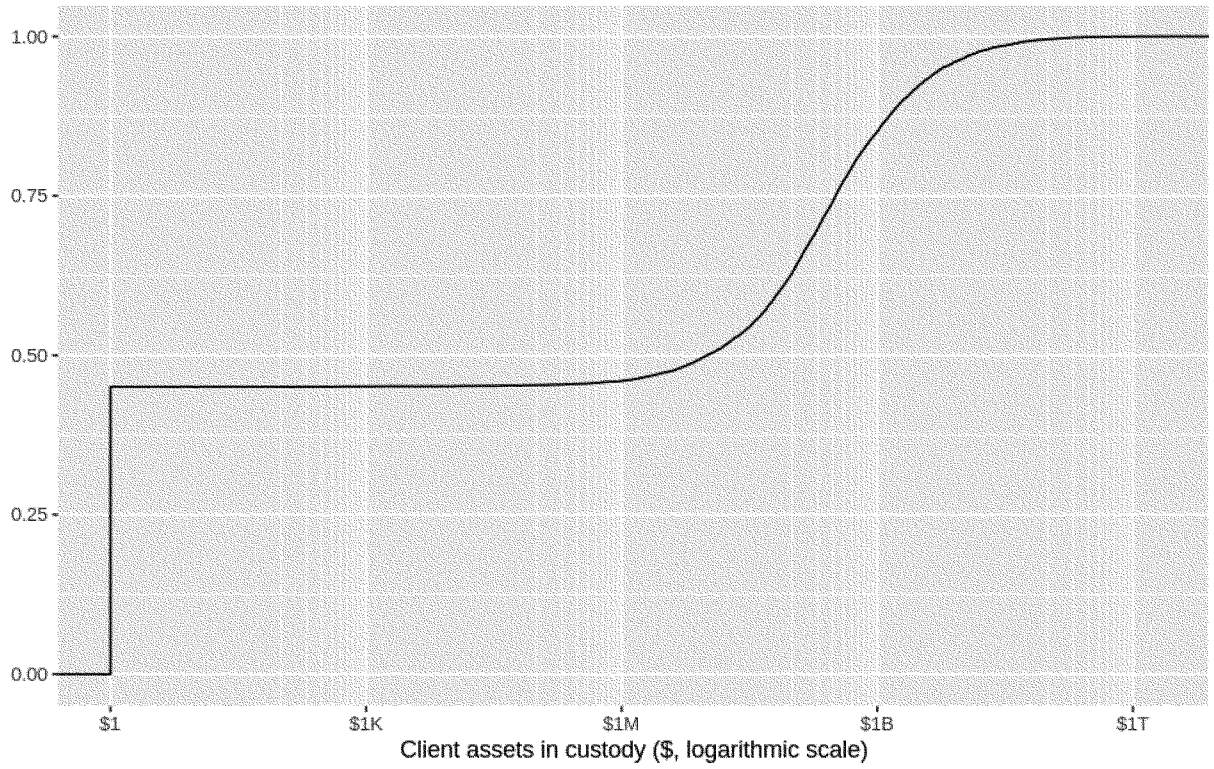

Figure 1: Cumulative distribution of client assets for which advisers have "custody" as defined in rule 206(4)-2. Plotted is the fraction of all advisers (y-axis) having less than the given amount of client assets in custody either directly or through a related person (x-axis, logarithmic scale). Data source: Form ADV filings.

Figure 1 plots the distribution of client assets for which advisers have custody as defined in rule 206(4)–2. The distribution is highly skewed: Four advisers have custody over more than $1 trillion, while half of advisers have custody over less than $10 million. Approximately two thirds of advisers have custody of over $100 million. Many such advisers are quite small, with half reporting fewer than 15 employees.[159] Nearly all (97%) advisers rely on an unrelated person to act as a qualified custodian for customer assets.[160] The qualified custodian industry is dominated by a small number of large U.S. entities.[161]

The funds that would be directly subject to the proposed rules include open-end funds, registered closed-end funds, business development companies, and unit investment trusts.[162] Table 1 presents the breakdown of funds registered with the Commission in 2020. In 2020, there were 15,750 registered funds, with over $25 trillion in net assets.[163] The vast majority of the registered funds (13,248) are open-end funds. Many of the funds (82%) are part of a fund family. There are 290 such fund families. As shown in Figure 2, fund families exhibit considerable variation in size: Some families consist of hundreds of funds, while others consist of just a handful of funds, with the median family consisting of 10 funds. The larger-than-median families represented the majority (10,389) of funds, and nearly all ($23 trillion) industry NAV.[164]

[159] Form ADV, Item 5A (as of Oct. 4, 2021).

[160] Form ADV, Item 9D (as of Oct. 4, 2021).

[161] Deloitte, *The Evolution of a Core Financial Service Custodian & Depository Banks* (2019), *available at https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/financial-services/lu-the-evolution-of-a-core-financial-service.pdf. See also* Eva Su, *Digital Assets and SEC Regulation* (*CRS Report No.* R46208) (updated June 23, 2021), *available at https://crsreports.congress.gov/product/pdf/R/R46208/5* (stating that four large banks service around $114 trillion of global assets under custody).

[162] *See supra* footnote 22.

[163] This amount represents a subset of the $113 trillion of assets under management of advisers. *See supra* footnote 155 and accompanying text.

[164] Form N–CEN. ''Family of investment companies'' means, except for insurance company separate accounts, any two or more registered investment companies that (1) share the same investment adviser or principal underwriter, and (2) hold themselves out to investors as related companies for purposes of investment and investor services.

TABLE 1—FUNDS SUBJECT TO PROPOSED RULE AMENDMENTS, SUMMARY STATISTICS

[For each type of fund, this table presents estimates of the number, net asset value (NAV), and the percentage of funds belonging to some fund family. It also presents the number and NAV of each type of fund that is part of one of the larger (above median) fund families. Data sources: 2020 N–1A, N–2, N–3, N–4, N–6, N–8B–2, S6, and N–CEN filings, Division of Investment Management Investment Company Series and Class Information (2020),[a] Division of Investment Management Business Development Company Report (2020).[b]]

Fund type	Number of funds	NAV [c] ($billion)	In family [d] (%)	Larger families	
				Number of funds [b]	NAV ($billion)
Open-End [e]	13,248	$24,837	82	9,944	$22,613
Closed-End [f]	691	321	81	431	221
BDC [g]	95	135			
UIT [h]	1,716				
Total	15,750	25,378	82	10,389	23,052

[a] SEC, *Commission Investment Company Series and Class Information, available at https://www.sec.gov/open/datasets-investment_company.html.*
[b] SEC, *Business Development Company Report, available at https://www.sec.gov/open/datasets-bdc.html.*
[c] NAV totals based on year 2020 Form N–CEN filings (as of Oct. 4, 2021) and Business Development Company Report.
[d] Family affiliation information is from Form N–CEN filings. Note that there are minor discrepancies in estimates of the total number of funds based on N–CEN filings and estimates (reported elsewhere in this table) based on fund registration forms.
[e] Form N–1A filers; includes all open-end funds, including ETFs registered on Form N–1A.
[f] Form N–2 filers not classified as BDCs.
[g] Form N–2 filers classified as BDCs.
[h] Form N–3, N–4, N–6, N–8B–2, and S–6 filers.

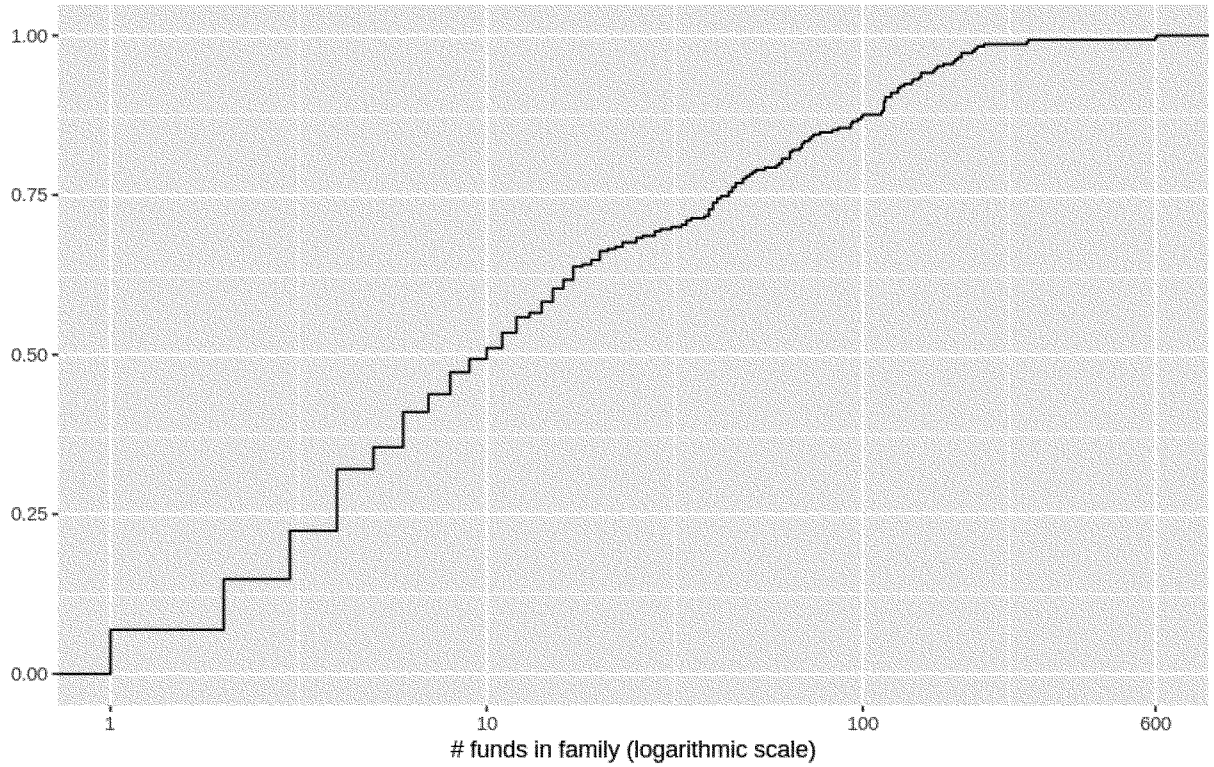

Figure 2: Cumulative distribution of fund family size. Plotted is the fraction of fund families (y-axis) having less than a given number of funds (x-axis, logarithmic scale). The plot shows that 50% of fund families have 10 or more funds.

Although private funds would not be directly subject to the proposed rules, they would be indirectly affected through the proposed provisions on advisers. Approximately one third of advisers (5,231) report advising private funds.[165] Private funds have grown dramatically over the past decade. As plotted in Figure 3, advisers' reported assets under management of private funds more than doubled from $8 trillion to $17 trillion, while the reported number of private funds grew from 24 thousand to 44 thousand.[166]

[165] Form ADV, Item 7B (as of Oct. 4, 2021).

[166] Form ADV, Schedule D (as of Sept. 30, 2021).

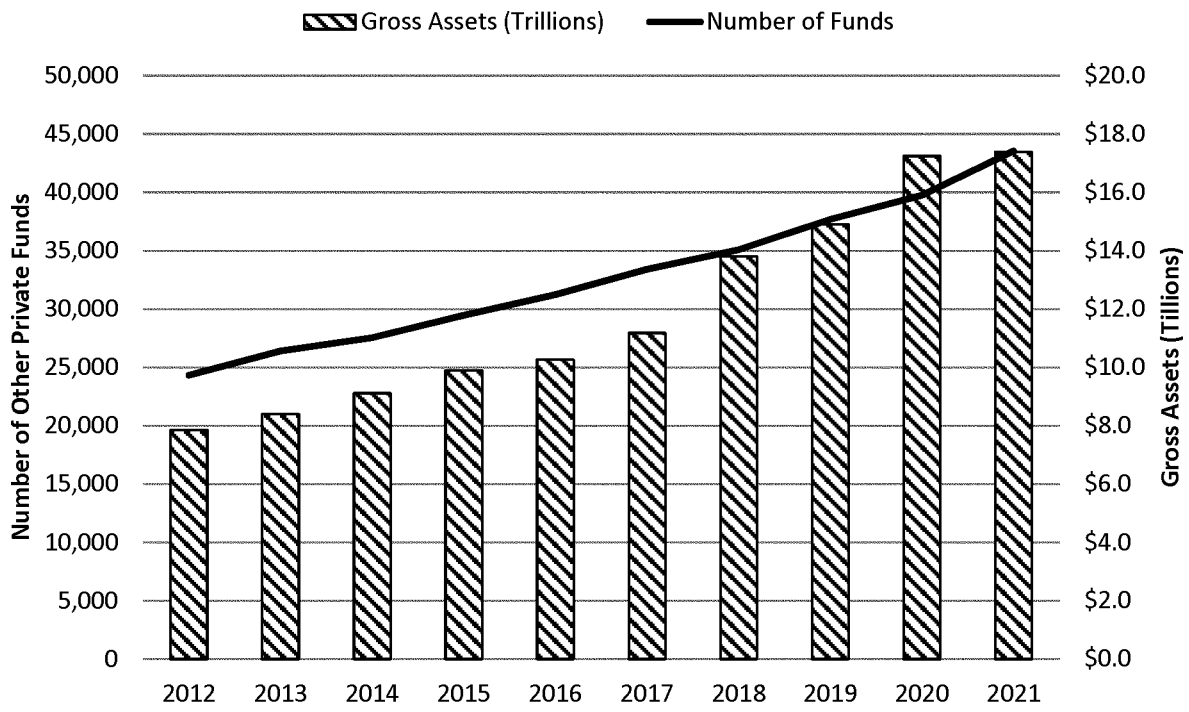

Figure 3: Private funds reported by advisers. Source: Form ADV filings, Schedule D.

BILLING CODE 8011–01–C

D. Benefits and Costs of the Proposed Rule and Form Amendments

The proposed rules would impose four types of new requirements on advisers and funds: (1) Cybersecurity policies and procedures; (2) cybersecurity disclosures; (3) regulatory reporting of cybersecurity incidents; and (4) recordkeeping of cybersecurity incidents. The new requirements would be substantially similar for both advisers and funds. In this section, we consider the benefits and costs of each of these in turn.[167]

1. Cybersecurity Policies and Procedures

The Commission's proposed risk management rules [168] would require all advisers and funds registered with the Commission to implement reasonably designed cybersecurity policies and procedures addressing key elements of cybersecurity preparedness: (1) Risk assessment, including assessment of risks associated with certain service providers, oversight of such providers, and appropriate written contracts with such providers; (2) user security and access; (3) information protection; (4) cybersecurity threat and vulnerability management; and (5) cybersecurity incident response and recovery.[169] Advisers and funds would need to review these policies and procedures at least annually and to prepare a written report of the review's findings; for funds the policies and reviews would be subject to board oversight.[170]

As discussed in section III.C.2, it can be argued that the fiduciary obligations of advisers, existing rules applicable to advisers and funds, the modern technological context, and commonly employed best practices that forms the baseline, may require funds and advisers to implement reasonably designed cybersecurity policies and procedures.[171] However, as noted earlier, Commission staff has observed that some funds and advisers practices in the cybersecurity area raise concerns, and there is reason [172] and evidence [173] to suggest that underinvestment in cybersecurity may be a fairly widespread problem.

a. Benefits

We believe that the Commission's proposed risk management rules would, by imposing comprehensive, explicit requirements to address key elements of cybersecurity preparedness, generally improve the cybersecurity policies and procedures of advisers and funds, and in so doing reduce registrants'—and hence their clients' and investors'—exposure to cybersecurity incidents, as well as reduce the costs incurred by registrants (and their clients and investors) in dealing with such incidents.

Because unaddressed cybersecurity risks impose externalities on the broader financial system, the proposed risk management rules would also likely reduce systemic risk in the economy.[174] In addition, we expect that by imposing explicit cybersecurity requirements on registrants, the proposed rules would enhance the Commission's ability to oversee and enforce rules designed to protect client and investor information and assets.

Registrants that have already implemented cybersecurity policies and

[167] Throughout the following, we also consider benefits and costs related to potential effects on economic efficiency, competition, and capital formation. We summarize these effects in section III.E.

[168] *See* proposed rules 206(4)–9 and 38a–2; *see also supra* section II.A (discussing proposed risk management rules).

[169] *See supra* section II.A.1 (discussing elements of proposed cybersecurity policies and procedures).

[170] In the case of funds, the initial cybersecurity policies and procedures would need to be approved by the fund's board, including a majority of its independent directors; the board would also be provided annual written reports detailing the findings of the reviews. *See supra* sections II.A.2 and II.A.3 (discussing annual written reports and fund board oversight).

[171] *See supra* section III.C.2 (discussing existing rules).

[172] *See supra* section III.C.1.

[173] *See* IIF/McKinsey Report, *supra* footnote 95.

[174] *See supra* footnote 97 and accompanying text.

procedures that adhere to best practices and are consistent with the proposed rules are not expected to undertake material changes to their existing policies and procedures, in which instance the proposed rules would have limited added benefits. Conversely, registrants who do not currently have cybersecurity policies and procedures or have policies and procedures that lack one or more of the enumerated elements, such as those that are not reasonably designed or not reviewed on an annual basis would need to improve their policies and procedures to comply with the proposed rules with attendant benefits to registrants, investors, the broader financial system, and regulators. As we do not currently have reliable data on the extent to which registrants' existing policies and procedures follow industry best practices, address cybersecurity risks, their ''reasonableness,'' or the frequency at which they are reviewed, it is not possible for us to quantify the scale of the benefits arising from the proposed requirements.[175]

b. Costs

We believe that the costs associated with the proposed amendments related to cybersecurity policies and procedures would primarily result from compliance costs borne by advisers and funds in the adoption and implementation of ''reasonably designed'' cybersecurity policies. In addition to the aforementioned direct compliance costs faced by registrants, the proposed requirements would likely impose indirect costs to service providers catering to advisers and funds. Under the proposal, the cybersecurity practices of these service providers would need to be evaluated by advisers and funds subject to the proposed amendments to help ensure that service providers implement and maintain cybersecurity measures that address the required elements of the policies and procedures provisions of this proposal.[176] Some of the cost of such evaluations, as well as the costs of resulting remedial actions may fall on service providers. Moreover, because the proposal requires registrants to include contractual provisions in its agreements with service providers to guarantee adherence to the required measures, the costs associated with negotiating such contractual provisions may also be partly borne by service providers.[177] Ultimately, all these costs may be passed on—in whole or in part—to clients and investors.

As discussed above, we believe that advisers and funds that currently follow cybersecurity best practices will likely find that their existing policies and procedures are largely consistent with the requirement of this proposal and as such, would not need to be materially altered. Similarly, we believe that advisers of private funds subject to the FTC Safeguards Rule will have already developed policies and procedures consistent with the requirements of the current proposal.[178] Consequently, for such registrants, the compliance costs associated with the proposed policies and procedures requirements would likely be minimal.[179] Conversely, registrants who currently do not have policies and procedures in place meeting the proposed requirement would bear compliance costs related to improving them. In the extreme, we expect that registrants with *no* current cybersecurity policies and procedures would have to bear substantial costs. Typical estimates of cybersecurity spending in the financial industry are on the order of 0.5% of revenue;[180] assuming that levels of spending of this order are required to obtain ''reasonably designed'' policies and procedures, registrants who have no such policies would need to bear costs of that order. Of course, as discussed above, it is unlikely that a fund or adviser operating today completely lacks cybersecurity policies and procedures. Here, the same issues that make quantifying the benefits impracticable also render quantification of compliance costs impracticable.[181] However, as discussed in section III.C.1 we believe that existing adviser and fund rules require certain cybersecurity practices to be substantially in place; consequently, the largest compliance costs resulting from the proposed policies and procedures requirement are likely to be borne by registrants not currently following industry noted best practices.[182] We also anticipate that the bulk of any compliance costs associated with developing and implementing policies and procedures would be incurred at the level of an advisory firm (or parent firm) and fund family, rather than by each adviser and fund individually.[183]

The proposed provisions require registrants to consider the cybersecurity risks resulting from their reliance on third-party service providers that receive, maintain, or process adviser or fund information, or are otherwise permitted to access their information systems and any information residing therein.[184] Thus, the proposed requirements would affect a broad range of service providers: Not only entities such as custodians, brokers, and valuation services, but also email providers, customer relationship management systems, cloud applications, and other technology vendors that meet this criterion. Registrants would be required to document that such service providers implement and maintain appropriate measures to protect information of clients and investors and the systems hosting said information, pursuant to a written contract between the registrant and its service provider.[185] As a result, practically all service providers providing business-critical services would face market pressure to (and thus bear costs related to) document and, in some cases, enhance their cybersecurity practices so as to satisfy affected registrants' requirements.[186] Some funds and advisers may find that one or several of their existing service providers may not be able to—or wish to—support compliance with the proposed rule. Similarly, some funds and advisers may find that one or several of their existing service providers may not be able to—or wish to—enter into suitable written contracts. In these cases, the fund or adviser would need to switch service providers and bear the associated switching costs, while the service providers would suffer loss of their fund and adviser customers.[187] In other cases, a fund or adviser may determine that a service provider can be used subject to renegotiation of service agreements,

[175] Generally, quantification in areas that involve ''reasonableness'' criteria is difficult as establishing reasonableness requires case-by-case consideration.

[176] *See* proposed rules 206(4)–9(a)(3)(ii) and 38a–2(a)(3)(ii).

[177] *Id.*

[178] *See supra* section III.C.2.

[179] We separately consider direct costs associated with information collection burdens within the meaning of the Paperwork Reduction Act in section IV. *See also supra* footnote 86.

[180] *See supra* footnote 107.

[181] As noted earlier, we do not currently have reliable data on the extent to which registrants address cybersecurity risks, their ''reasonableness,'' or the frequency at which they are evaluated.

[182] *See supra* section III.C.2.

[183] *See supra* section III.C.3 (noting that 82% of funds belong to 290 fund families).

[184] *See* proposed rules 206(4)–9 and 38a–2.

[185] *See supra* section II.A.1.c.

[186] We note that a service provider involved in any business-critical function would likely need to receive, maintain, or process either adviser or fund information.

[187] If for example the fund or adviser has insufficient market power to affect changes in the service provider's cybersecurity policies. This is most likely to occur with smaller advisers and funds employing generic service providers who do not specialize in providing services to funds or advisers.

potentially imposing substantial contracting costs on the parties.[188]

We expect that for service providers that offer specialized services to the adviser and fund industry, the proposed rule amendments would impose additional costs related to remediating and/or documenting the provider's cybersecurity practices so as to satisfy advisers and funds subject to the proposed amendments. These costs may be passed on to advisers and funds and ultimately to clients and investors. However, we do not generally expect these costs to be large, as we believe that the nature of service provider business models and resulting economies of scale give service providers motivation for and advantages in the development of robust cybersecurity measures and that such measures would generally address the elements required in this proposal.[189]

Providers of more generic services (*e.g.,* customer relationship management systems, cloud storage, or email systems) may also bear some costs related to satisfying requests from large funds and advisers attempting to assess service providers' cybersecurity risk. For example, such providers may be asked to provide additional documentation of their cybersecurity practices, to offer additional guarantees, or to change some aspect of their practices during contract negotiations. Even if satisfying the intent of these additional customer requirements would not represent a significant expense for service providers, contracting frictions are likely to prevent some service providers from doing so.[190] In such cases, registrants would bear costs related to finding alternative service providers while existing service providers would suffer lost revenue.[191]

The aforementioned costs would be particularly acute for smaller advisers and funds that rely on generic service providers. Smaller registrants may not have sufficient bargaining power with service providers of more generic services to effect meaningful changes in cybersecurity practices or contractual provisions.[192] Thus, to the extent that the existing cybersecurity practices of generic service providers cannot be reconciled with the proposed requirements, some advisers and funds may be forced to switch providers and bear the associated switching costs; at the same time, the former service providers would suffer loss of revenue from these customers.

2. Disclosures of Cybersecurity Risks and Incidents

Proposed amendments to part 2A for Form ADV and proposed amendments to fund registration statements would require a narrative description of the cybersecurity risks advisers' face, how they assess, prioritize, and address cybersecurity risks and any significant adviser or fund cybersecurity incidents that had occurred in the past two years.[193] Under the proposed amendments, significant cybersecurity incidents would need to be disclosed either by filing an amendment to Form ADV promptly (in the case of advisers) or by amending a prospectus by filing a supplement with the Commission (in the case of funds).[194] For fund registration statements, the proposed amendments would require the disclosures to be submitted using the Inline XBRL structured data language.[195]

a. Benefits

As discussed in section III.B there exists an information asymmetry between clients and investors vis-à-vis advisers and funds. This information asymmetry, together with limitations to private contracting,[196] inhibits clients' and investors' ability to screen and discipline advisers and funds based on the effectiveness of their cybersecurity policies. In principle, the proposed disclosure requirements would help alleviate this information asymmetry, and in so doing enable clients and investors to better assess the effectiveness of advisers' and funds' cybersecurity preparations and the cybersecurity risks of different advisers and funds. For example, clients and investors could use the frequency or nature of significant cybersecurity incidents—as disclosed under the proposed amendments—to infer an adviser's or fund's effort toward preventing cyberattacks. Likewise, clients and investors could use the narrative descriptions of cybersecurity incident handling procedures to avoid advisers and funds with less well-developed procedures.

The scale of an information asymmetry mitigation benefit would depend on the degree to which the proposed disclosures reveal information useful to clients and investors about risks and on their ability to use it to infer the level of cybersecurity preparations implemented by advisers and funds. Even when cybersecurity preparations are high, a cybersecurity attack may succeed.[197] If some types of reportable cybersecurity incidents are largely the result of chance while other types are a result of insufficient cybersecurity preparation, the client or investor would need to be able to differentiate between the two types of incidents to extract useful information about a fund's or adviser's level of cybersecurity preparations.[198] Many clients and investors are unlikely to be experts on cybersecurity, and their ability to make these distinctions could be limited.[199]

To the extent such information asymmetry reduction effects result from the proposed cybersecurity incident disclosures in fund registration statements, an Inline XBRL requirement would likely augment those effects by

[188] These costs include the direct costs associated with reviewing and renegotiating existing agreements as well as indirect costs arising from service providers requiring additional compensation for providing the required contractual provisions.

[189] For such service providers, the delivery of services via communication networks is often at the core of the business, practically necessitating reasonably designed cybersecurity policies. Moreover, such service providers generally deliver their products (or some customizations thereof) to multiple customers, resulting in economies of scale in the development of cybersecurity measures.

[190] For example, the costs associated with legal review of alterations to standard contracts may not be worth bearing if affected registrants represent a small segment of the service provider's business.

[191] At the same time, these frictions would benefit service providers that cater to customers in regulated industries.

[192] For example, it is highly unlikely that a small investment adviser would be able to effect any changes in its contracts with providers of generic services such as Amazon or Google.

[193] *See supra* section II.C.

[194] *See* proposed rule 204–3; *see also supra* footnotes 80 and 81 and accompanying text.

[195] *See supra* section II.C.4.

[196] *See* Tirole, *supra* footnote 94.

[197] Although ''adequate'' cybersecurity preparations can be expected to reduce cybersecurity incidents, they are unlikely to eliminate them entirely. For example, a firm may suffer a cybersecurity breach due to an attacker discovering a ''zero-day exploit'' (*i.e.,* an exploit that is not generally known to exist) in some underlying IT system. As a practical matter, even the best preparation (*e.g.,* keeping up to date with vendor patches, quickly addressing vulnerabilities, etc.) may not be effective against such exploits. Similarly, for many firms, it may not be feasible to fix a known vulnerability immediately (*e.g.,* weakness in an encryption algorithm) as the fix may require upgrades to numerous systems. In this case, many firms could be exposed to a vulnerability for some time. Because the time it takes for an attacker to exploit such a vulnerability successfully is likely to involve some element of chance, firms that ultimately suffer an incident resulting from such a vulnerability may simply be ''unlucky.''

[198] For example, incidents resulting from advanced persistent threats may be unavoidable, or avoidable only through very high level of effort. *See supra* footnote 100. On the other hand, incidents arising from brute force password attacks can be avoided with minimal effort. Observers unable to differentiate between these two types of incidents would have difficulty drawing correct inference about the relative effort of different incident reporters.

[199] They may however rely on experts for such assessments.

making the proposed disclosures more easily retrievable and usable for aggregation, comparison, filtering, and other analysis.[200] As a point of comparison, XBRL requirements for public operating company financial statement disclosures have been observed to mitigate information asymmetry by reducing information processing costs, thereby making the disclosures easier to access and analyze.[201] This reduction in information processing cost has been observed to facilitate the monitoring of companies by external parties, and, as a result, to influence companies' behavior, including their disclosure choices.[202]

While these observations are specific to operating company financial statement disclosures, and not to disclosures from funds that are outside the financial statements, such as the proposed cybersecurity incident disclosures, they indicate that the proposed Inline XBRL requirements could directly or indirectly (*i.e.,* through information intermediaries such as financial media, data aggregators, and academic researchers), provide fund investors with increased insight into cybersecurity-related incidents at specific funds and across funds, fund managers, and time periods.[203] Also, in contrast to XBRL financial statements (including footnotes), which consist of tagged quantitative and narrative disclosures, the proposed incident disclosures would consist largely of tagged narrative disclosures.[204] Tagging narrative disclosures can facilitate analytical benefits such as automatic comparison/redlining of these disclosures against prior periods and the performance of targeted artificial intelligence/machine learning assessments (tonality, sentiment, risk words, etc.) of specific cybersecurity disclosures rather than the entire unstructured document.[205]

The markets for advisory services and funds present clients and investors with a complex, multi-dimensional, choice problem. In choosing an adviser or fund, clients and investors may consider investment strategy, ratings or commentaries, return histories, fee structures, risk exposures, reputations, etc. While we are 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, attention-grabbing information such as past performance and commissions when making such choices.[206] Moreover, to the extent that cybersecurity disclosures are ''boilerplate'' they may be less informative.[207] Conversely, cybersecurity incidents—especially those that involve loss of customer data or assets—are likely to garner attention. Thus, we expect that the proposed requirement to disclose significant cybersecurity incidents would have more of a direct effect on clients' and investors' choices. In addition, third parties such as rating services, journalists, or ''adviser advisers'' [208]—who may be more capable of extracting useful information out of the proposed disclosures—may incorporate it in assessments ultimately provided to clients and investors. Whether directly or indirectly, registrants with subpar cybersecurity policies and procedures—as revealed by ''excess'' cybersecurity incidents—could face pressure to improve said policies to reduce such excess incidents. Similarly, with respect to the proposed disclosures of cybersecurity incident handling procedures, funds and advisers that disclose having substandard procedures could face market pressure to improve the quality of their cybersecurity incident handling procedures.[209]

The proposed incident disclosure requirement should also benefit the current clients and investors of advisers and funds that experience a cybersecurity incident by providing notice that personal information, assets, or funds may have been compromised. Based on the notice, the clients and investors could take timely remedial actions such as auditing financial statements, blocking accounts that may have been compromised, or monitoring account activity.

b. Costs

Because reasonably designed cybersecurity policies and procedures would—in practice—require the collection of information that make up the proposed disclosures, we do not believe that the disclosure requirement

[200] The proposed Inline XBRL requirement would apply to cybersecurity risks and incidents disclosures in fund registration statements on Forms N–1A, N–2, N–3, N–4, N–6, N–8B–2, and S–6. *See supra* section II.C.4. Advisers would not be required to tag the proposed Form ADV disclosures in Inline XBRL. *See supra* section II.C.1.

[201] *See., e.g.,* Joung W. Kim, Jee-Hae Lim, and Won Gyun No, The Effect of First Wave Mandatory XBRL Reporting Across the Financial Information Environment, 26.1 *Journal of Information Systems* 127–153 (Spring 2012) (finding evidence that ''mandatory XBRL disclosure decreases information risk and information asymmetry in both general and uncertain information environments''); Yuyun Huang, Jerry T. Parwada, Yuan George Shan, and Joey Wenling Yang, Insider Profitability and Public Information: Evidence From the XBRL Mandate (Working Paper) (Sept. 17, 2019) (finding that XBRL levels the playing field between insiders and non-insiders, in line with the hypothesis that ''the adoption of XBRL enhances the processing of financial information by investors and hence reduces information asymmetry'').

[202] *See, e.g.,* Jeff Zeyun Chen, Hyun A. Hong, Jeong-Bon Kim, and Ji Woo Ryou, Information Processing Costs and Corporate Tax Avoidance: Evidence from the SEC's XBRL Mandate, 40 *Journal of Accounting and Public Policy* 2 (Mar.–Apr. 2021) (finding XBRL reporting decreases likelihood of firm tax avoidance because ''XBRL reporting reduces the cost of IRS monitoring in terms of information processing, which dampens managerial incentives to engage in tax avoidance behavior''); Paul A. Griffin, Hyun A. Hong, Jeong-Bon Kim, and Jee-Hae Lim, The SEC's XBRL Mandate and Credit Risk: Evidence on a Link between Credit Default Swap Pricing and XBRL Disclosure (finding XBRL reporting enables better outside monitoring of firms by creditors, leading to a reduction in firm default risk), 2014 American Accounting Association Annual Meeting (2014); Elizabeth Blankespoor, The Impact of Information Processing Costs on Firm Disclosure Choice: Evidence from the XBRL Mandate, 57 *Journal of Accounting Research* 4 (Sept. 2019) (finding ''firms increase their quantitative footnote disclosures upon implementation of XBRL detailed tagging requirements designed to reduce information users' processing costs,'' and ''both regulatory and non-regulatory market participants play a role in monitoring firm disclosures,'' suggesting that the ''processing costs of market participants can be significant enough to impact firms' disclosure decisions'').

[203] *See, e.g.,* Nina Trentmann, Companies Adjust Earnings for Covid–19 Costs, but Are They Still a One-Time Expense? The Wall Street Journal (Sept. 4, 2020) (citing an XBRL research software provider as a source for the analysis described in the article); *Bloomberg Lists BSE XBRL Data, XBRL.org* (Mar. 17, 2019); Rani Hoitash, and Udi Hoitash, Measuring Accounting Reporting Complexity with XBRL, 93 *The Accounting Review* 259–287 (2018).

[204] The proposed fund disclosure requirements do not expressly require the disclosure of any quantitative values in the discussion of cybersecurity incidents; if a fund includes any quantitative values as nested within the required discussion (*e.g.,* disclosing the number of days until containment), those values would be individually detail tagged, in addition to the block text tagging of the narrative disclosures.

[205] To illustrate, using the search term ''remediation'' to search through the text of all fund registration statements over a certain period of time, so as to analyze the trends in funds' disclosures related to cybersecurity incident remediation efforts during that period, could return many narrative disclosures outside of the cybersecurity incident discussion (*e.g.,* disclosures related to potential environmental liabilities in the risk factors section).

[206] *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 (6) *The Journal of Business* 2095–2120 (2005).

[207] However, the process of adopting ''boilerplate'' language by advisers and funds may itself affect improvements in policies and procedures.

[208] ''Adviser advisers'' are advisers who assist clients in selecting other advisers to manage some subset of the client's portfolio.

[209] Here we are assuming that clients, investors, or third parties evaluating advisers and funds would favor advisers and funds that include standard language relating to cybersecurity procedures in their disclosures. Further, we assume that registrants with ''superior'' procedures could adopt standard disclosures with no cost; conversely registrants with ''substandard'' procedures would need to affect improvements in their procedures to be able to furnish the standard disclosure.

itself would impose significant compliance costs beyond those already discussed.[210] However, these disclosures may impose costs due to market reactions, and due to the information they reveal to cybercriminals.

Funds and advisers that report many cybersecurity incidents and—to a lesser extent—those who report less well-developed cybersecurity incident handling procedures may bear costs arising from reactions in the marketplace: They may lose business or suffer harm to their reputations and brand values.[211] These costs would likely be borne not only by advisers and funds with inadequate cybersecurity policies, but also those who experience cybersecurity incidents despite having made reasonable efforts to prevent them. In addition, to the extent that clients and investors ''overreact'' [212] to disclosures of cybersecurity breaches, advisers and funds may pursue a strategy of ''overinvestment'' in cybersecurity precautions (to avoid such overreactions) resulting in reduced efficiency.

Mandating disclosure about cybersecurity incidents entails a tradeoff. While disclosure can inform clients and investors, disclosure can also inform cyber attackers that they have been detected. Also, disclosing too much (*e.g.,* the types of systems that were affected, how they were compromised) could be used by cybercriminals to better target their attacks, imposing costs on registrants. For example, announcing a cybersecurity incident naming a specific piece of malware and the degree of compromise can imply a trove of details about the structure of the victim's computer systems, the security measures employed (or not employed), and potentially suggest promising attack vectors for future attacks by other would-be attackers. Under the proposed amendments, registrants would be required to disclose cybersecurity incidents through filing of amendments to From ADV or registration statements in a timely manner.[213] In so doing, the registrants would need to identify the entity or entities affected, when the incidents were discovered and whether they are ongoing, whether any data was stolen, altered, or accessed or used for any other unauthorized purpose, the effect of the incident on the adviser's operations, and whether the adviser or service provider has remediated or is currently remediating the incident.[214] Thus, registrants would generally not be required to disclose technical details about incidents that could compromise their cybersecurity going forward. As before, the costs associated with conveying this information to attackers is impracticable to estimate.[215]

In addition, for one type of registrant—unit investment trusts—the requirement to tag the cybersecurity incident disclosures in Inline XBRL would create additional compliance costs. Unlike the other funds subject to the proposed cybersecurity incident disclosure requirements, unit investment trusts that register on Form N–8B–2 and file post-effective amendments on Form S–6 are not currently subject to Inline XBRL requirements.[216] As such, for these unit investment trusts, the proposed Inline XBRL requirement would entail compliance costs beyond the marginal administrative costs associated with tagging an additional section of a filing that is already partially tagged.[217] For example, these unit investment trusts could incur implementation costs associated with licensing Inline XBRL compliance software and training staff to use the software to tag the cybersecurity incident disclosures. To the extent a unit investment trust outsources its tagging to a third-party service provider, any costs that such a service provider would incur in developing the capability to tag unit investment trust filings could be passed on to the unit investment trust. Given the improvements in technology and the increased familiarity with XBRL tagging at advisers and service providers since fund XBRL requirements were first adopted in 2009, we expect these costs would be diminished relative to the compliance costs that funds incurred at the time of initial XBRL adoption.[218]

3. Regulatory Reporting of Cybersecurity Incidents

Under the proposed rules, advisers would be required to report significant cybersecurity incidents to the Commission within 48 hours.[219] The reporting requirement would extend to significant cybersecurity incidents at an adviser's ''covered client''—a client that is a registered investment company or business development company, or a private fund.[220] Cybersecurity incident reports would be submitted on proposed new Form ADV–C, and amended when information reported previously becomes materially inaccurate or if new material information is discovered.[221] Under the proposed rules, significant cybersecurity incidents are those that significantly affect the critical operations of an adviser or fund or lead to unauthorized access or use of information that results in substantial harm to the adviser or its clients or a fund or its investors.[222] Form ADV–C reports would be treated as confidential by the Commission.[223]

a. Benefits

Confidential, regulatory reporting of significant cybersecurity incidents would allow the Commission staff to assess trends, identify emerging risks in cybersecurity, and facilitate information sharing among advisers and funds. It would also allow the Commission to better coordinate a response to cybersecurity incidents which have the potential to cause broader disruptions to the financial markets, undermine financial stability, and contribute to systemic risk.

As discussed in section III.B, advisers and funds have incentives to not disclose information about cybersecurity incidents. Such incentives reduce the information available about cybersecurity threats and thereby inhibit the efficacy of collective (*i.e.,* an

[210] *See supra* section III.D.1. Administrative costs related to disclosure, including costs associated with legal reviews of such disclosures and costs attendant to tagging an additional section of a fund registration statement that is already subject to Inline XBRL requirements, are covered in the Paperwork Reduction Act analysis in section IV. *See also supra* footnote 86.

[211] We expect that clients and investors will be more likely to act in response to realized cybersecurity incidents than in response to advisers and funds descriptions of their policies and procedures.

[212] Such overreactions can be the result of overconfidence about the precision of the signal. *See, e.g.,* Kent Daniel, David Hirshleifer, and Avanidhar Subrahmanyam, Investor Psychology and Security Market Under- and Overreactions, 53 (6) *The Journal of Finance* 1839–85 (Dec. 1998).

[213] *See supra* section II.C.

[214] *Id.*

[215] As noted in the Broad Economic Considerations section (*supra* section III.B), 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.

[216] *See supra* footnote 83.

[217] Such administrative costs are covered in the Paperwork Reduction Act analysis in section IV.

[218] As a point of comparison, an AICPA survey of small reporting companies found a 45% decline in the average annual cost and a 69% decline in the median annual cost of fully outsourced XBRL tagging services from 2014 to 2017. *See* Michael Cohn, AICPA Sees 45% Drop in XBRL Costs for Small Companies, *Acct. Today,* (Aug. 15, 2018), *available at https://www.accountingtoday.com/news/aicpa-sees-45-drop-in-xbrl-costs-for-small-reporting-companies.*

[219] *See* proposed rule 204–6; *see also supra* section II.B.

[220] *Id.; see also* proposed rule 38a–2.

[221] *See* proposed rule 204–6; *see also supra* section II.B.

[222] *See* proposed rule 204–6(b); *see also* proposed rule 206(4)–9.

[223] *See supra* section II.B.

industry's or a society's) cybersecurity measures.[224] At the same time, complete transparency in this area likely runs the risk of facilitating future attacks.[225] As discussed in section III.C.1, 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.[226] The proposed reporting requirement, by channeling incident reports through the Commission, would create the opportunity for sharing of information valuable in preventing future cyberattacks, while preserving confidentiality and limiting the cybersecurity risks of public disclosure. For example, a series of reports detailing the compromise of a system commonly employed by small advisers could result in the Commission issuing a notice to similar advisers of the risks of the particular system. On the other hand, a general uptick in ''phishing'' style attacks using particular language and originating from similar addresses could lead the Commission to issue a risk alert to all registrants. Of course, in some cases, it may not be possible for the Commission to disclose any information discovered from a report without violating the confidentiality of the reporting entity or without exacerbating cybersecurity risks for some entities.[227] In such cases, the Commission may still be able to share information with relevant law enforcement or national security agencies.

In addition to facilitating information sharing, the proposed reporting requirements could also allow the Commission to coordinate market-wide responses to cybersecurity incidents. For example, an incident that affects the ability of an important money market fund could be used by the Commission to initiate an inter-agency response aimed at ensuring stability in the money markets.[228] Alternatively, patterns discovered through the reports may trigger referral to national security agencies for further investigation.

The aforementioned benefits arising from improved information sharing and response coordination are contingent on the Commission creating effective schemes to do so as well as the utility of the required reports in mounting effective regulatory responses. In particular, delays in registrants' discovery of cybersecurity incidents may hinder the utility of such reports in triggering a ''real-time'' regulatory response.[229] Thus the utility of such reports may be confined to information sharing and referrals to law enforcement and national security agencies.

b. Costs

The proposed requirements for advisers and funds to adopt and implement reasonably designed cybersecurity policies and procedures include provisions related to ongoing monitoring of threats and vulnerabilities[230] as well as provisions related to cybersecurity incident response and recovery.[231] Compliance with the aforementioned provisions effectively requires the collection of information that is solicited on proposed Form ADV–C.[232] Thus, we do not believe that the proposed reporting requirement would impose compliance costs beyond those related to developing and implementing reasonably designed policies and procedures discussed in section III.D.1. The proposed filing requirements would entail certain administrative costs, and these are discussed in the Paperwork Reduction Act analysis in section IV. Other costs that could arise from the reporting provisions would be the potential for the unintended release of information disclosed on Form ADV–C through the Commission's response to such disclosures. Unintended release of such details could facilitate future cyberattacks against funds and advisers as well as against advisers and fund with similar vulnerabilities.

4. Recordkeeping

Under the new recordkeeping requirements advisers and funds would be required to maintain, for five years records of: (1) Cybersecurity policies and procedures;[233] (2) annual reviews thereof; (3) documents related to the annual reviews; (4) regulatory filings[234] related to cybersecurity incidents required under the proposed amendments;[235] (5) any cybersecurity incident; and (6) cybersecurity risk assessments.

a. Benefits

These proposed amendments would help facilitate the Commission's inspection and enforcement capabilities. As a result, the Commission would be better able to detect deficiencies in the advisers' and funds' cybersecurity hygiene so that such deficiencies could be remedied. Insofar as correcting deficiencies results in material improvement in the cybersecurity practices of individual advisers and funds that would reduce the risk and/or magnitude of future cybersecurity incidents, the proposed amendments would benefit clients and investors.

b. Costs

We do not expect the proposed recordkeeping requirements to impose additional compliance costs not covered elsewhere in this analysis. The compliance costs related to the creation of records subject to the recordkeeping provisions are covered in section III.D.1. As advisers and funds are currently subject to substantially similar recordkeeping requirements applicable to other required policies and procedures, we do not expect registrants will need to invest in new recordkeeping staff, systems, or procedures to satisfy the new recordkeeping requirements.[236] The marginal administrative costs arising from maintaining additional records related to these provisions using existing systems are covered in the Paperwork Reduction Act analysis in section IV.

E. Effects on Efficiency, Competition, and Capital Formation

As discussed in the foregoing sections, market imperfections could lead to underinvestment in cybersecurity by advisers and funds, and information asymmetry could

[224] *See, e.g.,* Denise E. Zheng and James A. Lewis, Cyber Threat Information Sharing, Center for Strategic and International Studies (Mar. 2015), *available at https://www.csis.org/analysis/cyber-threat-information-sharing* (recommending that regulators encourage information sharing).

[225] 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* Ross, Ron, Victoria Pillitteri, Richard Graubart, Deborah Bodeau, and Rosalie McQuaid, Developing Cyber Resilient Systems: A Systems Security Engineering Approach, *National Institute of Standards and Technology* (Dec. 2021), *available at https://doi.org/10.6028/NIST.SP.800-160v2r1.* See also *supra* section III.D.2 (discussion of costs associated with disclosure).

[226] *See supra* section III.C.1 (discussion of information sharing).

[227] For example, sharing information about the type of attack can be used to draw inferences about the type of system that was targeted, which may imply a particular target entity (*i.e.,* the entity known to use that system).

[228] Depending on the circumstances, such responses could be coordinated through FSOC or through bilateral contacts with other regulators.

[229] Under the proposed rules registrants would have to report incidents within 48 hours. *See* proposed rule 204–6(a).

[230] *See supra* section II.A.1.d.

[231] *See supra* section II.A.1.e.

[232] *See* proposed rules 206(4)–9(a)(5) and 38a–2(a)(5).

[233] *See* proposed rules 204–2 and 38a–2(e).

[234] For advisers, copies of any Form ADV–C filed. For funds, reports provided to the Commission pursuant to proposed rule 38a–2(a)(5).

[235] *See* proposed rules 204–2 and 38a–2(e).

[236] *See* proposed rules 204–2(a)(17) and 38–2(e).

contribute to inefficient production of cybersecurity defenses. The proposed rules and amendments aim to mitigate the inefficiencies resulting from these imperfections by: (1) Imposing mandates on cybersecurity policies and procedures that could reduce cybersecurity underinvestment;[237] (2) providing additional disclosure to inform clients and investors about advisers' and funds' cybersecurity efforts, reducing information asymmetry;[238] and (3) creating a reporting framework that could improve information sharing and improved cybersecurity defense production.[239] While the proposed rules and amendments have the potential to mitigate inefficiencies resulting from market imperfections, the scale of the overall effect will depend on numerous factors, including: The state of existing of cybersecurity preparations,[240] the degree to which the proposed provisions induce increases to these preparations,[241] the effectiveness of additional preparations at reducing cybersecurity risks,[242] the degree to which clients and investors value additional cybersecurity preparations,[243] the degree of information asymmetry and bargaining power between clients and investors vis-à-vis advisers and funds,[244] the bargaining power of registrants vis-à-vis service providers,[245] service providers' willingness to provide bespoke contractual provisions to registrants,[246] the informativeness of the proposed disclosures, the scale of the negative externalities on the broader financial system,[247] the effectiveness of existing information sharing arrangements, and the informativeness of the required regulatory reports (as well as the Commission's ability to make use of them).[248] As discussed earlier in this section, it is not practicable to measure most of these factors. As such, it is also not practicable to quantify the overall effect of the proposed provisions on economic efficiency. Although any increased efficiency resulting from the proposed provisions can generally be expected to lead to improved capital formation,[249] quantifying such effects is similarly impracticable.[250]

Because the proposed rules and amendments are likely to have differential effects on registrants along a number of dimensions, their overall effect on competition among registrants is difficult to predict. For example, smaller registrants—who we believe are less likely to have extensive cybersecurity measures already in place—are likely to face disproportionately higher costs resulting from the proposed rules and amendments.[251] Thus, the proposed rules and amendments could tilt the competitive playing field in favor of larger registrants. On the other hand, if clients and investors believe that the proposed rules and amendments effectively induce the appropriate level of cybersecurity effort among registrants, smaller registrants would likely benefit most from these improved perceptions. Similar differential effects could apply to registrants and service providers that are more (or less) focused on their digital business.

With respect to competition among registrants' service providers, the overall effect of the proposed rules and amendments is similarly ambiguous. It is likely that requiring affected registrants to provide oversight of service providers' cybersecurity practices pursuant to a written contract would lead some service providers to cease offering services to affected registrants.[252] This would almost certainly ''reduce'' competition in a crude sense: The number of potential service providers available to registrants would likely be diminished. However, this may ''improve'' competition in another sense: Service providers with ''inadequate'' cybersecurity practices (*i.e.,* those unwilling to commit contractually to implementing cybersecurity practices deemed ''reasonably designed'' by the registrant) would be unable to undercut service providers with ''adequate'' cybersecurity practices.

F. Alternatives Considered

In formulating our proposal, we have considered various alternatives. Those alternatives are discussed below and we have also requested comments on certain of these alternatives.

1. Alternatives to the Proposed Policies and Procedures Requirement

a. Require Only Disclosure of Cybersecurity Policies and Procedures Without Prescribing Elements

Rather than requiring registrants to adopt cybersecurity policies and procedures with specific enumerated elements, the Commission considered requiring advisers and funds to only provide explanations or summaries of their cybersecurity practices to their clients or investors.

We believe that such an approach would create weaker incentives to address potential underspending in cybersecurity measures as it would rely entirely on clients' and investors' (or third parties' providing analysis to clients and investors)[253] ability to assess the effectiveness of registrants' cybersecurity practices from registrants' explanations. Given the cybersecurity risks of disclosing detailed explanations of cybersecurity practices,[254] it is likely that such explanations would include only vague boilerplate language and provide little information that could be used by observers to infer the degree of cybersecurity preparedness. Such a ''disclosure-only'' regime is unlikely to be effective at resolving the underlying information asymmetry and would therefore be unlikely to affect meaningful change in registrants' cybersecurity practices.[255] Moreover, not requiring specific enumerated elements in cybersecurity policies and procedures would likely result in less uniform cybersecurity preparedness across registrants, undermining clients'

[237] *See supra* footnotes 92–96 and accompanying text; section III.D.1.

[238] *See supra* footnotes 92–96 and accompanying text; section III.D.2.

[239] *See supra* footnotes 118–123 and accompanying text; section III.D.3.

[240] *See supra* section III.C.1. Here, we are concerned about the degree to which registrants' state of cybersecurity preparations diverge from socially optimal levels.

[241] *See supra* footnote 175 and accompanying text.

[242] Formally, the marginal product of the proposed policies and procedures in the production of cybersecurity defenses.

[243] Formally, clients' and investors' utility functions—specifically the marginal utilities of advisers' and funds' cybersecurity hygiene.

[244] In other words, the degree to which clients and investors can affect the policies of advisers and funds. Generally, we expect that fund investors will typically be small and dispersed and thus be subject to large information asymmetry and have limited ability to affect the policies of funds. For clients of advisers the situation is likely to involve more heterogeneity, with some clients wielding very little power over adviser policies (*e.g.,* small retail clients) while others wield considerable power (*e.g.,* large pension funds).

[245] *See supra* footnotes 184–192 and accompanying text.

[246] *Id.*

[247] *See supra* section III.B.

[248] *See supra* section III.D.3.a.

[249] The proposed provisions do not implicate channels typically associated with capital formation (*e.g.,* taxation policy, financial innovation, capital controls, investor disclosure, intellectual property, rule-of-law, and diversification). Thus, the proposed rule amendments are likely to have only indirect, second order effects on capital formation arising from any improvements to economic efficiency.

[250] *Id.* Qualitatively, these effects are expected to be small.

[251] *See supra* footnote 97 and accompanying text.

[252] *See supra* footnotes 184–192 and accompanying text.

[253] *See supra* footnote 208 and accompanying text.

[254] *See supra* section III.D.2.B (discussing tradeoffs of cybersecurity disclosure).

[255] Here changes in cybersecurity practices would depend entirely on market discipline exerted by relatively uninformed market participants.

and investors' broader confidence in the fund and adviser industries. At the same time, the costs associated with this alternative would likely be minimal, as registrants would be unlikely to face pressure to adjust practices as a result of such disclosures.

b. Require Cybersecurity Policies and Procedures With More Limited Prescribed Elements

We also considered paring down some enumerated elements from the proposed cybersecurity policies and procedures requirement, more specifically the oversight of service providers component of the information protection element. In this regard, we considered narrowing the scope of the types of service providers to named service providers discussed further above and requiring a periodic review and assessment of a named service provider's cybersecurity policies and procedures in lieu of a written contract. We further considered requiring service providers that receive, maintain, or process adviser or fund information 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 registrants, especially smaller registrants who rely on generic service providers and would have difficulty effecting changes in contractual terms with such service providers.[256] However, given that in the current technological context [257] cybersecurity risk exposure of registrants is unlikely to be limited to (or even concentrated in) certain named service providers, narrowing the scope of service providers would likely lead to lower costs only insofar as it reduces effectiveness of the regulation. In other words, absent a written contractual arrangement with a service provider relating to the provider's cybersecurity practices, it is unlikely that registrants could satisfy their overarching obligations under the proposed rules.

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 registrants.[258] However, we preliminarily believe that it would be difficult to prescribe a set of characteristics for such a ''standard'' certification that would sufficiently address the varied types of advisers and funds and their respective service providers.[259]

c. Require Specific Prescriptive Requirements for Addressing Cybersecurity Risks

The Commission considered including more prescriptive elements in the cybersecurity policies and procedures requirement of the current proposal. For example, advisers and funds could have been required to implement particular controls (*e.g.,* specific encryption protocols, network architecture, or authentication procedures) 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 registrants,[260] any specific requirements would result in some registrants needing to substantially alter their cybersecurity policies and procedures.

The potential benefit of such an approach would be to provide assurance that advisers and funds have implemented certain specific cybersecurity hygiene practices. But this approach would also entail considerably higher costs as many registrants would need to adjust their existing practices. Considering the variety of advisers and funds registered with the Commission, it would be exceedingly difficult for the Commission to devise specific requirements that are appropriately suited for all registrants: A uniform set of requirements would certainly be both over- and under-inclusive, while providing varied requirements based on the circumstances of the registrant would be complex and impractical. For example, uniform prescriptive requirements that ensure reasonably designed cybersecurity policies and procedures for the largest, most sophisticated advisers and funds would likely be overly burdensome for smaller, less sophisticated advisers with more limited cybersecurity exposures. Conversely, if these uniform prescriptive requirements were tailored to advisers and funds with more limited operations or cybersecurity risk, such requirements likely would be inadequate to address larger registrants' cybersecurity risks appropriately. Alternatively, providing different requirements for different categories of registrants would involve considerable regulatory complexity in delineating the classes of advisers and defining the appropriate requirements for each class. More broadly, imposing detailed prescriptive requirements would effectively place the Commission in the role of dictating details of the IT practices of registrants without the benefit of the registrants' knowledge of their own particular circumstances. Moreover, given the complex and constantly evolving cybersecurity landscape, detailed regulatory requirements for cybersecurity practices would likely limit registrants' ability to adapt quickly to changes in the cybersecurity landscape.[261]

d. Require Audits of Internal Controls Regarding Cybersecurity

Instead of requiring advisers and funds to adopt and implement cybersecurity policies and procedures, the Commission considered requiring advisers and funds to obtain audits of the effectiveness of their existing cybersecurity controls—for example, by obtaining service organization control audits with respect to their cybersecurity practices. This approach would not have required advisers and funds to adopt and implement cybersecurity policies and procedures as proposed, but instead would have required advisers and funds 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 adviser's or fund's cybersecurity practices. If the firms providing such certifications have sufficient reputational motives to issue credible assessment,[262] and if the scope of such certifications is not overly circumscribed,[263] it is likely that registrants' cybersecurity practices

[256] *See supra* section III.D.1.b (discussing service providers).

[257] Specifically, a context where businesses increasingly rely on third-party ''cloud services'' that effectively place business data out of the business' immediate control.

[258] Service providers may currently be providing certifications as part of an adviser's or fund's policies and procedures.

[259] *See supra* section III.C.3 (discussing the variety of affected registrants); *see also infra* section III.F.1.c (discussing limitation of uniform prescriptive requirements).

[260] *See supra* section III.C.3.

[261] If as in the previous example, the Commission were to require registrants 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.

[262] 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.

[263] We are assuming that in this alternative, certification would not be limited to only evaluating whether a registrant'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.

would end up being more robust under this alternative than under the current proposal. By providing certification of a registrant's cybersecurity practices, a firm would—in effect—be ''lending'' its reputation to the registrant. Because ''lenders'' are naturally most sensitive to down-side risks (here, loss of reputation, lawsuits, damages, regulatory enforcement actions), one would expect them to avoid ''lending'' to registrants with cybersecurity practices whose effectiveness is questionable.[264]

While certification by credible 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 down-side risk, firms would likely be hesitant to provide cybersecurity certifications without a thorough understanding of a registrant's systems and practices; in many cases, developing such an understanding would involve considerable effort.[265] In addition, it is possible that the inherent ambiguity of what represents ''effective'' practices in an evolving context like cybersecurity would lead to a reluctance among third parties to provide the necessary certification services.[266]

e. Vary Requirements of the Proposed Rules on Cybersecurity and Procedures for Different Subsets of Advisers and Funds

The Commission considered requiring different elements in an adviser's or fund's cybersecurity policies and procedures based on characteristics of the adviser or fund. For example, advisers or funds with assets under management below a certain threshold or with only a limited number of clients or investors could have been required to implement more limited cybersecurity policies and procedures.

This approach could have scaled based on adviser or fund size, business or other criteria, with larger firms, for example, being required to address more elements in their cybersecurity policies and procedures or being required to implement more prescriptive cybersecurity measures. However, as discussed above, cybersecurity risks and vulnerabilities are likely to be unique to each adviser and fund depending on its particular operations, which could make it difficult to use any specific characteristics such as firm size, for example, as an effective proxy to determine the scope of their cybersecurity policies and procedures.

f. Administration and Oversight of Cybersecurity Policies and Procedures

The Commission considered various alternative requirements with respect to administration and oversight of an adviser's or fund's cybersecurity policies and procedures such as requiring advisers and funds to designate a CISO or requiring funds' boards to oversee directly a fund's cybersecurity policies and procedures. There is a broad spectrum of potential approaches to this alternative, ranging from the largely nominal (*e.g.,* requiring registrants to designate someone to be a CISO) to the stringent (*e.g.,* requiring a highly qualified CISO to attest to the effectiveness of the registrant's policies).

While employee designations and similar nominal requirements may improve accountability and enhance compliance in certain contexts, they are unlikely to lead to material improvements in highly technical aspects of business operations. Given the technical complexity of cybersecurity issues, imposing such nominal requirements is unlikely to do much to further the policy objectives or provide substantial economic benefit. At the same time, while such an approach would increase regulatory complexity, it would likely entail minimal costs for registrants.

On the other hand, stringent requirements such as requiring an attestation from a highly qualified CISO as to the effectiveness of a registrant's cybersecurity practices in specific enumerated areas could be quite effective. Expert practitioners in cybersecurity are in high demand and command high salaries.[267] Thus, such an approach would impose substantial ongoing costs on registrants who do not already have appropriately qualified individuals on staff. This burden would be disproportionately borne by smaller registrants, for whom keeping a dedicated CISO on staff would be cost prohibitive. Allowing registrants 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.[268]

2. Modify Requirements for Structuring Disclosure of Cybersecurity Risks and Incidents

The Commission considered changing the scope of the tagging requirements for the proposed fund cybersecurity incident disclosures, such as by removing the requirements for all or a subset of funds. For example, the tagging requirements could have excluded unit investment trusts, which are not currently required to tag any filings in Inline XBRL.[269] Under such an alternative, unit investment trusts would submit their cybersecurity disclosures in unstructured HTML or ASCII, and forego the initial Inline XBRL implementation costs (such as the cost of training in-house staff to prepare filings in Inline XBRL, and the cost to license Inline XBRL filing preparation software from vendors) and ongoing Inline XBRL compliance burdens that would result from the proposed tagging requirement.[270] However, narrowing the scope of tagging requirements, whether based on fund structure, fund size, or other criteria, would diminish the

[264] Under the proposal it is the registrant itself that effectively ''certifies'' its own cybersecurity policies and procedures. Like the third-party auditor, the registrant faces down-side risks from ''certifying'' inadequate cybersecurity practices (*i.e.,* Commission enforcement actions). However, unlike the auditor, the registrant also realizes the potential up-side: Cost savings through reduced cybersecurity expenditures.

[265] It would be difficult for an auditor to provide a credible assessment of the effectiveness of the registrant's cybersecurity practices without first understanding the myriad of systems involved and how those practices are implemented. Presumably, a registrant would not bear these costs as it is likely to possess such an understanding.

[266] What constitutes ''effective'' practices with respect to cybersecurity is likely not as universally accepted as what constitutes ''adequate'' internal controls with respect to accounting or financial disclosure. Thus certifying a firm's cybersecurity practices would likely involve more litigation risk and uncertainty than traditional financial auditing.

[267] 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, *Heidrick & Struggles* (2020), *available at https://www.heidrick.com/-/media/heidrickcom/publications-and-reports/2020-north-american-chief-information-security-officer-ciso-compensation-survey.pdf.*

[268] 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 supra* section III.F.1.d (describing the audit regime alternative).

[269] By contrast, funds that file Forms N–1A, N–2, N–3, N–4, and N–6 are currently subject to Inline XBRL tagging requirements for portions of those filings. *See supra* footnote 85.

[270] *See infra* section III.D.3.b. Funds file registration statements and amendments using the Commission's EDGAR electronic filing system, which generally requires filers to use ASCII or HTML for their document submissions, subject to certain exceptions. *See* Regulation S–T, 17 CFR 232.101(a)(1)(iv); 17 CFR 232.301; EDGAR Filer Manual (Volume II) version 60 (Dec. 2021), at 5–1. To the extent unit investment trusts are part of the same fund family as other types of funds that are subject to Inline XBRL requirements, they may be able to leverage those other funds' existing Inline XBRL tagging experience and software, which would mitigate the initial Inline XBRL implementation costs that unit investment trusts would incur under the proposal.

extent of any informational benefits that would accrue as a result of the proposed disclosure requirements by making the excluded funds' cybersecurity incident disclosures comparatively costlier to process and analyze.

The scope of structuring requirements for the proposed disclosures could also have been expanded to cover advisers in addition to funds. Under the proposal, advisers would provide the required cybersecurity disclosures as part of their narrative brochures, which advisers must file electronically with the Commission as a text-searchable PDF file using the FINRA-administered IARD system.[271] Alternatively, the Commission could require advisers to structure the cybersecurity disclosures in IARD-specific XML. Such a requirement would not impose additional incremental compliance costs on advisers, who would use an online form provided by the IARD system to submit their disclosures and would not be required to develop technical expertise to comply with the structuring requirement.[272] However, such an alternative would result in investors receiving most of the narrative brochure disclosures in PDF format and the remaining cybersecurity disclosures—outside the PDF brochure—in IARD-specific XML, which could lead to investor confusion about the location of the disclosures.

3. Public Disclosure of Form ADV–C

The Commission considered requiring the public disclosure of Form ADV–C in the proposal. Assuming that the information submitted by registrants through Form ADV–C filings does not change, making Form ADV–C filings public would increase clients' and investors' information about cybersecurity incidents and thus improve their ability to draw inferences about an adviser's or fund's level of cybersecurity preparations. At the same time, doing so would also assist would-be attackers, who would gain additional insight into the vulnerabilities of a victim's systems. As discussed in section III.D.2.b, release of too much detail about a cybersecurity incident could further compromise cybersecurity of the victim, especially in the short term. Given these risks, requiring public disclosure of Form ADV–C filings would likely have the effect of significantly reducing the detail provided by registrants in these filings. As a result, the information set of clients, investors, 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 systemic risks to the financial system would be diminished.

IV. Paperwork Reduction Act Analysis

A. Introduction

Certain provisions of the proposed amendments contain ''collection of information'' requirements within the meaning of the Paperwork Reduction Act of 1995 (''PRA'').[273] We are submitting the proposed collections of information to the Office of Management and Budget (''OMB'') for review in accordance with the PRA.[274] The proposed rules 206(4)–9, 38a–2, 204–6, and proposed new Form ADV–C would include new information collection burdens, and the proposed amendments would have an effect on the current collection of information burdens of rule 204–2 and rule 204–3 under the Investment Advisers Act and Form ADV, as well as Form N–1A and other registration forms with respect to the Investment Company Act.

Certain funds have current requirements to submit to the Commission information included in their registration statements, or information included in or amended by any post-effective amendments to such registration statements, in response to certain form items in structured data language (''Investment Company Interactive Data'').[275] This also includes the requirement for funds to submit interactive data to the Commission for any form of prospectus filed pursuant to 17 CFR 230.497(c) or 17 CFR 230.497(e) under the Securities Act that includes information in response to certain form items. The proposed amendments to fund registration forms include new structured data requirements to tag information about significant fund cybersecurity incidents using Inline XBRL. Although the interactive data filing requirements are included in the instructions to each form, we are separately reflecting the hour and cost burdens for these requirements in the burden estimate for Investment Company Interactive Data and not in the estimate for each registration statement form.

The titles of new collections of information we are proposing are ''Rule 206(4)–9 under the Investment Advisers Act,'' ''Rule 38a–2 under the Investment Company Act,'' ''Rule 204–6 under the Investment Advisers Act,'' and ''Form ADV–C.'' OMB has not yet assigned control numbers for these titles. The titles for the existing collections of information are: (1) ''Rule 204–2 under the Investment Advisers Act of 1940'' (OMB control number 3235–0278); (2) Rule 204–3 under the Investment Advisers Act of 1940'' (OMB control number 3235–0047); (3) ''Form ADV'' (OMB control number 3235–0049); (4) ''Form N–1A, Registration Statement under the Securities Act and under the Investment Company Act for Open-End Management Investment Companies'' (OMB control number 3235–0307); (5) ''Form N–2, Registration Statement of Closed-End Management Investment Companies'' (OMB control number 3235–0026); (6) ''Form N–3, Registration of Separate Accounts Organized as Management Investment Companies'' (OMB control number 3235–0316); (7) ''Form N–4, Registration Statement of Separate Accounts Organized as Unit Investment Trust'' (OMB control number 3235–0318); (8) ''Form N–6, Registration Statement of Separate Accounts Organized as Unit Investment Trust'' (OMB control number 3235–0503); (9) ''Form N–8B–2, Registration Statement of Unit Investment Trusts Which Are Currently Issuing Securities'' (OMB control number 3235–0186); (10) ''Form S–6, for Registration under the Securities Act of Unit Investment Trusts registered on Form N–8B–2'' (OMB control number 3235–0184); and (11) ''Investment Company Interactive Data'' (OMB control number 3235–0642).

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.

Each requirement to disclose information, offer to provide information, or adopt policies and procedures constitutes a collection of information requirement under the PRA. These collections of information would help increase the likelihood that advisers and funds are prepared to respond to a cybersecurity incident, and collectively would serve the Commission's interest in protecting investors by reducing the risk that a cybersecurity incident could significantly affect a firm's operations and lead to significant harm to clients

[271] *See* 17 CFR 275.203(a)(1); General Instruction 5 of Form ADV Part 2. The proposed requirement is also more technically feasible than an Inline XBRL requirement for the advisers' disclosures, because the IARD system does not currently accommodate Inline XBRL filings.

[272] *See* FINRA Form ADV Guide, *available at https://www.iard.com/sites/iard/files/formADV_guide.pdf.*

[273] 44 U.S.C. 3501 through 3521.

[274] 44 U.S.C. 3507(d); 5 CFR 1320.11.

[275] The paperwork burdens for the rules under section 8(b) of the Investment Company Act are imposed through the forms and reports that are subject to the requirements in these rules and are reflected in the PRA burdens of those documents.

and investors. The Commission staff would also use the collection of information in its examination and oversight program in identifying patterns and trends across registrants. We discuss below the collection of information burdens associated with the proposed rules and rule amendments.

B. Rule 206(4)–9

Proposed rule 206(4)–9 would require an adviser to adopt and implement written policies and procedures that are reasonably designed to address cybersecurity risks.[276] These cybersecurity policies and procedures would need to be tailored based on the complexity of the adviser's business operations and attendant cybersecurity risks. The proposed rule would require policies and procedures that 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. The proposed rule includes certain minimum activities associated with each of these elements, including requirements for an adviser to identify and oversee any service providers that receive, maintain, or process adviser information, or are otherwise permitted to access its information systems and any information residing therein.

In addition to adopting and implementing such policies and procedures, the proposed rule would require advisers to review and assess, at least annually, the design and effectiveness of their cybersecurity policies and procedures. More specifically, proposed rule 206(4)–9 would require that an adviser at least annually: (1) Review and assess the design and effectiveness of the cybersecurity policies and procedures; and (2) prepare a written report that, at a minimum, describes the review, 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.[277]

The respondents to these collection of information requirements would be investment advisers that are registered or required to be registered with the Commission. As of October 31, 2021, there were 14,774 investment advisers registered with the Commission. As noted above, these requirements are mandatory, and all registered investment advisers would be subject to the requirements of the proposed rule. Responses provided to the Commission in the context of its examination and oversight program concerning proposed rule 206(4)–9 would be kept confidential subject to the provisions of applicable law. These collections of information would help increase the likelihood that advisers and funds are prepared to respond to a cybersecurity incident, and help protect investors from being significantly harmed by a cybersecurity incident. These collections would also help facilitate the Commission's inspection and enforcement capabilities. We have made certain estimates of the burdens associated with the proposed rule solely for the purpose of this PRA analysis. The table below summarizes the initial and ongoing annual burden and cost estimates associated with the proposed rule's policies and procedures and review and report requirements.

TABLE 1—RULE 206(4)–9 PRA ESTIMATES

	Internal initial burden hours	Internal annual burden hours [1]	Wage rate [2]	Internal time costs	Annual external cost burden
PROPOSED RULE 206(4)–9 ESTIMATES					
Adopting and implementing policies and procedures [3].	50	21.67 hours [4]	$396 (blended rate for compliance attorney and assistant general counsel).	$8,581.32	[5] $1,488
Annual review of policies and procedures and report of review.	0	10 hours [6]	$396 (blended rate for compliance attorney and assistant general counsel).	$3,960	[7] $1,984
Total new annual burden per adviser.		31.67 hours		$12,541.32	$3,472
Number of advisers		× 14,774		× 14,774	× 14,774
Total new annual aggregate burden.		320,152.58 hours		$185,285,462	$51,295,328

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 2020 ("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 25 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] We estimate 10 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 supra* note 5 (regarding wage rates with respect to external cost estimates).

[276] *See* proposed rule 206(4)–9; *supra* section II.A (discussing the cybersecurity policies and procedures requirements).

[277] *See* proposed rule 206(4)–9(b).

C. Rule 38a–2

Proposed rule 38a–2 would require a fund to adopt and implement written policies and procedures reasonably designed to address cybersecurity risks.[278] These cybersecurity policies and procedures would address: Risk assessment, user security and access, information protection, threat and vulnerability management, and incident response and recovery. The proposed rule includes certain minimum activities associated with each of these elements, including requirements for the fund to identify and oversee any service providers that receive, maintain, or process fund information, or are otherwise permitted to access its information systems and any information residing therein.

Under the rule, a fund would also, at least annually: (1) Review and assess the design and effectiveness of those policies and procedures; and (2) prepare and provide to the fund's board a written report.[279] The written report would also include an explanation of any control tests performed, any cybersecurity incident that occurred since the date of the last report, and any material changes to the policies and procedures since the date of the last report.

Finally, a fund would need to keep records related to the policies and procedures, written reports, annual review, and any reports provided to the Commission. Specifically, the fund would have to maintain copies for at least five years, the first two years in an easily accessible place, of: (1) Its cybersecurity policies and procedures; (2) copies of written reports provided to its board; (3) records documenting the fund's cybersecurity annual review; (4) any report of a significant fund cybersecurity incident provided to the Commission by its adviser that the proposed rule would require; (5) records documenting the occurrence of a cybersecurity incident, including records related to any response and recovery from such an incident; and (6) and records documenting a fund's cybersecurity risk assessments.[280]

Each requirement to disclose information, offer to provide information, or to adopt policies and procedures constitutes a collection of information requirement under the PRA. The respondents to proposed rule 38a–2 would be registered investment companies and BDCs.[281] We estimate that 14,749 funds would be subject to these proposed rule requirements.[282] The collections of information associated with these requirements would be mandatory, and responses provided to the Commission in the context of its examination and oversight program concerning proposed rule 38a–2 would be kept confidential subject to the provisions of applicable law. These collections of information would help increase the likelihood that funds are prepared to respond to a cybersecurity incident, and help protect investors from being significantly harmed by a cybersecurity incident. These collections would also help facilitate the Commission's inspection and enforcement capabilities. We have made certain estimates of the burdens associated with the proposed rule, as discussed below, solely for the purpose of this PRA analysis. The table below summarizes the initial and ongoing annual burden and cost estimates associated with the proposed rule.

TABLE 2—RULE 38A–2: PRA ESTIMATES

	Internal initial burden hours	Internal annual burden hours [1]	Wage rate [2]	Internal time costs	Annual external cost burden
PROPOSED RULE 38A–2 ESTIMATES					
Adopting and implementing policies and procedures.	60	25 hours [3]	$425 (blended rate for compliance attorney and assistant general counsel).	$10,625	[4] $5,952
Annual review of policies and procedures and report.	9	6 hours [5]	$425 (blended rate for compliance attorney and assistant general counsel).	$2,550	[6] $992
Recordkeeping	1	1 hour	$356 (blended rate for compliance attorney and senior programmer).	$356	$0
Total new annual burden per fund		32 hours		$13,531	$6,944
Number of funds		× 14,749 funds [7]		× 14,749 funds	[8] 7,375
Total new annual aggregate burden.		471,968 hours		$199,568,719	$51,212,000

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 the SIFMA Wage Report. The estimated figures are modified by firm size, employee benefits, overhead, and adjusted to account for the effects of inflation.

[3] Includes initial burden estimates annualized over a three-year period, plus 5 ongoing annual burden hours. The estimate of 25 hours is based on the following calculation: ((60 initial hours/3) + 5 additional ongoing burden hours) = 25 hours.

[4] This estimated burden is based on the estimated wage rate of $496/hour, for 12 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.

[5] Includes initial burden estimates annualized over a three-year period, plus 8 ongoing annual burden hours. The estimate of 6 hours is based on the following calculation: ((9 initial hours/3) + 3 additional ongoing burden hours) = 6 hours.

[6] This estimated burden is based on the estimated wage rate of $496/hour, for 2 hours, for outside legal services. *See supra* footnote 4 (regarding wage rates with respect to external cost estimates).

[7] Includes all registered investment companies, plus BDCs.

[278] *See* proposed rule 38a–2; *supra* section II.A (discussing the cybersecurity policies and procedures requirements).

[279] For unit investment trusts, the written report would be provided to the principal underwriter or depositor.

[280] For unit investment trusts, copies of materials provided the principal underwriter or depositor similarly would be required to be maintained for at least five years after the end of the fiscal year in which the documents were provided.

[281] *See* proposed rule 38a–2(f) (defining ''fund'').

[282] As of December 2020, we estimate 14,654 registered investment companies and 95 BDCs.

[8] We estimate that 50% of funds will use outside legal services for these collections of information. This estimate takes into account that funds may elect to use outside legal services (along with in-house counsel), based on factors such as fund budget and the fund's standard practices for using outside legal services, as well as personnel availability and expertise.

D. Rule 204–2

Under section 204 of the Advisers Act, investment advisers registered or required to register with the Commission under section 203 of the Advisers Act must make and keep for prescribed periods such records (as defined in section 3(a)(37) of the Exchange Act), furnish copies thereof, and make and disseminate such reports as the Commission, by rule, may prescribe as necessary or appropriate in the public interest or for the protection of investors. Rule 204–2 sets forth the requirements for maintaining and preserving specified books and records. This collection of information is found at 17 CFR 275.204–2 and is mandatory. The Commission staff uses the collection of information in its examination and oversight program. As noted above, responses provided to the Commission in the context of its examination and oversight program concerning the proposed amendments to rule 204–2 would be kept confidential subject to the provisions of applicable law.

As part of the proposed cybersecurity risk management rules, we are proposing corresponding amendments to rule 204–2, the books and records rule. The proposed amendments would require advisers to retain: (1) A copy of their cybersecurity policies and procedures formulated pursuant to proposed rule 206(4)–9 that is in effect, or at any time within the past five years was in effect; (2) a copy of the adviser's written report documenting the annual review of its cybersecurity policies and procedures pursuant to proposed rule 206(4)–9 in the last five years; (3) a copy of any Form ADV–C filed by the adviser under rule 204–6 in the last 5 years; (4) records documenting the occurrence of any cybersecurity incident, as defined in rule 206(4)–9(c), occurring in the last five years, including records related to any response and recovery from such an incident; and (5) records documenting any risk assessment conducted pursuant to the cybersecurity policies and procedures required by rule 206(4)–9(a)(1) in the last five years.[283] These proposed amendments would help facilitate the Commission's inspection and enforcement capabilities.

The respondents to this collection of information are investment advisers registered or required to be registered with the Commission. All such advisers will be subject to the proposed amendments to rule 204–2. As of October 31, 2021, there were 14,774 advisers that would be subject to these policies and procedures requirement. In our most recent Paperwork Reduction Act submission for rule 204–2, we estimated for rule 204–2 a total annual aggregate hour burden of 2,764,563 hours, and the total annual aggregate external cost burden is $175,980,426.[284] The table below summarizes the initial and ongoing annual burden estimates associated with the proposed amendments to rule 204–2.[285]

TABLE 3—RULE 204–2 PRA ESTIMATES

	Internal hour burden		Wage rate	Internal time costs	Annual external cost burden
PROPOSED ESTIMATES FOR RULE 204–2 AMENDMENTS					
Retention of cybersecurity policies and procedures.	1	×	$68 (blended rate for general clerk and compliance clerk).	$68	$0
Total burden per adviser				$68	0
Total number of affected advisers	× 14,774			× 14,774	0
Sub-total burden	14,774 hours			$1,004,632	0
Retention of written report documenting annual review.	1	×	$68 (blended rate for general clerk and compliance clerk).	$68	0
Total annual burden per adviser	1			$68	0
Total number of affected advisers	× 14,774			× 14,774	0
Sub-total burden	14,774 hours			$1,004,632	0
Retention of copy of any Form ADV–C filed in last 5 years.	1	×	$68 (blended rate for general clerk and compliance clerk).	$68	0
Total annual burden per adviser	1			$68	0
Total number of affected advisers	× 14,774			× 14,774	0
Sub-total burden	14,774 hours			$1,004,632	0
Retention of records documenting a cybersecurity incident.	1	×	$68 (blended rate for general clerk and compliance clerk).	$68	0
Total annual burden per adviser	1			$68	0
Total number of affected advisers	× 14,774			× 14,774	0
Sub-total burden	14,774 hours			$1,004,632	0

[283] *See* proposed rule 204–2(a)(17)(i) through (vii).

[284] Supporting Statement for the Paperwork Reduction Act Information Collection Submission for Revisions to Rule 204–2, OMB Report, OMB 3235–0278 (Aug. 2021).

[285] We estimate the hourly wage rate for compliance clerk is $70 and a general clerk is $62. The hourly wages used are from the SIFMA Wage Report.

TABLE 3—RULE 204–2 PRA ESTIMATES—Continued

	Internal hour burden		Wage rate	Internal time costs	Annual external cost burden
Retention of records documenting an adviser's cybersecurity risk assessment.	1	×	$68 (blended rate for general clerk and compliance clerk).	$68	0
Total annual burden per adviser	1	....		$68	0
Total number of affected advisers	× 14,774	....		× 14,774	0
Sub-total burden	14,774 hours	....		$1,004,632	0
Total annual aggregate burden of rule 204–2 amendments.	73,870 hours	....		$5,023,160	0
Current annual estimated aggregate burden of rule 204–2.	2,764,563 hours	....		$175,980,426	0
Total annual aggregate burden of rule 204–2.	2,838,433 hours	....		$181,003,586	0

E. Rule 204–6

Proposed rule 204–6 would require investment advisers to report on new Form ADV–C a significant adviser cybersecurity incident or a significant fund cybersecurity incident. The rule would define a significant adviser cybersecurity incident as a cybersecurity incident, or a group of related incidents, that significantly disrupts or degrades the adviser's ability, or the ability of a private fund client of the adviser, to maintain critical operations, or leads to the unauthorized access or use of adviser information, where the unauthorized access or use of such information results in: (1) Substantial harm to the adviser, or (2) substantial harm to a client, or an investor in a private fund, whose information was accessed.[286] Proposed rule 204–6 would also require advisers to amend promptly any previously filed Form ADV–C in the event information reported on the form becomes materially inaccurate; if new material information about a previously reported incident is discovered; and after resolving a previously reported incident or closing an internal investigation pertaining to pertaining to a previously disclosed incident.

The respondents to this collection of information are investment advisers registered or required to be registered with the Commission. As noted above, this requirement is mandatory, and all registered investment advisers will be subject to the requirements of the proposed rule. Responses provided to the Commission would be kept confidential subject to the provisions of applicable law. This collection of information would help the Commission's examination and oversight program efforts in identifying patterns and trends across registrants regarding such incidents. As of October 31, 2021, there were 14,774 registered advisers that would be subject to this reporting requirement. The table below summarizes the initial and ongoing annual burden and cost estimates associated with the proposed rule's reporting requirement.

TABLE 4—RULE 204–6 PRA ESTIMATES

	Internal initial burden hours	Internal annual burden hours		Wage rate	Internal time costs	Annual external cost burden
PROPOSED ESTIMATES						
Making a determination of significant cybersecurity incident.	3	3 hours [1]	×	$353 (blended rate for assistant general counsel, compliance manager and systems analyst).	$1,059	[2] $1,488
Amending Form ADV–C as required *(e.g.,* if any of the information previously filed on Form ADV–C becomes materially inaccurate).	1	1 hour	×	$396 (blended rate for assistant general counsel and compliance manager).	$396	[3] $496
Total new annual burden per adviser.		4 hours	....		$1,455	$1,984
Number of advisers		× 14,774	....		× 14,774	× 14,774
Total new aggregate annual burden.		59,096 hours	....		$21,496,170	$29,311,616

Notes:

[1] Includes initial burden estimates annualized over a three-year period, plus 2 ongoing annual burden hours. The estimate of 6 hours is based on the following calculation: ((3 initial hours/3) + 2 additional ongoing burden hours) = 3 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] This estimated burden is based on the estimated wage rate of $496/hour, for 1 hour, for outside legal services.

[286] *See* proposed rule 204–6(b).

F. Form ADV–C

The Commission is proposing a new Form ADV–C to require an adviser to provide information regarding a significant cybersecurity incident in a structured format through a series of check-the-box and fill-in-the-blank questions. Proposed Form ADV–C would require advisers to report certain information regarding a significant cybersecurity incident in order to allow the Commission and its staff to understand the nature and extent of the cybersecurity incident and the adviser's response to the incident. We believe that collecting information in a structured format would enhance the Commission's and its staff's ability to effectively carry out the risk-based examination program and other risk assessment and monitoring activities. The structured format would also assist the Commission and its staff in assessing trends in cybersecurity incidents across the industry.

The respondents to this collection of information are investment advisers registered or required to be registered with the Commission. As noted above, the collection of this information is mandatory for all registered advisers. Information filed on Form ADV–C would be kept confidential subject to the provisions of applicable law. As of October 31, 2021, there were 14,774 registered advisers that would be subject to this reporting requirement. The table below summarizes the initial and ongoing annual burden and cost estimates associated with filing proposed Form ADV–C.

TABLE 5—FORM ADV–C PRA ESTIMATES

	Internal initial burden hours	Internal annual burden hours		Wage rate	Internal time costs	Annual external cost burden
PROPOSED FORM ADV–C ESTIMATES						
Form ADV–C	3	1.5 hours [1]	×	$396 (blended rate for assistant general counsel and compliance manager).	$594	[2] $496
Total new annual burden per adviser.		1.5 hours				$496
Number of advisers		× 14,774			× 14,774	× 14,774
Total new aggregate annual burden.		22,161 hours			$8,775,756	$7,327,904

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.

G. Form ADV

Form ADV is the investment adviser registration form under the Advisers Act. Part 1 of Form ADV contains information used primarily by Commission staff, and Part 2A is the client brochure. Part 2B requires advisers to create brochure supplements containing information about certain supervised persons. Part 3: Form CRS (relationship summary) requires certain registered investment advisers to prepare and file a relationship summary for retail investors. We use the information on Form ADV to determine eligibility for registration with us and to manage our regulatory and examination programs. Clients and investors use certain of the information to determine whether to hire or retain an investment adviser, as well as what types of accounts and services are appropriate for their needs. The collection of information is necessary to provide advisory clients, prospective clients, other market participants and the Commission with information about the investment adviser and its business, conflicts of interest and personnel. Rule 203–1 under the Advisers Act requires every person applying for investment adviser registration with the Commission to file Form ADV. Rule 204–4 under the Advisers Act requires certain investment advisers exempt from registration with the Commission (''exempt reporting advisers'' or ''ERAs'') to file reports with the Commission by completing a limited number of items on Form ADV. Rule 204–1 under the Advisers Act requires each registered and exempt reporting adviser to file amendments to Form ADV at least annually, and requires advisers to submit electronic filings through IARD. The paperwork burdens associated with rules 203–1, 204–1, and 204–4 are included in the approved annual burden associated with Form ADV and thus do not entail separate collections of information. These collections of information are found at 17 CFR 275.203–1, 275.204–1, 275.204–4 and 279.1 (Form ADV itself) and are mandatory. Responses are not kept confidential.

We are proposing amendments to Form ADV to provide clients and prospective clients with information regarding an adviser's cybersecurity risks and significant cybersecurity incidents that have occurred in the past two years. Specifically, the proposed amendments would add a new Item 20 entitled ''Cybersecurity Risks and Incidents'' to Form ADV's narrative brochure, or Part 2A. The brochure, which is publicly available and the primary client-facing disclosure document, contains information about the investment adviser's business practices, fees, risks, conflicts of interest, and disciplinary events. We believe the narrative format of the brochure would allow advisers to present clear and meaningful cybersecurity disclosure to their clients and prospective clients. Advisers would be required to, in plain English, describe cybersecurity risks that could materially affect the advisory services they offer and describe how they assess, prioritize, and address cybersecurity risks created by the nature and scope of their business. The proposed amendments would also require advisers to describe any significant adviser cybersecurity incidents that have occurred within the last two years.

The collection of information is necessary to improve information available to us and to the general public about advisers' cybersecurity risks and

incidents. Our staff would use this information to help prepare for examinations of investment advisers. This information would be particularly useful for staff in reviewing an adviser's compliance with the proposed rulemakings and rule amendments. We are not proposing amendments to Parts 1 or 3 of Form ADV.

The respondents to current Form ADV are investment advisers registered with the Commission or applying for registration with the Commission and exempt reporting advisers.[287] Based on the IARD system data as of October 31, 2021, approximately 14,774 investment advisers were registered with the Commission, and 4,985 exempt reporting advisers file reports with the Commission. The amendments we are proposing would increase the information requested in Part 2A of Form ADV for registered investment advisers. Because exempt reporting advisers are not required to complete Form ADV Part 2A, they would not be subject to the proposed amendments to Form ADV Part 2A and would therefore not be subject to this collection of information.[288] However, these exempt reporting advisers are included in the PRA for purposes of updating the overall Form ADV information collection. In addition, the burdens associated with completing Part 3 are included in the PRA for purposes of updating the overall Form ADV information collection.[289] Based on the prior revision of Form ADV, we estimated the annual compliance burden to comply with the collection of information requirement of Form ADV is 433,004 burden hours and an external cost burden estimate of $14,125,083.[290] We propose the following changes to our PRA methodology for Form ADV:

• *Form ADV Parts 1 and 2.* Form ADV PRA has historically calculated a per adviser per year hourly burden for Form ADV Parts 1 and 2 for each of (1) the initial burden and (2) the ongoing burden, which reflects advisers' filings of annual and other-than-annual updating amendments. We noted in previous PRA amendments that most of the paperwork burden for Form ADV Parts 1 and 2 would be incurred in the initial submissions of Form ADV. However, recent PRA amendments have continued to apply the total initial hourly burden for Parts 1 and 2 to all currently registered or reporting RIAs and ERAs, respectively, in addition to the estimated number of new advisers expected to be registering or reporting with the Commission annually. We believe that the total initial hourly burden for Form ADV Parts 1 and 2 going forward should be applied only to the estimated number of expected new advisers annually. This is because currently registered or reporting advisers have generally already incurred the total initial burden for filing Form ADV for the first time. On the other hand, the estimated expected new advisers will incur the full total burden of initial filing of Form ADV, and we believe it is appropriate to apply this total initial burden to these advisers. We propose to continue to apply any new initial burdens resulting from proposed amendments to Form ADV Part 2, as applicable, to all currently registered or reporting investment advisers plus all estimated expected new RIAs and ERAs annually.

Table 6 below summarizes the burden estimates associated with the proposed amendments to Form ADV Part 2A. The proposed new burdens take into account changes in the numbers of advisers since the last approved PRA for Form ADV, and the increased wage rates due to inflation.

TABLE 6—FORM ADV PRA ESTIMATES

	Internal initial burden hours	Internal annual amendment burden hours [1]	Wage rate [2]	Internal time costs	Annual external cost burden [3]
PROPOSED AMENDMENTS TO FORM ADV					
RIAs (burden for Parts 1 and 2, not including private fund reporting) [4]					
Proposed addition (per adviser) to Part 2A (Item 20).	3 hours	0.2 hours	$279.50 per hour (blended rate for senior compliance examiner and compliance manager) [5].	3.2 hours × $279.50 = $894.4.	1 hour of external legal services ($496) for ¼ of advisers that prepare Part 2; 1 hour of external compliance consulting services ($739) for ½ of advisers that prepare Part 2.[6]
Current burden per adviser [7].	29.72 hours [8]	11.8 hours [9]	$273 per hour (blended rate for senior compliance examiner and compliance manager).	(29.72 + 11.8) × $273 = $11,334.96.	$2,069,250 aggregated (previously presented only in the aggregate) [10]
Revised burden per adviser.	29.72 hours + 3 hours = 32.72 hours.	0.2 hours + 11.8 hours = 12 hours.	$279.50 (blended rate for senior compliance examiner and compliance manager).	(32.72 + 12) × $279.5 = $12,499.24.	$4,689.50.[11]
Total revised aggregate burden estimate.	61,140.08 [12]	183,456 hours [13]	Same as above	(61,140.08 + 183,456) × $279.5 = $68,364,604.40.	$9,701,372.[14]

[287] An exempt reporting adviser is an investment adviser that relies on the exemption from investment adviser registration provided in either section 203(*l*) of the Advisers Act because it is an adviser solely to one or more venture capital funds or section 203(m) of the Advisers Act because it is an adviser solely to private funds and has assets under management in the United States of less than $150 million.

[288] An exempt reporting adviser is not a registered investment adviser and therefore would not be subject to the proposed amendments to Item 5 of Form ADV Part 1A. Exempt reporting advisers are required to complete a limited number of items in Part 1A of Form ADV (consisting of Items 1, 2.B., 3, 6, 7, 10, 11, and corresponding schedules), and are not required to complete Part 2.

[289] *See* Updated Supporting Statement for PRA Submission for Amendments to Form ADV under the Investment Advisers Act of 1940 (''Approved Form ADV PRA'').

[290] *See* Investment Adviser Marketing, Final Rule, Investment Advisers Act Release No. 5653 (Dec. 22, 2020) [81 FR 60418 (Mar. 5, 2021)] and corresponding submission to the Office of Information and Regulatory Affairs at *reginfo.gov* (''2021 Form ADV PRA'').

TABLE 6—FORM ADV PRA ESTIMATES—Continued

	Internal initial burden hours	Internal annual amendment burden hours [1]	Wage rate [2]	Internal time costs	Annual external cost burden [3]
RIAs (burden for Part 3) [15]					
No proposed changes	.....	.....	.....	.....	
Current burden per RIA	20 hours, amortized over three years = 6.67 hours [16].	1.58 hours [17]	$273 (blended rate for senior compliance examiner and compliance manager).	$273 × (6.67 + 1.71) = $2,287.74.	$2,433.74 per adviser.[18]
Total updated aggregate burden estimate.	66,149.59 hours [19]	14,573.92 hours [20]	Same as above	$22,562,221 (($279.50 × (66,149.59 hours + 14,573.92 hours)).	$8,157,555.[21]
ERAs (burden for Part 1A, not including private fund reporting) [22]					
No proposed changes					
Current burden per ERA	3.60 hours [23]	1.5 hours + final filings [24]	$273 (blended rate for senior compliance examiner and compliance manager).	Wage rate × total hours (see below).	$0
Total updated aggregate burden estimate.	1,245.6 [25]	8,033.6 hours [26]	Same as above	$2,593,536.40 ($279.5 × (1,245.6 + 8,033.6 hours)).	$0.
Private Fund Reporting [27]					
No proposed changes	.....	.....	.....	.....	
Current burden per adviser to private fund.	1 hour per private fund [28].	N/A–included in the existing annual amendment reporting burden for ERAs.	$273 (blended rate for senior compliance examiner and compliance manager).	.....	Cost of $46,865.74 per fund, applied to 6% of RIAs that report private funds.[29]
Total updated aggregate burden estimate.	1,150 hours [30]	N/A	Same as above	$3,978,123.5 ($279.5 × 14,233 hours)).	$15,090,768.30.[31]
TOTAL ESTIMATED BURDENS, INCLUDING AMENDMENTS					
Current per adviser burden/external cost per adviser.	23.82 hours [32]	.....	.....	23.82 hours × $273 = $6,502.86 per adviser cost of the burden hour.	$777.[33]
Revised per adviser burden/external cost per adviser.	16.28 hours [34]	.....	.....	16.28 hours × $279.5 = $4,550.26 per adviser cost of the burden hour.	$1,598.03.[35]
Current aggregate burden estimates.	433,004 initial and amendment hours annually [36]			433,004 × $273 = $118,210,092 aggregate cost of the burden hour.	$14,125,083.[37]
Revised aggregate burden estimates.	335,748.793 [38] Initial and amendment hours annually			290,831.73 × $279.5 = $81,287,468.54 aggregate cost of the burden hour.	$32,949,695.30.[39]

Notes:

[1] This column estimates the hourly burden attributable to annual and other-than-annual updating amendments to Form ADV, plus RIAs' ongoing obligations to deliver codes of ethics to clients.

[2] As with Form ADV generally, and pursuant to the currently approved PRA (*see* 2021 Form ADV PRA), we expect that for most RIAs and ERAs, the performance of these functions will most likely be equally allocated between a senior compliance examiner and a compliance manager, or persons performing similar functions. The Commission's estimates of the relevant wage rates are based on salary information for the securities industry compiled by the SIFMA Wage Report. The estimated figures are modified by firm size, employee benefits, overhead, and adjusted to account for the effects of inflation. For RIAs and ERAs that do not already have a senior compliance or a compliance manager, we expect that a person performing a similar function would have similar hourly costs. The estimated wage rates in connection with the proposed PRA estimates are adjusted for inflation from the wage rates used in the currently approved PRA analysis.

[3] External fees are in addition to the projected hour per adviser burden. Form ADV has a one-time initial cost for outside legal and compliance consulting fees in connection with the initial preparation of Parts 2 and 3 of the form. In addition to the estimated legal and compliance consulting fees, investment advisers of private funds incur one-time costs with respect to the requirement for investment advisers to report the fair value of private fund assets.

[4] Based on Form ADV data as of October 31, 2021, we estimate that there are 14,774 RIAs (''current RIAs'') and 514 advisers that are expected to become RIAs annually (''newly expected RIAs'').

[5] The $279.50 wage rate reflects current estimates from the SIFMA Wage Report of the blended hourly rate for a senior compliance examiner ($243) and a compliance manager ($316). ($243 + $316) /2 = $279.5.

[6] We estimate that a quarter of RIAs would seek the help of outside legal services and half would seek the help of compliance consulting services in connection with the proposed amendments to Form ADV Part 2. This is based on previous estimates and ratios we have used for advisers we expect to use external services for initially preparing various parts of Form ADV. *See* 2020 Form ADV PRA Renewal (the subsequent amendment to Form ADV described in the 2021 Form ADV PRA did not change that estimate). Because the SIFMA Wage Report does not include a specific rate for outside compliance consultant, we are proposing to use the rates in the SIFMA Wage Report for outside management consultant, as we have done in the past when estimating the rate of outside compliance counsel. We are adjusting these external costs for inflation, using the currently estimated costs for outside legal counsel and outside management consultants in the SIFMA Wage Report: $495 per hour for outside counsel, and $739 per hour for outside management consultant (compliance consultants).

[7] Per above, we are proposing to revise the PRA calculation methodology to apply the full initial burden only to expected RIAs, as we believe that current RIAs have generally already incurred the burden of initially preparing Form ADV.

[8] *See* 2020 Form ADV PRA Renewal (stating that the estimate average collection of information burden per adviser for Parts 1 and 2 is 29.22 hours, prior to the most recent amendment to Form ADV). *See also* 2021 Form ADV PRA (adding 0.5 hours to the estimated initial burden for Part 1A in connection with the most recent amendment to Form ADV). Therefore, the current estimated average initial collection of information hourly burden per adviser for Parts 1 and 2 is 29.72 hours (29.22 + 0.5 = 29.72).

[9] The currently approved average total annual burden for RIAs attributable to annual and other-than-annual updating amendments to Form ADV Parts 1 and 2 is 10.5 hours per RIA, plus 1.3 hours per year for each RIA to meet its obligation to deliver codes of ethics to clients (10.5 + 1.3 = 11.8 hours per adviser). *See* 2020 Form ADV PRA Renewal (these 2020 hourly estimates were not affected by the 2021 amendments to Form ADV). As we explained in previous PRAs, we estimate that each RIA filing Form ADV Part 1 will amend its form 2 times per year, which consists of one interim updating amendment (at an estimated 0.5 hours per amendment), and one annual updating amendment (at an estimated 8 hours per amendment), each year. We also explained that we estimate that each RIA will, on average, spend 1 hour per year making interim amendments to brochure supplements, and an additional 1 hour per year to prepare brochure supplements as required by Form ADV Part 2. *See id.*

[10] *See* 2020 Form ADV PRA Renewal (the subsequent amendment to Form ADV described in the 2021 Form ADV PRA did not affect that estimate).

[11] External cost per RIA includes the external cost for initially preparing Part 2, which we have previously estimated to be approximately 10 hours of outside legal counsel for a quarter of RIAs, and 8 hours of outside management consulting services for half of RIAs. *See* 2020 Form ADV Renewal (these estimates were not affected by subsequent amendments to Form ADV). We add to this burden the estimated external cost associated with the proposed amendment (an additional hour of each, bringing the total to 11 hours and 9 hours, respectively, for ¼ and ½ of RIAs, respectively). (((.25 × 14,774 RIAs) × ($496 × 11 hours)) + ((0.50 × 14,774 RIAs) × ($739 × 9 hours))) /14,774 RIAs = $4,689.50 per adviser.

[12] Per above, we are proposing to revise the PRA calculation methodology for current RIAs to not apply the full initial burden to current RIAs, as we believe that current RIAs have generally already incurred the initial burden of preparing Form ADV. Therefore, we calculate the initial burden associated with complying with the proposed amendment of 3 initial hours × 14,774 current RIAs = 44,322 initial hours in the first year aggregated for current RIAs. We are not amortizing this burden because we believe current advisers will incur it in the first year. For expected RIAs, we estimate that they will incur the full revised initial burden, which is 32.72 hours per RIA. Therefore, 32.72 hours × 514 expected RIAs = 16,818.08 aggregate hours for expected RIAs. We do not amortize this burden for expected new RIAs because we expect a similar number of new RIAs to incur this initial burden each year. Therefore, the total revised aggregate initial burden for current and expected RIAs is 44,322 hours + 16,818.08 hours = 61,140.08 aggregate initial hours.

[13] 12 amendment hours × (14,774 current RIAs + 514 expected new RIAs) = 183,456 aggregate amendment hours.

[14] Per above, for current RIAs, we are proposing to not apply the currently approved external cost for initially preparing Part 2, because we believe that current RIAs have already incurred that initial external cost. For current RIAs, therefore, we are applying only the external cost we estimate they will incur in complying with the proposed amendment. Therefore, the revised total burden for current RIAs is (((.25 × 14,774 RIAs) × ($496 × 1 hour)) + ((0.50 × 14,774 RIAs) × ($739 × 1 hour))) /14,774 RIAs = $7,290,969 aggregated for current RIAs, We do not amortize this cost for current RIAs because we expect current RIAs will incur this initial cost in the first year. For expected RIAs, we apply the currently approved external cost for initially preparing Part 2 plus the estimated external cost for complying with the proposed amendment. Therefore, $4,689.50 per expected RIA × 514 = $2,410,403 aggregated for expected RIAs. We do not amortize this cost for expected new RIAs because we expect a similar number of new RIAs to incur this external cost each year. $7,290,969 aggregated for current RIAs + $2,410,403 aggregated for expected RIAs = $9,701,372 aggregated external cost for RIAs.

[15] Even though we are not proposing amendments to Form ADV Part 3 (''Form CRS''), the burdens associated with completing Part 3 are included in the PRA for purposes of updating the overall Form ADV information collection. Based on Form ADV data as of October 31, 2021, we estimate that 8,877 current RIAs provide advice to retail investors and are therefore required to complete Form CRS, and we estimate an average of 347 expected new RIAs to be advising retail advisers and completing Form CRS for the first time annually.

[16] *See* Form CRS Relationship Summary; Amendments to Form ADV, Investment Advisers Act Release No. 5247 (Jun. 5, 2019) [84 FR 33492 (Sep. 10, 2019)] (''2019 Form ADV PRA''). Subsequent PRA amendments for Form ADV have not adjusted the burdens or costs associated with Form CRS. Because Form CRS is still a new requirement for all applicable RIAs, we have, and are continuing to, apply the total initial amendment burden to all current and expected new RIAs that are required to file Form CRS, and amortize that initial burden over three years for current RIAs.

[17] As reflected in the currently approved PRA burden estimate, we stated that we expect advisers required to prepare and file the relationship summary on Form ADV Part 3 will spend an average 1 hour per year making amendments to those relationship summaries and will likely amend the disclosure an average of 1.71 times per year, for approximately 1.58 hours per adviser. *See* 2019 Form ADV PRA (these estimates were not amended by the 2021 amendments to Form ADV).

[18] *See* 2020 Form ADV PRA Amendment (this cost was not affected by the subsequent amendment to Form ADV and was not updated in connection with that amendment; while this amendment did not break out a per adviser cost, we calculated this cost from the aggregate total and the number of advisers we estimated prepared Form CRS). Note, however, that in our 2020 Form ADV PRA Renewal, we applied the external cost only to expected new retail RIAs, whereas we had previously applied the external cost to current and expected retail RIAs. We believe that since Form CRS is still a newly adopted requirement, we should continue to apply the cost to both current and expected new retail RIAs. *See* 2019 Form ADV PRA.

[19] 8,877 current RIAs × 6.67 hours each for initially preparing Form CRS = 59,209.59 aggregate hours for current RIAs initially filing Form CRS. For expected new RIAs initially filing Form CRS each year, we are not proposing to use the amortized initial burden estimate, because we expect a similar number of new RIAs to incur the burden of initially preparing Form CRS each year. Therefore, 347 expected new RIAs × 20 initial hours for preparing Form CRS = 6,940 aggregate initial hours for expected RIAs. 59,209.59 hours + 6,940 hours = 66,149.59 aggregate hours for current and expected RIAs to initially prepare Form CRS.

[20] 1.58 hours × (8,877 current RIAs updating Form CRS + 347 expected new RIAs updating Form CRS) = 14,573.92 aggregate amendment hours per year for RIAs updating Form CRS.

[21] We have previously estimated the initial preparation of Form CRS would require 5 hours of external legal services for an estimated quarter of advisers that prepare Part 3, and; 5 hours of external compliance consulting services for an estimated half of advisers that prepare Part 3. *See* 2020 PRA Renewal (these estimates were not amended by the most recent amendment to Form ADV). The hourly cost estimate of $496 and $739 for outside legal services and management consulting services, respectively, are based on an inflation-adjusted figure in the SIFMA Wage Report. Therefore, (((.25 × 8,877 current RIAs preparing Form CRS) × ($496 × 5 hours)) + ((0.50 × 8,877 current RIAs preparing Form CRS) × ($739 × 5 hours))) = $21,903,997.50. For current RIAs, since this is still a new requirement, we amortize this cost over three years for a per year initial external aggregated cost of $7,301,332.50. For expected RIAs that we expect would prepare Form CRS each year, we use the following formula: (((.25 × 347 expected RIAs preparing Form CRS) × ($496 × 5 hours)) + ((0.50 × 347 expected RIAs preparing Form CRS) × ($739 × 5 hours))) = $856,222.50 aggregated cost for expected RIAs. We are not amortizing this initial cost because we estimate a similar number of new RIAs would incur this initial cost in preparing Form CRS each year, $7,301,332.50 + $856,222.50 = $8,157,555 aggregate external cost for current and expected RIAs to initially prepare Form CRS.

[22] Based on Form ADV data as of October 31, 2021, we estimate that there are 4,985 currently reporting ERAs (''current ERAs''), and an average of 346 expected new ERAs annually (''expected ERAs'').

[23] *See* 2021 Form ADV PRA.

[24] The previously approved average per adviser annual burden for ERAs attributable to annual and updating amendments to Form ADV is 1.5 hours. *See* 2021 Form ADV PRA. As we have done in the past, we add to this burden the burden for ERAs making final filings, which we have previously estimated to be 0.1 hour per applicable adviser, and we estimate that an expected 371 current ERAs will prepare final filings annually, based on Form ADV data as of December 2020.

[25] For current ERAs, we are proposing to not apply the currently approved burden for initially preparing Form ADV, because we believe that current ERAs have already incurred this burden. For expected ERAs, we are applying the initial burden of preparing Form ADV of 3.6 hours. Therefore, 3.6 hours × 346 expected new ERAs per year = 1,245.6 aggregate initial hours for expected ERAs. For these expected ERAs, we are not proposing to amortize this burden, because we expect a similar number of new ERAs to incur this burden each year. Therefore, we estimate 1,245.6 aggregate initial annual hours for expected ERAs.

[26] The previously approved average total annual burden of ERAs attributable to annual and updating amendments to Form ADV is 1.5 hours. *See* 2020 Form ADV Renewal (this estimate was not affected by the subsequent amendment to Form ADV). As we have done in the past, we added to this burden the currently approved burden for ERAs making final filings of 0.1 hour, and multiplied that by the number of final filings we are estimating ERAs would file per year (371 final filings based on Form ADV data as of December 2020). (1.5 hours × 4,985 currently reporting ERAs) + (0.1 hour × 371 final filings) = 7,514.6 updated aggregated hours for currently reporting ERAs. For expected ERAs, the aggregate burden is 1.5 hours for each ERA attributable to annual and other-than-annual updating amendments to Form ADV × 346 expected new ERAs = 519 annual aggregated hours for expected new ERAs updating Form ADV (other than for private fund reporting). The total aggregate amendment burden for ERAs (other than for private fund reporting) is 7,514.6 + 519 = 8,033.6 hours.

[27] Based on Form ADV data as of October 31, 2021, we estimate that 5,232 current RIAs advise 43,501 private funds, and expect an estimated 136 new RIAs will advise 407 reported private funds per year. We estimate that 4,959 current ERAs advise 23,476 private funds, and estimate an expected 372 new ERAs will advise 743 reported private funds per year. Therefore, we estimate that there are 66,977 currently reported private funds reported by current private fund advisers (43,501 + 23,476), and there will be annually 1,150 new private funds reported by expected private fund advisers (407 + 743). The total number of current and expected new RIAs that report or are expected to report private funds is 5,368 (5,232 current RIAs that report private funds + 136 expected RIAs that would report private funds).

[28] *See* 2020 Form ADV PRA Renewal (this per adviser burden was not affected by subsequent amendments to Form ADV).

[29] We previously estimated that an adviser without the internal capacity to value specific illiquid assets would obtain pricing or valuation services at an estimated cost of $37,625 each on an annual basis. *See* Rules Implementing Amendments to the Investment Advisers Act of 1940, Investment Advisers Act Release No. IA–3221 (Jun. 22, 2011) [76 FR 42950 (Jul. 19, 2011)]. However, because we estimated that external cost in 2011, we are proposing to use an inflation-adjusted cost of $46,865.74, based on the CPI calculator published by the Bureau of Labor Statistics at *https://www.bls.gov/data/inflation_calculator.htm.* As with previously approved PRA methodologies, we continue to estimate that 6% of RIAs have at least one private fund client that may not be audited. See 2020 Form ADV PRA Renewal.

[30] Per above, for currently reported private funds, we are proposing to not apply the currently approved burden for initially reporting private funds on Form ADV, because we believe that current private fund advisers have already incurred this burden. For the estimated 1,150 new private funds annually of expected private fund advisers, we calculate the initial burden of 1 hour per private fund. 1 hour per expected new private fund × 1,150 expected new private funds = 1,150 aggregate hours for expected new private funds. For these expected new private funds, we are not proposing to amortize this burden, because we expect new private fund advisers to incur this burden with respect to new private funds each year. Therefore, we estimate 1,150 aggregate initial hours for expected private fund advisers.

[31] As with previously approved PRA methodologies, we continue to estimate that 6% of registered advisers have at least one private fund client that may not be audited, therefore we estimate that the total number of audits for current and expected RIAs is 6% × 5,368 current and expected RIAs reporting private funds or expected to report private funds = 322.08 audits. We therefore estimate that approximately 322 registered advisers incur costs of $46,865.74 each on an annual basis (see note 29 describing the cost per audit), for an aggregate annual total cost of $15,090,768.30.

[32] 433,004 currently approved burden hours /18,179 advisers (current and expected annually) = 23.82 hours per adviser. *See* 2021 Form ADV PRA.

[33] $14,125,083 currently approved aggregate external cost /18,179 advisers (current and expected annually) = $777 blended average external cost per adviser.

[34] 335,748.79 aggregate annual hours for current and expected new advisers (see infra note [38]) /(14,774 current RIAs + 514 expected RIAs + 4,985 current ERAs + 346 expected ERAs) = 16.28 blended average hours per adviser.

[35] $32,949,695.30 aggregate external cost for current and expected new advisers (see infra note [39]) /(20,619 advisers current and expected annually) = $1,598.03 blended average hours per adviser.

[36] *See* 2021 Form ADV PRA.

[37] *See* 2021 Form ADV PRA.

[38] 61,140.08 hours + 183,456 hours + 66,149.59 hours + 14,573.92 hours + 1,245.6 + 8,033.6 hours + 1,150 hours = 335,748.79 aggregate annual hours for current and expected new advisers.

[39] $9,701,372 + $8,157,555 + $15,090,768.30 = $32,949,695.30.

H. Rule 204–3

Rule 204–3, the ''brochure rule,'' requires an investment adviser to deliver its brochure and brochure supplements to its new clients or prospective clients before or at the start of the advisory relationship and to deliver annually thereafter the full updated brochure or a summary of material changes to its brochure. The rule also requires that advisers deliver an amended brochure or brochure supplement (or just a statement describing the amendment) to clients only when disciplinary information in the brochure or supplement becomes materially inaccurate. The brochure assists the client in determining whether to retain, or continue employing, the adviser. Advisers registered with the Commission are required to prepare and electronically file firm brochures through the IARD.

Our proposed amendments to rule 204–3 would require an adviser to deliver interim brochure amendments promptly to existing clients if the adviser adds disclosure of a cybersecurity incident to its brochure or materially revises information already disclosed in its brochure about such an incident. We believe that requiring an adviser to deliver the brochure amendment promptly would enhance investor protection by enabling clients to take protective or remedial measures to the extent appropriate. It would also assist investors in determining whether their engagement of that particular adviser remains appropriate and consistent with their investment objectives.

The collection of information the brochure rule requires is necessary for several reasons. For example, it enables the client or prospective client to evaluate the adviser's background and qualifications, and to determine whether the adviser's services and practices are appropriate for that client. It also informs the client of the nature of the adviser's business, which may inform or limit the client's rights under the advisory contract. The information that rule 204–3 requires to be contained in the brochure is used by the Commission and staff in its enforcement, regulatory, and examination programs.

The respondents to this collection of information are investment advisers registered or required to be registered with the Commission. As noted above, the collection of this information is mandatory for all registered advisers. Responses are not kept confidential. As of October 31, 2021, there were 14,774 registered advisers that would be subject to this brochure requirement. The table below summarizes the initial and ongoing annual burden and cost estimates associated with the proposed rule's reporting requirement.

Table 7 below summarizes the initial and ongoing annual burden estimates associated with the proposed amendments to rule 204–3.

TABLE 7—RULE 204–3 PRA ESTIMATES

	Internal initial burden hours	Internal annual burden hours		Wage rate	Internal time costs	Annual external cost burden
PROPOSED ESTIMATES						
Annual delivery of brochure	[1] 1.66	1.66 hours	×	$64 (general clerk)	$106.24	$0
Interim delivery of updates to disciplinary action [2].	[3] 0.1	0.1 hour	×	$64 (general clerk)	$6.40	0
Interim delivery of updates to cybersecurity incidents.	[4] 0.1	0.1 hour	×	$64 (general clerk)	$6.40	0
Supplement tracking systems [5]	[6] 200	200 hours	×	$64 (general clerk)	$12,800	0
Total new annual burden per adviser		201.86 hours			$12,919.04	
Number of advisers		×14,774			×14,774	
Total new aggregate annual burden		2,982,279.64 hours.			$190,865,897	

Notes:

[1] We continue to estimate that, with a bulk mailing, an adviser will require no more than 0.02 hours to send the adviser's brochure or summary of material changes to each client, or an annual burden of 1.66 hours per adviser. (0.02 hours per client x 83 clients per adviser based on IARD data as of October 31, 2021) = approximately 1.66 hours per adviser. We note that the burden for preparing brochures is already incorporated into a separate burden estimate for Form ADV. We expect that most advisers will make their annual delivery as part of a mailing of an account statement or other periodic report they already make to clients; therefore, we estimate that the additional burden will be adding a few pages to the mailing.

[2] See approved rule 204–3 PRA.

[3] This is the previously approved burden estimate for interim delivery of updates to disciplinary action on Form ADV. We are not changing this estimate.

[4] This relates only to the amount of time it will take advisers to deliver interim updates to clients, as required by the proposed rule amendments. The burden for preparing interim updates is already incorporated into a separate burden estimate for Form ADV. This mailing may not be included with a mailing of a statement or other periodic report; therefore, we estimate that it will take slightly more time to deliver interim updates than to deliver the annual brochure or summary of material changes.

[5] We estimate that large advisers will need to design and implement systems to track changes in supervised persons providing investment advice to particular clients. We do not expect that such systems will be necessary for small advisers or medium advisers.

For purposes of the estimates in this section, we have categorized small advisers as those with 10 or fewer employees, medium-sized advisers as those with between 11 and 1,000 employees, and large advisers as those with over 1,000 employees. According to IARD data, only 1.70% of medium advisers report in response to Form ADV, Part 1A, Item 5.B.(1) that more than 250 employees perform investment advisory functions.

[6] See approved rule 204–3 PRA. This includes estimated time for large advisers to design and implement systems to track that the right supplements are delivered to the right clients as personnel providing investment advice to those clients change.

I. Form N–1A

The proposed amendments to Form N–1A would require a description of any significant cybersecurity incident that has occurred in a fund's last two fiscal years. The proposed disclosure amendments would require that a fund disclose to investors in its registration statement whether a significant fund cybersecurity incident has or is currently affecting the fund or its service providers.

Form N–1A generally imposes two types of reporting burdens on investment companies: (1) The burden of preparing and filing the initial registration statement; and (2) the burden of preparing and filing post-effective amendments to a previously effective registration statement. In our most recent Paperwork Reduction Act submission for Form N–1A, we estimated for Form N–1A a total aggregate annual hour burden of 1,672,077 hours, and a total annual aggregate annual external cost burden of $132,940,008.[291] Compliance with the disclosure requirements of Form N–1A is mandatory, and the responses to the disclosure requirements will not be kept confidential. These collections of information would help increase the likelihood that funds are prepared to respond to a cybersecurity incident, and would provide Commission staff with information in its examination and oversight program in identifying patterns and trends across registrants regarding such incidents. Based on filing data as of December 30, 2020, we estimate that 13,248 funds would be subject to these proposed amendments.

The table below summarizes our PRA initial and ongoing annual burden estimates associated with the proposed amendments to Form N–1A.

TABLE 8—FORM N–1A PRA ESTIMATES

	Internal initial burden hours	Internal annual burden hours [1]	Wage rate [2]	Internal time costs	Annual external cost burden
PROPOSED FORM N–1A ESTIMATES					
Cybersecurity incident disclosures [3].	21	15 hours [4]	$356 (blended rate for compliance attorney and senior programmer).	$5,340	[5] $992
Number of funds		× 13,248 funds [6]		× 13,248 funds	[7] × 6,624
Total new aggregate annual burden.		198,720 hours		$70,744,320	$6,571,008
TOTAL ESTIMATED BURDENS INCLUDING AMENDMENTS					
Current aggregate annual burden estimates.		+ 1,672,077 hours			+ $132,940,008
Revised aggregate annual burden estimates.		1,870,797 hours			$139,511,016

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 the SIFMA Wage Report. The estimated figures are modified by firm size, employee benefits, overhead, and adjusted to account for the effects of inflation.

[3] This estimate represents the average burden for a filer. Filers that experience one or several fund cybersecurity incidents are expected to incur higher burdens.

[4] Includes initial burden estimates annualized over a three-year period, plus 8 ongoing annual burden hours. The estimate of 15 hours is based on the following calculation: ((21 initial hours/3) + 8 additional ongoing burden hours) = 15 hours.

[5] This estimated burden is based on the estimated wage rate of $496/hour, for 2 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] Includes all open-end funds, including ETFs, registered on Form N–1A.

[7] We estimate that 50% of funds will use outside legal services for these collections of information. This estimate takes into account that funds may elect to use outside legal services (along with in-house counsel), based on factors such as fund budget and the fund's standard practices for using outside legal services, as well as personnel availability and expertise.

J. Form N–2

The proposed amendments to Form N–2 would require a description of any significant cybersecurity incident that has occurred in a fund's last two fiscal years. The proposed disclosure amendments would require that a fund disclose to investors in its registration statement whether a significant fund cybersecurity incident has or is currently affecting the fund, any subsidiary, or the fund's service providers.

Form N–2 generally imposes two types of reporting burdens on investment companies: (1) The burden of preparing and filing the initial

[291] On September 9, 2021, the Office of Management and Budget approved without change a revision of the currently approved information collection estimate for Form N–1A.

registration statement; and (2) the burden of preparing and filing post-effective amendments to a previously effective registration statement. In our most recent Paperwork Reduction Act submission for Form N–2, we estimated for Form N–2 a total aggregate annual hour burden of 94,350 hours, and a total aggregate annual external cost burden of $6,269,752.[292] Compliance with the disclosure requirements of Form N–2 is mandatory, and the responses to the disclosure requirements will not be kept confidential. These collections of information would help increase the likelihood that funds are prepared to respond to a cybersecurity incident, and would provide Commission staff with information in its examination and oversight program in identifying patterns and trends across registrants regarding such incidents. Based on filing data as of December 30, 2020, we estimate that 786 funds, including BDCs, would be subject to these proposed amendments.

The table below summarizes our PRA initial and ongoing annual burden estimates associated with the proposed amendments to Form N–2.

TABLE 9—FORM N–2 PRA ESTIMATES

	Internal initial burden hours	Internal annual burden hours [1]	Wage rate [2]	Internal time costs	Annual external cost burden
PROPOSED FORM N–2 ESTIMATES					
Cybersecurity incident disclosures [3].	21	15 hours [4]	$356 (blended rate for compliance attorney and senior programmer).	$5,340	$992 [5]
Number of funds		× 786 funds [6]		× 786 funds	× 393 [7]
Total new aggregate annual burden.		11,790 hours		$4,197,240	$389,856
TOTAL ESTIMATED BURDENS INCLUDING AMENDMENTS					
Current aggregate annual burden estimates.		+ 94,350 hours			+ $6,269,752
Revised aggregate annual burden estimates.		106,140 hours			$6,659,608

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 the SIFMA Wage Report. The estimated figures are modified by firm size, employee benefits, overhead, and adjusted to account for the effects of inflation.

[3] This estimate represents the average burden for a filer. Filers that experience one or several fund cybersecurity incidents are expected to incur higher burdens.

[4] Includes initial burden estimates annualized over a three-year period, plus 8 ongoing annual burden hours. The estimate of 15 hours is based on the following calculation: ((21 initial hours/3) + 8 additional ongoing burden hours) = 15 hours.

[5] This estimated burden is based on the estimated wage rate of $496/hour, for 2 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] Includes 691 registered closed-end funds and 95 BDCs.

[7] We estimate that 50% of funds will use outside legal services for these collections of information. This estimate takes into account that funds may elect to use outside legal services (along with in-house counsel), based on factors such as fund budget and the fund's standard practices for using outside legal services, as well as personnel availability and expertise.

K. Form N–3

The proposed amendments to Form N–3 would require a description of any significant cybersecurity incident that has occurred in a fund's last two fiscal years. The proposed disclosure amendments would require that a fund disclose to investors in its registration statement whether a significant fund cybersecurity incident has or is currently affecting the fund, insurance company, or the fund's service providers.

Form N–3 generally imposes two types of reporting burdens on investment companies: (1) The burden of preparing and filing the initial registration statement; and (2) the burden of preparing and filing post-effective amendments to a previously effective registration statement. In our most recent Paperwork Reduction Act submission for Form N–3, we estimated for Form N–3 a total aggregate annual hour burden of 2,836 hours, and a total aggregate annual external cost burden of $123,114.[293] Compliance with the disclosure requirements of Form N–3 is mandatory, and the responses to the disclosure requirements will not be kept confidential. These collections of information would help increase the likelihood that funds are prepared to respond to a cybersecurity incident, and would provide Commission staff with information in its examination and oversight program in identifying patterns and trends across registrants regarding such incidents. Based on filing data as of December 30, 2020, we estimate that 14 funds would be subject to these proposed amendments.

The table below summarizes our PRA initial and ongoing annual burden estimates associated with the proposed amendments to Form N–3.

[292] On September 17, 2020, the Office of Management and Budget approved without change a revision of the currently approved information collection estimate for Form N–2.

[293] On August 13, 2020, the Office of Management and Budget approved without change a revision of the currently approved information collection estimate for Form N–3.

TABLE 10—FORM N–3 PRA ESTIMATES

	Internal initial burden hours	Internal annual burden hours [1]	Wage rate [2]	Internal time costs	Annual external cost burden
PROPOSED FORM N–3 ESTIMATES					
Cybersecurity incident disclosures [3].	21	15 hours [4]	$356 (blended rate for compliance attorney and senior programmer).	$5,340	[5] $992
Number of funds		× 14 funds		× 14 funds	[6] × 7
Total new aggregate annual burden.		210 hours		$74,760	$6,944
TOTAL ESTIMATED BURDENS INCLUDING AMENDMENTS					
Current aggregate annual burden estimates.		+ 2,836 hours			+ $123,114
Revised aggregate annual burden estimates.		3,046 hours			$130,058

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 the SIFMA Wage Report. The estimated figures are modified by firm size, employee benefits, overhead, and adjusted to account for the effects of inflation.
[3] This estimate represents the average burden for a filer. Filers that experience one or several fund cybersecurity incidents are expected to incur higher burdens.
[4] Includes initial burden estimates annualized over a three-year period, plus 8 ongoing annual burden hours. The estimate of 15 hours is based on the following calculation: ((21 initial hours/3) + 8 additional ongoing burden hours) = 15 hours.
[5] This estimated burden is based on the estimated wage rate of $496/hour, for 2 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] We estimate that 50% of funds will use outside legal services for these collections of information. This estimate takes into account that funds may elect to use outside legal services (along with in-house counsel), based on factors such as fund budget and the fund's standard practices for using outside legal services, as well as personnel availability and expertise.

L. Form N–4

The proposed amendments to Form N–4 would require a description of any significant cybersecurity incident that has occurred in a fund's last two fiscal years. The proposed disclosure amendments would require that a fund disclose to investors in its registration statement whether a significant fund cybersecurity incident has or is currently affecting the fund, depositor, or the fund's service providers.

Form N–4 generally imposes two types of reporting burdens on investment companies: (1) The burden of preparing and filing the initial registration statement; and (2) the burden of preparing and filing post-effective amendments to a previously effective registration statement. In our most recent Paperwork Reduction Act submission for Form N–4, we estimated for Form N–4 a total aggregate annual hour burden of 292,487 hours, and a total aggregate annual external cost burden of $33,348,866.[294] Compliance with the disclosure requirements of Form N–4 is mandatory, and the responses to the disclosure requirements will not be kept confidential. These collections of information would help increase the likelihood that funds are prepared to respond to a cybersecurity incident, and would provide Commission staff with information in its examination and oversight program in identifying patterns and trends across registrants regarding such incidents. Based on filing data as of December 30, 2020, we estimate that 418 funds would be subject to these proposed amendments.

The table below summarizes our PRA initial and ongoing annual burden estimates associated with the proposed amendments to Form N–4.

TABLE 11—FORM N–4 PRA ESTIMATES

	Internal initial burden hours	Internal annual burden hours [1]	Wage rate [2]	Internal time costs	Annual external cost burden
PROPOSED FORM N–4 ESTIMATES					
Cybersecurity incident disclosures [3].	21	15 hours [4]	$356 (blended rate for compliance attorney and senior programmer).	$5,340	[5] $992
Number of funds		× 418 funds		× 418 funds	[6] × 209
Total new aggregate annual burden.		6,270 hours		$2,232,120	$207,328

[294] On October 26, 2021, the Office of Management and Budget approved without change a revision of the currently approved information collection estimate for Form N–4.

TABLE 11—FORM N–4 PRA ESTIMATES—Continued

	Internal initial burden hours	Internal annual burden hours [1]	Wage rate [2]	Internal time costs	Annual external cost burden
TOTAL ESTIMATED BURDENS INCLUDING AMENDMENTS					
Current aggregate annual burden estimates.	.....	+ 292,487 hours ...	.....	.....	+ $33,348,866
Revised aggregate annual burden estimates.	.....	198,757 hours	.....	.....	$33,556,194

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 the SIFMA Wage Report. The estimated figures are modified by firm size, employee benefits, overhead, and adjusted to account for the effects of inflation.
[3] This estimate represents the average burden for a filer. Filers that experience one or several fund cybersecurity incidents are expected to incur higher burdens.
[4] Includes initial burden estimates annualized over a three-year period, plus 8 ongoing annual burden hours. The estimate of 15 hours is based on the following calculation: ((21 initial hours/3) + 8 additional ongoing burden hours) = 15 hours.
[5] This estimated burden is based on the estimated wage rate of $496/hour, for 2 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] We estimate that 50% of funds will use outside legal services for these collections of information. This estimate takes into account that funds may elect to use outside legal services (along with in-house counsel), based on factors such as fund budget and the fund's standard practices for using outside legal services, as well as personnel availability and expertise.

M. Form N–6

The proposed amendments to Form N–6 would require a description of any significant cybersecurity incident that has occurred in a fund's last two fiscal years. The proposed disclosure amendments would require that a fund disclose to investors in its registration statement whether a significant fund cybersecurity incident has or is currently affecting the fund, depositor, or the fund's service providers.

Form N–6 generally imposes two types of reporting burdens on investment companies: (1) The burden of preparing and filing the initial registration statement; and (2) the burden of preparing and filing post-effective amendments to a previously effective registration statement. In our most recent Paperwork Reduction Act submission for Form N–6, we estimated for Form N–6 a total aggregate annual hour burden of 31,987 hours, and a total aggregate annual external cost burden of $3,816,692.[295] Compliance with the disclosure requirements of Form N–6 is mandatory, and the responses to the disclosure requirements will not be kept confidential. These collections of information would help increase the likelihood that funds are prepared to respond to a cybersecurity incident, and would provide Commission staff with information in its examination and oversight program in identifying patterns and trends across registrants regarding such incidents. Based on filing data as of December 30, 2020, we estimate that 236 funds would be subject to these proposed amendments.

The table below summarizes our PRA initial and ongoing annual burden estimates associated with the proposed amendments to Form N–6.

TABLE 12—FORM N–6 PRA ESTIMATES

	Internal initial burden hours	Internal annual burden hours [1]	Wage rate [2]	Internal time costs	Annual external cost burden
PROPOSED FORM N–6 ESTIMATES					
Cybersecurity incident disclosures [3].	21	15 hours [4]	$356 (blended rate for compliance attorney and senior programmer).	$5,340	[5] $992
Number of funds	.....	× 236 funds	.....	× 236 funds	[6] × 118
Total new aggregate annual burden.	.....	3,540 hours	.....	$1,260,240	$117,056
TOTAL ESTIMATED BURDENS INCLUDING AMENDMENTS					
Current aggregate annual burden estimates.	.....	+ 31,987 hours	.....	.....	+ $3,816,692
Revised aggregate annual burden estimates.	.....	35,527 hours	.....	.....	$3,933,748

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 the SIFMA Wage Report. The estimated figures are modified by firm size, employee benefits, overhead, and adjusted to account for the effects of inflation.
[3] This estimate represents the average burden for a filer. Filers that experience one or several fund cybersecurity incidents are expected to incur higher burdens.

[295] On October 26, 2021, the Office of Management and Budget approved without change a revision of the currently approved information collection estimate for Form N–6.

[4] Includes initial burden estimates annualized over a three-year period, plus 8 ongoing annual burden hours. The estimate of 15 hours is based on the following calculation: ((21 initial hours/3) + 8 additional ongoing burden hours) = 15 hours.

[5] This estimated burden is based on the estimated wage rate of $496/hour, for 2 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] We estimate that 50% of funds will use outside legal services for these collections of information. This estimate takes into account that funds may elect to use outside legal services (along with in-house counsel), based on factors such as fund budget and the fund's standard practices for using outside legal services, as well as personnel availability and expertise.

N. Form N–8B–2 and Form S–6

The proposed amendments to Form N–8B–2 would require a description of any significant cybersecurity incident that has occurred in a fund's last two fiscal years. The proposed disclosure amendments would require that a fund disclose to investors in its registration statement whether a significant fund cybersecurity incident has or is currently affecting the fund, depositor, or the fund's service providers. Form N–8B–2 is used by UITs to initially register under the Investment Company Act pursuant to section 8 thereof.[296] UITs are required to file Form S–6 in order to register offerings of securities with the Commission under the Securities Act.[297] As a result, UITs file Form N–8B–2 only once when the UIT is initially created and then use Form S–6 to file all post-effective amendments to their registration statements in order to update their prospectuses.[298]

In our most recent Paperwork Reduction Act submission for Form N–8B–2, we estimated for Form N–8B–2 a total aggregate annual hour burden of 28 hours, and total aggregate annual external cost burden of $10,300.[299] We currently estimate for Form S–6 a total aggregate annual hour burden of 107,359 hours, and an aggregate annual external cost burden estimate of $68,108,956.[300] Compliance with the disclosure requirements of Form N–8B–2 and Form S–6 is mandatory, and the responses to the disclosure requirements will not be kept confidential. These collections of information would help increase the likelihood that funds are prepared to respond to a cybersecurity incident, and would provide Commission staff with information in its examination and oversight program in identifying patterns and trends across registrants regarding such incidents. Based on filing data as of December 30, 2020, we estimate that one filing would be subject to the proposed amendments under Form N–8B–2 and 1,047 filings would be subject to the proposed amendments under Form S–6.[301]

The table below summarizes our PRA annual burden estimates associated with the proposed amendments to Form N–8B–2 and Form S–6.

TABLE 13—FORM N–8B–2 PRA ESTIMATES

	Internal annual burden hour [1]	Wage rate [2]	Internal time costs	Annual external cost burden
PROPOSED FORM N–8B–2 ESTIMATES				
Cybersecurity incident disclosures [3]	1 hour	$356 (blended rate for compliance attorney and senior programmer).	$356	[4] $992
Number of filings	× 1 filing		× 1 filing	[5] × 0.5
Total new aggregate annual burden	1 hour		$356	$496
TOTAL ESTIMATED BURDENS INCLUDING AMENDMENTS				
Current aggregate annual burden estimates	+ 28 hours			+ $10,300
Revised aggregate annual burden estimates	29 hours			$10,796

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 the SIFMA Wage Report. The estimated figures are modified by firm size, employee benefits, overhead, and adjusted to account for the effects of inflation.

[3] This estimate represents the average burden for a filer. Filers that experience one or several fund cybersecurity incidents are expected to incur higher burdens.

[4] This estimated burden is based on the estimated wage rate of $496/hour, for 2 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.

[5] We estimate that 50% of funds will use outside legal services for these collections of information. This estimate takes into account that funds may elect to use outside legal services (along with in-house counsel), based on factors such as fund budget and the fund's standard practices for using outside legal services, as well as personnel availability and expertise.

[296] *See* Form N–8B–2 [17 CFR 274.12].

[297] *See* Form S–6 [17 CFR 239.16]. Form S–6 is used for registration under the Securities Act of securities of any UIT registered under the Securities Act on Form N–8B–2.

[298] Form S–6 incorporates by reference the disclosure requirements of Form N–8B–2 and allows UITs to meet the filing and disclosure requirements of the Securities Act.

[299] On January 21, 2021, the Office of Management and Budget approved without change a revision of the currently approved information collection estimate for Form N–8B–2.

[300] On July 30, 2020, the Office of Management and Budget approved without change a revision of the currently approved information collection estimate for Form S–6.

[301] The number of unit investment trusts that report being registered under the Investment Company Act on Form N–8B–2 is 47; however, we believe using the number of filings instead of registrants would form a more accurate estimate of annual burdens. This estimate is based on the average number of filings made on Form N–8B–2 and Form S–6 from 2018 to 2020.

TABLE 14—FORM S–6 PRA ESTIMATES

	Internal initial burden hours	Internal annual burden hours [1]	Wage rate [2]	Internal time costs	Annual external cost burden
PROPOSED FORM S–6 ESTIMATES					
Cybersecurity incident disclosures [3].	21	15 hours [4]	$356 (blended rate for compliance attorney and senior programmer).	$5,340	[5] $992
Number of filings		× 1,047 filings		× 1,047 filings	× 524 [6]
Total new aggregate annual burden.		15,705 hours		$5,590,980	$519,312
TOTAL ESTIMATED BURDENS INCLUDING AMENDMENTS					
Current aggregate annual burden estimates.		+ 107,359 hours			+ $68,108,956
Revised aggregate annual burden estimates.		123,064 hours			$68,628,268

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 the SIFMA Wage Report. The estimated figures are modified by firm size, employee benefits, overhead, and adjusted to account for the effects of inflation.

[3] This estimate represents the average burden for a filer. Filers that experience one or several fund cybersecurity incidents are expected to incur higher burdens.

[4] Includes initial burden estimates annualized over a three-year period, plus 8 ongoing annual burden hours. The estimate of 15 hours is based on the following calculation: ((21 initial hours/3) + 8 additional ongoing burden hours) = 15 hours.

[5] This estimated burden is based on the estimated wage rate of $496/hour, for 2 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] We estimate that 50% of filers will use outside legal services for these collections of information. This estimate takes into account that funds may elect to use outside legal services (along with in-house counsel), based on factors such as fund budget and the fund's standard practices for using outside legal services, as well as personnel availability and expertise.

O. Investment Company Interactive Data

We are proposing to amend Form N–1A, Form N–2, Form N–3, Form N–4, Form N–6, Form N–8B–2, and Form S–6; rule 485 and rule 497 under the Securities Act; and rule 11 and rule 405 of Regulation S–T to require certain new structured data reporting requirements for funds.[302] Specifically, the proposed amendments would include new structured data requirements that would require funds to tag the information that the proposal would require funds to include in their registration statements about significant fund cybersecurity incidents using Inline XBRL.[303] The purpose of these information collections is to make information of significant fund cybersecurity incidents easier for investors to analyze and to help automate regulatory filings and business information processing, and to improve consistency between all types of funds with respect to the accessibility of cybersecurity information they provide to the market.

Funds filing registration statements on Form N–1A, Form N–2, Form N–3, Form N–4, and Form N–6 already submit certain information using Inline XBRL. Based on filing data as of December 30, 2020, we estimate that 14,702 funds filing registration statements on these forms would be subject to the proposed interactive data amendments. UITs filing initial registration statements on Form N–8B–2 and post-effective amendments on Form S–6 are not currently subject to requirements to submit information in structured form. Because these UITs have not previously been subject to Inline XBRL requirements, we assume that these funds would experience additional burdens related to one-time costs associated with becoming familiarized with Inline XBRL reporting. These costs would include, for example, the acquisition of new software or the services of consultants, and the training of staff. Based on filing data as of December 30, 2020, we estimate that 1,048 filings would be subject to these proposed amendments. In our most recent Paperwork Reduction Act submission for Investment Company Interactive Data, we estimated a total aggregate annual hour burden of 252,602 hours, and a total aggregate annual external cost burden of $15,350,750.[304] Compliance with the interactive data requirements is mandatory, and the responses will not be kept confidential.

The table below summarizes our PRA initial and ongoing annual burden estimates associated with the proposed amendments to Form N–1A, Form N–2, Form N–3, Form N–4, Form N–6, Form N–8B–2, and Form S–6, as well as Regulation S–T.

[302] The Investment Company Interactive Data collection of information do not impose any separate burden aside from that described in our discussion of the burden estimates for this collection of information.

[303] *See supra* section II.C.4; *see also* proposed rule 405(b)(2)–(3) of Regulation of S–T; proposed rule 485(c)(3); proposed rule 497(c) and 497(e); proposed General Instruction C.3.(g)(i) and (ii) of Form N–1A; proposed General Instruction I.2 and 3 of Form N–2; proposed General Instruction C.3(h)(i) and (ii) of Form N–3; proposed General Instruction C.3(h)(i) and (ii) of Form N–4; proposed General Instruction C.3(h)(i) and (ii) of Form N–6; proposed General Instruction 2.(*l*) of Form N–8B–2; and proposed General Instruction 5 of Form S–6.

[304] On November 9, 2020, the Office of Management and Budget approved without change a revision of the currently approved information collection estimate for Registered Investment Company Interactive Data.

TABLE 15—INVESTMENT COMPANY INTERACTIVE DATA PRA ESTIMATES

	Internal initial burden hours	Internal annual burden hours [1]	Wage rate [2]	Internal time costs	Annual external cost burden
PROPOSED INTERACTIVE DATA ESTIMATES					
Cybersecurity incident information for current XBRL filers [3].	1	1 hour [4]	$356 (blended rate for compliance attorney and senior programmer).	$356	$50 [5]
Number of funds		× 14,702 funds [6]		× 14,702 funds	× 14,702 funds
Cybersecurity incident information for new XBRL filers [7].	9	4 hours [8]	$356 (blended rate for compliance attorney and senior programmer).	$1,424	$900 [9]
Number of filings		× 1,048 filings [10]		× 1,048 filings	× 1,048 filings
Total new aggregate annual burden.		18,894 hours [11]		$6,726,264 [12]	$1,678,300 [13]
TOTAL ESTIMATED BURDENS INCLUDING AMENDMENTS					
Current aggregate annual burden estimates.		+ 252,602 hours			+ $15,350,750
Revised aggregate annual burden estimates.		271,496 hours			$17,029,050

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 the SIFMA Wage Report. The estimated figures are modified by firm size, employee benefits, overhead, and adjusted to account for the effects of inflation.

[3] This estimate represents the average burden for a filer on Form N–1A, Form N–2, Form N–3, Form N–4, and Form N–6 that is currently subject to interactive data requirements.

[4] Includes initial burden estimates annualized over a three-year period, plus 0.67 ongoing annual burden hours. The estimate of 1 hour is based on the following calculation: ((1 initial hour/3) + 0.67 additional ongoing burden hours) = 1 hour.

[5] We estimate an incremental external cost for filers on Form N–1A, Form N–2, Form N–3, Form N–4, and Form N–6 as they already submit certain information using Inline XBRL.

[6] Based on filing data as of December 30, 2020, we estimate 13,248 funds filing on Form N–1A; 786 funds, including BDCs, filing on Form N–2; 14 funds filing on Form N–3; 418 funds filing on Form N–4; and 236 funds on Form N–6, totaling 14,702 funds.

[7] This estimate represents the average burden for a filer on Form N–8B–2 and Form S–6 that is not currently subject to interactive data requirements.

[8] Includes initial burden estimates annualized over a three-year period, plus 1 ongoing annual burden hour. The estimate of 4 hours is based on the following calculation: ((9 initial hours/3) + 1 additional ongoing burden hour) = 4 hours.

[9] We estimate an external cost for filers on Form N–8B–2 and Form S–6 of $900 to reflect one-time compliance and initial set-up costs. Because these filers have not been previously been subject to Inline XBRL requirements, we estimate that these funds would experience additional burdens related to one time-costs associated with becoming familiar with Inline XBRL reporting. These costs would include, for example, the acquisition of new software or the services of consultants, or the training of staff.

[10] The number of unit investment trusts that report being registered under the Investment Company Act on Form N–8B–2 is 47; however, we believe using the number of filings instead of registrants would form a more accurate estimate of annual burdens. This estimate is therefore based on the average number of filings made on Form N–8B–2 and Form S–6 from 2018 to 2020.

[11] 18,894 hours = (14,702 funds × 1 hour) + (1,048 filings x 4 hours).

[12] $6,726,264 internal time cost = (14,702 funds × $356) + (1,048 filings × $1,424).

[13] $1,678,300 annual external cost = (14,702 funds × $50) + (1,048 filings × $900).

P. Request for Comment

We request comment on whether these estimates are reasonable. Pursuant to 44 U.S.C. 3506(c)(2)(B), the Commission solicits comments in order to: (1) Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the Commission, including whether the information will have practical utility; (2) evaluate the accuracy of the Commission's estimate of the burden of the proposed collection of information; (3) determine whether there are ways to enhance the quality, utility, and clarity of the information to be collected; and (4) determine whether there are 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.

Persons wishing to submit comments on the collection of information requirements of the proposed amendments should direct them to the OMB Desk Officer for the Securities and Exchange Commission, *MBX.OMB.OIRA.SEC_desk_officer@omb.eop.gov,* and should send a copy to Vanessa A. Countryman, Secretary, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549–1090, with reference to File No. S7–04–22. OMB is required to make a decision concerning the collections of information between 30 and 60 days after publication of this release; therefore a comment to OMB is best assured of having its full effect if OMB receives it within 30 days after publication of this release. Requests for materials submitted to OMB by the Commission with regard to these collections of information should be in writing, refer to File No. S7–04–22, and be submitted to the Securities and Exchange Commission, Office of FOIA Services, 100 F Street NE, Washington, DC 20549–2736.

V. Initial Regulatory Flexibility Act Analysis

The Commission has prepared the following Initial Regulatory Flexibility Analysis (''IRFA'') in accordance with section 3(a) of the Regulatory Flexibility Act (''RFA'').[305] It relates to: (1) Proposed rule 206(4)–9 under the Advisers Act; (2) proposed rule 38a-2 under the Investment Company Act; (3) proposed rule 204–6 under the Advisers

[305] 5 U.S.C. 603(a).

Act; (4) proposed amendments to rule 204–3 under the Investment Advisers Act; (5) proposed amendments to rule 204–2 under the Advisers Act; (6) proposed Form ADV–C; (7) proposed amendments to Form ADV Part 2A; and (8) proposed amendments to Form N–1A, Form N–2, Form N–3, Form N–4, Form N–6, Form N–8B–2, and Form S–6 (''fund registration forms'') as well as proposed conforming amendments to rule 485 and rule 497 under the Securities Act and rule 11 and rule 405 of Regulation S–T.

A. Reason for and Objectives of the Proposed Action

The reasons for, and objectives of, the proposed rules are discussed in more detail in sections I and II, above. The burdens of these requirements on small advisers and funds are discussed below as well as above in sections III and IV, which discuss the burdens on all advisers and funds. Sections II through IV also discuss the professional skills that we believe compliance with the proposed rules form amendments would require.

We are proposing rule 206(4)–9 under the Advisers Act and rule 38a–2 under the Investment Company Act to require all advisers and funds registered with the Commission to adopt and implement cybersecurity policies and procedures. Advisers and funds are increasingly relying on technology systems and networks and face increasing cybersecurity risks. These proposed rules would therefore require all advisers and funds to consider and mitigate cybersecurity risk to enhance investor protection.[306]

We are also proposing rules and amendments, discussed below, regarding recordkeeping, reporting, and disclosure.[307] We are proposing amendments to recordkeeping requirements under rule 204–2 to: (1) Conform the books and records rule to the proposed cybersecurity risk management rules; (2) help ensure that an investment adviser retains records of all of its documents related to its cybersecurity risk management; and (3) facilitate the Commission's inspection and enforcement capabilities.

We are proposing a new reporting requirement for advisers under proposed rule 204–6 using proposed Form ADV–C. We believe this requirement to provide prompt notice of significant cybersecurity incidents would help the Commission and its staff in its efforts to protect investors in connection with cybersecurity incidents by describing the nature and extent of a particular cybersecurity incident and the firm's response to the incident. The structured format of Form ADV–C would enhance the staff's ability to carry out our risk-based examination program and other risk assessment and monitoring activities effectively, including assessing trends in cybersecurity incidents across the industry.

Finally, we are proposing disclosure amendments for advisers and funds as well as related amendments to the brochure delivery rule, rule 204–3, for advisers. These proposed amendments are designed to enhance investor protection by ensuring cybersecurity risk or incident-related information is available to increase understanding and insight into an adviser's or fund's cybersecurity history and risks. For example, given the potential effect that significant cybersecurity incidents could have on an adviser's clients, we believe that requiring an adviser to deliver the brochure amendment under the proposed amendments to rule 204–3 promptly would enhance investor protection by enabling clients to take protective or remedial measures to the extent appropriate.

We believe that the proposed amendments discussed above would, together, improve the ability of clients and prospective clients to evaluate and understand relevant cybersecurity risks and incidents that advisers, funds and their personnel face and their potential effect on the advisers' and fund's services and operations.

1. Proposed Rule 206(4)–9

Proposed rule 206(4)–9 would require policies and procedures that address: (1) Risk assessment; (2) user security and access; (3) information protection; (4) threat and vulnerability management; and (5) cybersecurity incident response and recovery. The proposed rule would also require an annual review of these cybersecurity policies and procedures, in which an adviser: (1) Reviews and assesses the design and effectiveness of the cybersecurity policies and procedures; and (2) prepares a written report that, at a minimum, describes the review, 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. Proposed rule 206(4)–9 would allow firms to tailor their cybersecurity policies and procedures to fit the nature and scope of their business and address their individual cybersecurity risks.

2. Proposed Rule 38a–2

The policies and procedures proposed under rule 38a–2 under the Investment Company Act would address: (1) Risk assessment; (2) user security and access; (3) information protection; (4) threat and vulnerability management; and (5) cybersecurity incident response and recovery. The fund's cybersecurity policies and procedures would be reviewed and assessed at least annually. In addition, proposed rule 38a–2 would require that a fund maintain a copy of its cybersecurity policies and procedures that are in effect, or at any time in the last five years were in effect, in an easily accessible place. The fund would also have to maintain copies for at least five years, the first two years in an easily accessible place, of: (1) Copies of written reports provided to its board; (2) records documenting the fund's cybersecurity review; (3) any report of a significant fund cybersecurity incident provided to the Commission by its adviser that the proposed rule would require; (4) records documenting the occurrence of any cybersecurity incident, including records related to any response and recovery from such an incident; and (5) records documenting a fund's cybersecurity risk assessment.

3. Proposed Amendments to Rule 204–2

We are proposing related amendments to rule 204–2, the books and records rule, under the Advisers Act, which sets forth requirements for maintaining, making, and retaining advertisements. We are proposing to amend the current rule to require advisers to retain (1) a copy of their cybersecurity policies and procedures formulated pursuant to proposed rule 206(4)–9 that are in effect, or at any time within the past five years were in effect; (2) a copy of the adviser's written report documenting the annual review of its cybersecurity policies and procedures pursuant to proposed rule 206(4)–9; (3) a copy of any Form ADV–C filed by the adviser under rule 204–6 in the last five years; (4) records documenting the occurrence of any cybersecurity incident, as defined in rule 206(4)–9(c), occurring in the last five years, including records related to any response and recovery from such an incident; and (5) records documenting any risk assessment conducted pursuant to the cybersecurity policies and

[306] *See* proposed rule 206(4)–9 and proposed rule 38a–2; *supra* section II.A (discussing the cybersecurity policies and procedures requirements).

[307] *See* proposed rule 204–2 (recordkeeping); proposed rule 204–6, and amendments to rule 204–3 and Form ADV (reporting); and amendments to Forms N–1A, N–2, N–3, N–4, N–6, N–8B–2, and S–6 (disclosure).

procedures required by rule 206(4)–9(a)(1) in the last five years.[308]

4. Proposed Rule 204–6

We are proposing a new reporting requirement under proposed rule 204–6. Under the proposed rule, any adviser registered or required to be registered with the Commission as an investment adviser would be required to submit proposed Form ADV–C promptly, but in no event more than 48 hours, after having a reasonable basis to conclude that a significant adviser cybersecurity incident or a significant fund cybersecurity incident had occurred or is occurring.[309] The proposed rule would also require advisers to amend any previously filed Form ADV–C promptly, but in no event more than 48 hours after, information reported on the form becomes materially inaccurate; if new material information about a previously reported incident is discovered; and after resolving a previously reported incident or closing an internal investigation pertaining to a previously disclosed incident.[310]

5. Form ADV–C

As discussed above, we are proposing a new reporting requirement under proposed rule 204–6 using proposed Form ADV–C. This new Form ADV–C would require an adviser to provide information regarding a significant cybersecurity incident in a structured format through a series of check-the-box and fill-in-the-blank questions. Proposed Form ADV–C would require advisers to report certain information regarding a significant cybersecurity incident in order to allow the Commission and its staff to understand the nature and extent of the cybersecurity incident and the adviser's response to the incident.

6. Proposed Amendments to Form ADV Part 2A

We are proposing amendments to Form ADV that are designed to provide clients and prospective clients with information regarding cybersecurity risks and incidents that could materially affect the advisory relationship. The proposed amendments would add a new Item 20 entitled ''Cybersecurity Risks and Incidents'' to Form ADV's narrative brochure, or Part 2A. The brochure, which is publicly available and the primary client-facing disclosure document, contains information about the investment adviser's business practices, fees, risks, conflicts of interest, and disciplinary information. Advisers would be required to, in plain English, describe cybersecurity risks that could materially affect the advisory services they offer and describe how they assess, prioritize, and address cybersecurity risks created by the nature and scope of their business.

The proposed amendments would also require advisers to describe any cybersecurity incidents that have occurred within the last two years that have significantly disrupted or degraded the adviser's ability to maintain critical operations, or has led to the unauthorized access or use of adviser information, resulting in substantial harm to the adviser or its clients. The description of each incident, to the extent known, must include the following information: The entity or entities affected, when the incident was discovered and whether it is ongoing, whether any data was stolen, altered, or accessed or used for any other unauthorized purpose, the effect of the incident on the adviser's operations, and whether the adviser or a service provider has remediated or is currently remediating the incident.

7. Proposed Amendments to Rule 204–3

Currently, rule 204–3(b) does not require advisers to deliver interim brochure amendments to existing clients unless the amendment includes certain disciplinary information in response to Item 9 Part 2A. We are proposing amendments to rule 204–3 that would require an adviser to deliver interim brochure amendments to existing clients promptly if the adviser adds disclosure of a cybersecurity incident to its brochure or materially revises information already disclosed in its brochure about such an incident.[311]

8. Proposed Amendments to Fund Registration Forms, Rules Under the Securities Act, and Regulation S–T

The Commission also is proposing disclosure requirements on funds' registration statements to enhance investor protection by requiring that cybersecurity incident-related information is available to increase understanding in these areas and help ensure that investors and clients are making informed investment decisions. Our proposal would require a fund to provide prospective and current investors with disclosure about significant fund cybersecurity incidents on Forms N–1A, N–2, N–3, N–4, N–6, N–8B–2, and S–6. Our proposal, including the proposed amendments to the fund registration forms and conforming amendments to rule 485 and rule 497 under the Securities Act, and rule 11 and rule 405 of Regulation S–T, would also require a fund to tag information about significant fund cybersecurity incidents using Inline XBRL.

B. Legal Basis

The Commission is proposing rule 206(4)–9, rule 204–6, and Form ADV–C under the Advisers Act under the authority set forth in sections 203(d), 206(4), and 211(a) of the Advisers Act of 1940 [15 U.S.C. 80b–3(d), 10b–6(4) and 80b–11(a)]. The Commission is proposing amendments to rule 204–3 under the Advisers Act under the authority set forth in sections 203(d), 206(4), 211(a) and 211(h) of the Advisers Act of 1940 [15 U.S.C. 80b–3(d), 10b–6(4) and 80b–11(a) and (h)]. The Commission is proposing amendments to rule 204–2 under the Advisers Act under the authority set forth in sections 204 and 211 of the Advisers Act of 1940 [15 U.S.C. 80b–4 and 80b–11]. The Commission is proposing amendments to Form ADV under section 19(a) of the Securities Act [15 U.S.C. 77s(a)], sections 23(a) and 28(e)(2) of the Exchange Act [15 U.S.C. 78w(a) and 78bb(e)(2)], section 319(a) of the Trust Indenture Act of 1939 [15 U.S.C. 7sss(a)], section 38(a) of the Investment Company Act [15 U.S.C. 80a–37(a)], and sections 203(c)(1), 204, and 211(a) of the Advisers Act of 1940 [15 U.S.C. 80b–3(c)(1), 80b–4, and 80b–11(a)]. The Commission is proposing rule 38a–2 under the authority set forth in sections 31(a), and 38(a) of the Investment Company Act [15 U.S.C. 80a–30(a) and 80a–37(a)]. The Commission is proposing amendments to Form N–1A, Form N–2, Form N–3, Form N–4, Form N–6, Form N–8B–2, and Form S–6 under the authority set forth in sections 8, 30, and 38 of the Investment Company Act [15 U.S.C. 80a–8, 80a–29, and 80a–37] and sections 6, 7(a), 10 and 19(a) of the Securities Act [15 U.S.C. 77f, 77g(a), 77j, 77s(a)]. The Commission is proposing amendments to rule 232.11 and 232.405 under the authority set forth in section 23 of the Exchange Act [15 U.S.C. 78w]. The Commission is proposing amendments to rule 230.485 and rule 230.497 under the authority set forth in sections 10 and 19 of the Securities Act [15 U.S.C. 77j and 77s].

C. Small Entities Subject to the Rules and Rule Amendments

In developing these proposals, we have considered their potential effect on

[308] *See* proposed rule 204–2(a)(17)(i), (iv) through (vii).

[309] *See* proposed rule 204–6.

[310] *See id.*

[311] *See* proposed rule 204–3(b)(4).

small entities that would be subject to the proposed rules and amendments. The proposed rules and amendments would affect many, but not all, investment advisers registered with the Commission, including some small entities.

1. Small Entities Subject to Proposed Rule 206(4)–9, Proposed Rule 204–6, Proposed Form ADV–C and Proposed Amendments to Rule 204–2, Rule 204–3, and Form ADV Part 2A

Under Commission rules, for the purposes of the Advisers Act and the RFA, an investment adviser generally is a small entity if it: (1) Has assets under management having a total value of less than $25 million; (2) did not have total assets of $5 million or more on the last day of the most recent fiscal year; and (3) does not control, is not controlled by, and is not under common control with another investment adviser that has assets under management of $25 million or more, or any person (other than a natural person) that had total assets of $5 million or more on the last day of its most recent fiscal year.[312] Our proposed rules and amendments would not affect most investment advisers that are small entities (''small advisers'') because they are generally registered with one or more state securities authorities and not with the Commission. Under section 203A of the Advisers Act, most small advisers are prohibited from registering with the Commission and are regulated by state regulators. Based on IARD data, we estimate that as of October 31, 2021, approximately 579 SEC-registered advisers are small entities under the RFA.[313]

As discussed above in section III.C (the Economic Analysis), the Commission estimates that based on IARD data as of October 31, 2021, approximately 14,774 investment advisers would be subject to proposed rule 206(4)–9 and the related proposed amendments to rule 204–2 under the Advisers Act.

All of the approximately 579 SEC-registered advisers that are small entities under the RFA would be subject to proposed rule 206(4)–9, proposed rule 204–6, and proposed Form ADV–C as well as the proposed amendments to rule 204–2, rule 204–3 and Form ADV Part 2A.

2. Small Entities Subject to Proposed Rule 38a–2 and Proposed Amendments to Fund Registration Forms

For purposes of Commission rulemaking in connection with the Regulatory Flexibility Act, an investment company is a small entity if, together with other investment companies in the same group of related investment companies, it has net assets of $50 million or less as of the end of its most recent fiscal year (a ''small fund'').[314] All of the approximately 27 registered open-end mutual funds, 6 registered ETFs, 23 registered closed-end funds, 5 UITs, and 9 BDCs (collectively, 70 funds) that are small entities under the RFA would be subject to proposed rule 38a–2 and the proposed amendments to fund registration forms, including the structured data requirements.[315]

D. Projected Reporting, Recordkeeping and Other Compliance Requirements

1. Proposed Rule 206(4)–9

Proposed rule 206(4)–9 would impose certain reporting and compliance requirements on investment advisers, including those that are small entities. All registered investment advisers, including small entity advisers, would be required to comply with the proposed rule's policies and procedures and annual review requirement. The proposed requirements, including compliance and recordkeeping requirements, are summarized in this IRFA (section V.A. above). All of these proposed requirements are also discussed in detail, above, in sections I and II, and these requirements and the burdens on respondents, including those that are small entities, are discussed above in sections III and IV (the Economic Analysis and Paperwork Reduction Act Analysis, respectively) and below. The professional skills required to meet these specific burdens are also discussed in sections II through IV.

There are different factors that would affect whether a smaller adviser incurs costs relating to these requirements that are higher or lower than the estimates discussed in section IV.B. For example, we would expect that smaller advisers may not already have cybersecurity programs that would meet all of the elements that would be required under the proposed amendments. Also, while we would expect larger advisers to incur higher costs related to this proposed rule in absolute terms relative to a smaller adviser, we would expect a smaller adviser to find it more costly, per dollar managed, to comply with the proposed requirements because it would not be able to benefit from a larger adviser's economies of scale.

As discussed above, there are approximately 579 small advisers currently registered with us, and we estimate that 100 percent of advisers registered with us would be subject to the proposed rule 206(4)–9. As discussed above in our Paperwork Reduction Act Analysis in section IV, the proposed rule 206(4)–9 under the Advisers Act, which would require advisers to prepare policies and procedures related to cybersecurity risks and incidents, as well as annual review of those policies and procedures, which would create a new annual burden of approximately 31.67 hours per adviser, or 18,336.93 hours in aggregate for small advisers. We therefore expect the annual monetized aggregate cost to small advisers associated with our proposed amendments would be $7,262,139.36.[316]

2. Proposed Rule 38a–2

The proposed amendments contain compliance requirements regarding policies and procedures, reporting, recordkeeping, and other requirements to manage cybersecurity risks and incidents. All registered investment companies and BDCs, including small entities, would be required to comply with the proposed rule's requirements. We discuss the specifics of these burdens in the Economic Analysis and Paperwork Reduction Act sections above. The proposed requirements, including compliance and recordkeeping requirements, are summarized in this IRFA (section V.A. above). All of these proposed requirements are also discussed in detail in sections I and II above, and these requirements and the burdens on respondents, including those that are small entities, are discussed above in sections III and IV (the Economic Analysis and Paperwork Reduction Act Analysis, respectively) and below. The professional skills required to meet

[312] Advisers Act rule 0–7(a) [17 CFR 275.0–7].

[313] Based on SEC-registered investment adviser responses to Items 5.F. and 12 of Form ADV.

[314] *See* rule 0–10(a) under the Investment Company Act [17 CFR 270.0–10(a)].

[315] This estimate is derived an analysis of data obtained from Morningstar Direct as well as data reported to the Commission for the period ending June 2021. We expect few, if any, separate accounts would be treated as small entities because state law generally treats separate account assets as the property of the sponsoring insurance company. Rule 0–10(b) under the Investment Company Act aggregates each separate account's assets with the assets of the sponsoring insurance company, together with assets held in other sponsored separate accounts.

[316] $185,303,708 total cost × (579 small advisers/14,774 advisers) = $7,262,139.36.

these specific burdens are also discussed in sections II through IV.

There are different factors that would affect whether a smaller fund incurs costs relating to these requirements that are higher or lower than the estimates discussed in section IV.C. For example, we would expect that smaller funds—and more specifically, smaller funds that are not part of a fund complex—may not have cybersecurity programs that would meet all the elements that would be required under the proposed amendments. Also, while we would expect larger funds or funds that are part of a large fund complex to incur higher costs related to this requirement in absolute terms relative to a smaller fund or a fund that is part of a smaller fund complex, we would expect a smaller fund to find it more costly, per dollar managed, to comply with the proposed requirement because it would not be able to benefit from a larger fund complex's economies of scale. Notwithstanding the economies of scale experienced by large versus small funds, we would not expect the costs of compliance associated with the new requirements to be meaningfully different for small versus large funds.

As discussed above, there are approximately 70 funds that are small entities currently registered with us, and we estimate that 100 percent of funds registered with us would be subject to the proposed rule 38a–2. As discussed above in our Paperwork Reduction Act Analysis in section IV, the proposed rule 38a–2 under the Investment Company Act, which would require funds to prepare policies and procedures related to cybersecurity risks and incidents, as well as annual review of those policies and procedures, would create a new annual burden of approximately 32 hours per fund, or 2,240 hours in aggregate for funds that are small entities. We therefore expect the annual monetized aggregate cost to small funds associated with our proposed amendments would be $947,170.[317]

3. Proposed Amendments to Rule 204–2

The proposed amendments to rule 204–2 would impose certain recordkeeping requirements on investment advisers, including those that are small entities. All registered investment advisers, including small entity advisers, would be required to comply with the recordkeeping amendments, which are summarized in this IRFA (section V.C. above). The proposed amendments are also discussed in detail, above, in sections I and II, and the requirements and the burdens on respondents, including those that are small entities, are discussed above in sections III and IV (the Economic Analysis and Paperwork Reduction Act Analysis, respectively) and below. The professional skills required to meet these specific burdens are also discussed in sections II through IV.

As discussed above, there are approximately 579 small advisers currently registered with us, and we estimate that 100 percent of advisers registered with us would be subject to the proposed amendments to rule 204–2. As discussed above in our Paperwork Reduction Act Analysis in section IV, the proposed amendments to rule 204–2 under the Advisers Act, which would require advisers to retain certain copies of documents required under proposed rule 206(4)–9 and proposed rule 204–6, would create a new annual burden of approximately 5 hours per adviser, or 2,895 hours in aggregate for small advisers. We therefore expect the annual monetized aggregate cost to small advisers associated with our proposed amendments would be $196,860.[318]

4. Proposed Rule 204–6

Proposed rule 204–6 would impose certain reporting and compliance requirements on investment advisers, including those that are small entities. Specifically, proposed rule 204–6 would require advisers to report significant cybersecurity incidents with the Commission by filing proposed Form ADV–C. All registered investment advisers, including small entity advisers, would be required to comply with the proposed rule's reporting requirement by filing proposed Form ADV–C. The proposed requirements, including reporting and compliance requirements, are summarized in this IRFA (section V.C. above). All of these proposed requirements are also discussed in detail, above, in sections I and II, and these requirements and the burdens on respondents, including those that are small entities, are discussed above in sections III and IV (the Economic Analysis and Paperwork Reduction Act Analysis, respectively) and below. The professional skills required to meet these specific burdens are also discussed in sections II through IV.

As discussed above, there are approximately 579 small advisers currently registered with us, and we estimate that 100 percent of advisers registered with us would be subject to proposed rule 204–6. As discussed above in our Paperwork Reduction Act Analysis in section IV, proposed rule 204–6 under the Advisers Act, which would require advisers to report to the Commission any significant adviser cybersecurity incident or significant fund cybersecurity incident, would create a new annual burden of approximately 4 hours per adviser, or 2,316 hours in aggregate for small advisers. We therefore expect the annual monetized aggregate cost to small advisers associated with our proposed amendments would be $343,926.[319]

5. Form ADV–C

Proposed Form ADV–C would impose certain reporting and compliance requirements on investment advisers, including those that are small entities. All registered investment advisers, including small entity advisers, would be required to comply with the proposed Form ADV–C's requirements. The proposed requirements, including reporting and compliance requirements, are summarized in this IRFA (section V.C. above). All of these proposed requirements are also discussed in detail, above, in sections I and II, and these requirements and the burdens on respondents, including those that are small entities, are discussed above in sections III and IV (the Economic Analysis and Paperwork Reduction Act Analysis, respectively) and below. The professional skills required to meet these specific burdens are also discussed in sections II through IV.

As discussed above, there are approximately 579 small advisers currently registered with us, and we estimate that 100 percent of advisers registered with us would be subject to proposed Form ADV–C. As discussed above in our Paperwork Reduction Act Analysis in section IV, proposed Form ADV–C, which advisers would file to report any significant cybersecurity incidents, would create a new annual burden of approximately 1.5 hours per adviser, or 868.5 hours in aggregate for small advisers. We therefore expect the annual monetized aggregate cost to small advisers associated with our proposed amendments would be $343,926.[320]

[317] 70 small funds × $13,531 internal time cost per fund = $947,170.

[318] $5,023,160 total cost × (579 small advisers/14,774 advisers) = $196,860.

[319] $8,775,756 total cost × (579 small advisers/14,774 advisers) = $343,926.

[320] $8,775,756 total cost × (579 small advisers/14,774 advisers) = $343,926.

6. Proposed Amendments to Form ADV Part 2A

The proposed amendments to Form ADV would impose certain reporting and compliance requirements on investment advisers, including those that are small entities. All registered investment advisers, including small entity advisers, would be required to comply with the proposed amendments to Form ADV Part 2A. The proposed requirements are summarized in this IRFA (section V.C. above). They are also discussed in detail, above, in sections I and II, and these requirements and the burdens on respondents, including those that are small entities, are discussed above in sections III and IV (the Economic Analysis and Paperwork Reduction Act Analysis, respectively) and below. The professional skills required to meet these specific burdens are also discussed in sections II through IV.

As discussed above, there are approximately 579 advisers currently registered with us, and we estimate that 100 percent of advisers registered with us would be subject to the proposed amendments to Form ADV Part 2A. As discussed above in our Paperwork Reduction Act Analysis in section IV, the proposed amendments, which would require advisers to disclose any cybersecurity risks and incidents in their brochure, would create a new annual burden of approximately 16.28 hours per adviser, or 9,426.12 hours in aggregate for small advisers. We therefore expect the annual monetized aggregate cost to small advisers associated with our proposed amendments would be $3,185,694.08.[321]

7. Proposed Amendments to Rule 204–3

The proposed amendments to rule 204–3 would impose certain reporting and compliance requirements on investment advisers, including those that are small entities. All registered investment advisers, including small entity advisers, would be required to comply with the proposed amendments to rule 204–3. The proposed amendments are summarized in this IRFA (section V.C. above). They are also discussed in detail, above, in sections I and II, and these requirements and the burdens on respondents, including those that are small entities, are discussed above in sections III and IV (the Economic Analysis and Paperwork Reduction Act Analysis, respectively) and below. The professional skills required to meet these specific burdens are also discussed in sections II through IV.

As discussed above, there are approximately 579 small advisers currently registered with us, and we estimate that 100 percent of advisers registered with us would be subject to the proposed amendments to rule 204–3. As discussed above in our Paperwork Reduction Act Analysis in section IV, the proposed amendments, which would require advisers to deliver an amended brochure if the amendment adds disclosure of an event, or materially revises information already disclosed about an event that involves a cybersecurity incident, would create a new annual burden of approximately 0.1 hours per adviser, or 57.9 hours in aggregate for small advisers. We therefore expect the annual monetized aggregate cost to small advisers associated with our proposed amendments would be $3,705.60.[322]

8. Proposed Amendments to Fund Registration Forms, Rule 485 and Rule 497 Under the Securities Act, and Rule 11 and Rule 405 of Regulation S–T

The Commission also is proposing enhanced disclosure requirements on registration statements to enhance investor protection by requiring that cybersecurity incident-related information is available to increase understanding in these areas and help ensure that investors and clients can make informed investment decisions. Our proposal would require funds to provide prospective and current investors with disclosure about significant fund cybersecurity incidents on Forms N–1A, N–2, N–3, N–4, N–6, N–8B–2, and S–6, as applicable. Our proposal would also require a fund to tag information about significant fund cybersecurity incidents using Inline XBRL.

These requirements will impose burdens on all funds, including those that are small entities. The proposed requirements, including compliance and recordkeeping requirements, are summarized in this IRFA (section V.A. above). All of these proposed requirements are also discussed in detail in sections I and II above, and these requirements and the burdens on respondents, including those that are small entities, are discussed above in sections III and IV (the Economic Analysis and Paperwork Reduction Act Analysis, respectively) and below. The professional skills required to meet these specific burdens are also discussed in sections II through IV.

As discussed above, there are approximately 27 registered open-end mutual funds, 6 registered ETFs, 23 registered closed-end funds, 5 UITs, and 9 BDCs (collectively, 70 funds) that are small entities under the RFA that would be subject to the proposed amendments to fund registration forms.[323] As discussed above in our Paperwork Reduction Act Analysis in section IV, the proposed amendments to disclosure forms, which would require funds to provide disclosure about significant cybersecurity incidents, would create a new annual burden. We therefore expect the annual monetized aggregate cost to small funds associated with our proposed amendments would be $404,060.[324]

There are different factors that would affect whether a smaller fund incurs costs related to this requirement that are on the higher or lower end of the estimated range. For example, while we would expect larger funds or funds that are part of a large fund complex to incur higher costs related to this requirement in absolute terms relative to a smaller fund or a fund that is part of a smaller fund complex, we would expect a smaller fund to find it more costly, per dollar managed, to comply with the proposed requirement because it would not be able to benefit from a larger fund complex's economies of scale. For example, a large firm may have a business unit that manages cybersecurity for the whole firm, often led by a Chief Information Security Officer. The costs of that consolidated function, while substantial, would be spread across the whole firm, leading to economies of scale.

Notwithstanding the economies of scale experienced by large versus small funds, we would not expect the costs of compliance associated with the new disclosure requirements to be meaningfully different for small versus large funds. The costs of compliance would likely vary based on the significant fund cybersecurity incident. For example, a fund, no matter the size,

[321] $81,287,468.54 total cost × (579 small advisers/14,774 advisers) = $3,185,694.08.

[322] $94,553.6 total cost × (579 small advisers/14,774 advisers) = $3,705.60.

[323] This estimate is derived an analysis of data obtained from Morningstar Direct as well as data reported to the Commission for the period ending June 2021. We expect few, if any, separate accounts would be treated as small entities because state law generally treats separate account assets as the property of the sponsoring insurance company. Rule 0–10(b) under the Investment Company Act aggregates each separate account's assets with the assets of the sponsoring insurance company, together with assets held in other sponsored separate accounts.

[324] $404,060 = (70 funds × $5,340 disclosure form internal time cost) + (65 current XBRL filers × $356 interactive data internal time cost) + (5 new XBRL filers × $1,424 interactive data internal time cost).

would experience more burden if it experienced multiple significant fund cybersecurity incidents.

We are proposing to require all funds, including small entities, to tag the disclosure about significant fund cybersecurity incidents in Inline XBRL in accordance with rule 405 of Regulation S–T and the EDGAR Filer Manual. Large and small funds would both incur the costs associated with the proposed structured data requirements on a proportional basis. Furthermore, as noted above, based on our experience implementing tagging requirements that use the XBRL, we recognize that some funds that would be affected by the proposed requirement, particularly filers with no Inline XBRL tagging experience, likely would incur initial costs to acquire the necessary expertise and/or software as well as ongoing costs of tagging required information in Inline XBRL. The incremental effect of any fixed costs, including ongoing fixed costs, of complying with the proposed Inline XBRL requirement may be greater for smaller filers. However, we believe that smaller funds in particular may benefit more from any enhanced exposure to investors that could result from these proposed requirements. If reporting the disclosures in a structured data language increases the availability of, or reduces the cost of collecting and analyzing, key information about funds, smaller funds may benefit from improved coverage by third-party information providers and data aggregators.

E. Duplicative, Overlapping, or Conflicting Federal Rules

1. Proposed Rule 206(4)–9

Investment advisers do not have obligations under the Advisers Act specifically for policies and procedures related to cybersecurity risks and incidents. However, their fiduciary duties require them to take steps to protect client interests, which would include steps to minimize operational and other risks that could lead to significant business disruptions or a loss or misuse of client information. Since cybersecurity incidents can lead to significant business disruptions and loss or misuse of client information, advisers should already be taking steps to minimize cybersecurity risks in accordance with their fiduciary duties. In addition, rule 206(4)–7 under the Advisers Act already requires advisers to consider their fiduciary and regulatory obligations and formalize policies and procedures reasonably designed to address them. While rule 206(4)–7 does not enumerate specific elements that an adviser must include in its compliance program, advisers may already be assessing the cybersecurity risks created by their particular circumstances when developing their compliance policies and procedures to address such risks.

Other Commission rules also require advisers to consider cybersecurity. For example, as described above, advisers subject to Regulation S–P are required to, among other things, adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information.[325] In addition, advisers subject to Regulation S–ID must develop and implement a written identity theft program.[326] Nevertheless, while some advisers may have established effective cybersecurity programs under the existing regulatory framework, there are no Commission rules that explicitly require firms to adopt and implement comprehensive cybersecurity policies and procedures.

Recently, the Federal Deposit Insurance Corporation, the Board of Governors of the Federal Reserve System, and the Office of the Comptroller of the Currency adopted a new rule that would require certain banking organizations in the United States to notify Federal banking regulators of any cybersecurity incidents within 36 hours of discovering an incident (''bank cybersecurity rule'').[327] To the extent that a bank or one of its subsidiaries is also registered with the Commission as an investment adviser, there may be overlapping notification requirements. Additionally, to the extent a firm is required to implement cybersecurity-related policies and procedures due to its status as a banking organization, if such a firm is also registered with the Commission, our proposed rules requiring advisers and funds to adopt and implement cybersecurity policies and procedures may result in some overlapping regulatory requirements with respect to cybersecurity. However, our proposed amendments related to cybersecurity are designed to address the cybersecurity risks created as a result of a firm's operations as an adviser or fund, which may not be sufficiently addressed under cybersecurity regulations applicable to banks.

In addition, the FTC recently amended their Standards for Safeguarding Customer Information that contains a number of modifications to the existing FTC Safeguards Rule with respect to data security requirements to protect customer financial information.[328] We understand that private funds are generally subject to the FTC Safeguards Rule and to the extent that a private fund is managed by an adviser that is registered with Commission, our proposed rule requiring advisers to adopt and implement cybersecurity policies and procedures may result in some overlapping regulatory requirements with respect to protecting information. However, our proposed amendments related to cybersecurity are designed to address the cybersecurity risks created as a result of an adviser's operations and not specifically those related to the protection of customer financial information by private funds.

2. Proposed Rule 38a–2

Commission staff have not identified any Federal rules that duplicate, overlap, or conflict with the proposed rule 38a–2.

3. Proposed Amendments to Rule 204–2

As part of proposed rule 206(4)–9 and proposed rule 204–6, we are proposing corresponding amendments to the books and records rule. There are no duplicative, overlapping, or conflicting Federal rules with respect to the proposed amendments to rule 204–2.

4. Proposed Rule 204–6

Proposed rule 204–6 would create a new reporting requirement for advisers to report significant cybersecurity incidents to the Commission. There are no duplicative, overlapping, or conflicting Federal rules with respect to proposed rule 204–6.

5. Form ADV–C

Our proposed Form ADV–C would require advisers to provide information regarding a significant cybersecurity incident through a series of check-the-box and fill-in-the-blank questions related to the nature and extent of the cybersecurity incident and the adviser's response to the incident. The information requested on proposed Form ADV–C would not be duplicative of, overlap, or conflict with, other information advisers are required to provide on Form ADV.

[325] *See supra* footnote 14 and accompanying text.

[326] *See supra* footnote 16.

[327] *See* Office of the Comptroller of the Currency, Federal Reserve System, and Federal Deposit Insurance Corporation, *Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers* (Nov. 18, 2021) [86 FR 66424 (Nov. 23, 2021)].

[328] *See* Federal Trade Commission, *Standards for Safeguarding Customer Information* (Oct. 27, 2021) [86 FR 70272 (Dec. 9, 2021)].

6. Proposed Amendments to Form ADV

Our proposed new Item 20 in Form ADV Part 2A would require advisers to: (1) Describe any cybersecurity risks that could materially affect the advisory services they offer and how they assess, prioritize, and address cybersecurity risks; and (2) describe any cybersecurity incidents that have occurred in the past two fiscal years that have significantly disrupted or degraded the adviser's ability to maintain critical operations, or has led to the unauthorized access or use of adviser information, resulting in substantial harm to the adviser or its clients. These proposed requirements would not be duplicative of, overlap, or conflict with, other information advisers are required to provide on Form ADV.

7. Proposed Amendments to Rule 204–3

Our proposed amendments to rule 204–3(b) would require an adviser to promptly deliver interim brochure amendments to existing clients if the adviser adds disclosure of a cybersecurity incident to its brochure or materially revises information already disclosed in its brochure about such an incident. There are no duplicative, overlapping, or conflicting Federal rules with respect to the proposed amendments to rule 204–3.

8. Proposed Amendments to Fund Registration Forms, Rules Under the Securities Act, and Regulation S–T

Commission staff have not identified any Federal rules that duplicate, overlap, or conflict with the proposed amendments to Forms N–1A, N–2, N–3, N–4, N–6, N–8B–2, and S–6, conforming amendments to rule 485 and 497 under the Securities Act, and rule 11 and rule 405 of Regulation S–T.

F. Significant Alternatives

The Regulatory Flexibility Act directs the Commission to consider significant alternatives that would accomplish our stated objective, while minimizing any significant economic effect on small entities. We considered the following alternatives for small entities in relation to our proposal: (1) Exempting advisers and funds that are small entities from the proposed policies and procedures and disclosure requirements, to account for resources available to small entities; (2) establishing different requirements or frequency, to account for resources available to small entities; (3) clarifying, consolidating, or simplifying the compliance requirements under the proposal for small entities; and (4) using design rather than performance standards.

1. Proposed Rule 206(4)–9

The RFA directs the Commission to consider significant alternatives that would accomplish our stated objectives, while minimizing any significant adverse effect on small entities. We considered the following alternatives for small entities in relation to the proposed rule 206(4)–9: (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 believes that establishing different compliance or reporting requirements for small advisers, or exempting small advisers from the proposed rule, or any part thereof, would be inappropriate under these circumstances. Because the protections of the Advisers Act are intended to apply equally to clients of both large and small firms, it would be inconsistent with the purposes of the Advisers Act to specify differences for small entities under the proposed rule 206(4)–9 and corresponding changes to rule 204–2. As discussed above, we believe that the proposed rule would result in multiple benefits to clients. For example, having appropriate cybersecurity policies and procedures in place would help address any cybersecurity risks and incidents that occur at the adviser and help protect advisers and their clients from greater risk of harm. We believe that these benefits should apply to clients of smaller firms as well as larger firms. Establishing different conditions for large and small advisers even though advisers of every type and size rely on technology systems and networks and thus face increasing cybersecurity risks would negate these benefits. The corresponding changes to rule 204–2 are narrowly tailored to address proposed rule 206(4)–9.

Regarding the second alternative, we believe the current proposal is clear and that further clarification, consolidation, or simplification of the compliance requirements is not necessary. As discussed above, the proposed rule would require advisers to adopt and implement cybersecurity policies and procedures 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.[329] Advisers would also be required under the rule to conduct an annual review and assessment of these policies and procedures. The proposed rule would provide clarity in the existing regulatory framework regarding cybersecurity and serve as an explicit requirement for firms to adopt and implement comprehensive cybersecurity programs.

Regarding the third alternative, we determined to use performance standards rather than design standards. Although the proposed rule requires policies and procedures that are reasonably designed to address a certain number of elements, we do not place certain conditions or restrictions on how to adopt and implement such policies and procedures. The general elements are designed to enumerate core areas that firms must address when adopting, implementing, reassessing and updating their cybersecurity policies and procedures. As discussed above, given the number and varying characteristics of advisers, we believe firms need the ability to tailor their cybersecurity policies and procedures based on their individual facts and circumstances. Proposed rule 206(4)–9 therefore allows advisers to address the general elements based on the particular cybersecurity risks posed by each adviser's operations and business practices. The proposed rule would also provide flexibility for the adviser to determine the personnel who would implement and oversee the effectiveness of its cybersecurity policies and procedures.

2. Proposed Rule 38a–2 and Proposed Amendments to the Fund Registration Forms, Rules Under the Securities Act, and Regulation S–T

We do not believe that exempting small funds from the provisions of the proposed amendments would permit us to achieve our stated objectives. We believe funds of all sizes are subject to cybersecurity risks and may experience cybersecurity incidents. Cybersecurity incidents affecting funds also can cause substantial harm to their investors, including by interfering with the fund's ability to execute its investment strategy or theft of fund or client data. If the proposal did not include policies and procedures requirements for small funds, we believe the lack could raise investor protection concerns for investors in small funds, in that a small fund would not be subject to the same compliance framework and therefore

[329] *See* proposed rule 206(4)–9. *See also supra* section II.A.

may not have as robust of a compliance program as funds that were subject to the required framework. For the same reasons, we also do not believe that it would be appropriate to establish different cybersecurity requirements, frequency of disclosure or reporting, or interactive data requirements for small funds.

We also believe the current proposal is clear and that further clarification, consolidation, or simplification of the compliance requirements is not necessary. As discussed above, the proposed rule would require funds to adopt and implement cybersecurity policies and procedures 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.[330] Funds would also be required under the rule to conduct an annual review and assessment of these policies and procedures. The proposed rule would provide clarity in the existing regulatory framework regarding cybersecurity and serve as an explicit requirement for funds to adopt and implement comprehensive cybersecurity programs.

The costs associated with the proposed amendments would vary depending on the fund's particular circumstances, and on the number and severity of cybersecurity incidents that a fund experiences. These variations would result in different burdens on funds' resources. In particular, we expect that a fund that has experienced multiple cybersecurity incidents would bear more expense related to the proposed amendments. To protect investors of both small and large funds, we believe that it is appropriate for the costs associated with the proposed amendments to be based on the costs of: (1) Implementing a fund's cybersecurity policies and procedures; and (2) disclosing any significant fund cybersecurity incident, instead of adjusting these costs to account for a fund's size.

Finally, with respect to the use of design rather than performance standards, the proposed amendments generally use design standards for all funds subject to the amendments, regardless of size. Although the proposed rule requires policies and procedures that are reasonably designed to address a certain number of elements, we do not place certain conditions or restrictions on how to adopt and implement such policies and procedures. The general elements are designed to enumerate core areas that firms must address when adopting, implementing, reassessing and updating their cybersecurity policies and procedures. We believe that providing funds with the flexibility permitted in the proposal to design the fund's own individual cybersecurity policies and procedures is appropriate, because the result would be compliance activities that are tailored to the particular cybersecurity risks posed by each fund's operations and business practices. The proposed rule would provide flexibility for a fund to determine the personnel who would implement and oversee the effectiveness of its cybersecurity policies and procedures. In addition, we are aware that cybersecurity threats and risk change to reflect current technology, and the proposed design standards for funds would permit them to be able to modify their cybersecurity programs in response to these developments.

3. Proposed Rule 204–6 and Form ADV–C

The RFA directs the Commission to consider significant alternatives that would accomplish our stated objectives, while minimizing any significant adverse effect on small entities. We considered the following alternatives for small entities in relation to the proposed rule 204–6 and the corresponding proposed Form ADV–C: (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 and Form ADV–C for such small entities; (3) the use of performance rather than design standards; and (4) an exemption from coverage of the proposed rule and Form ADV–C, or any part thereof, for such small entities.

Regarding the first and fourth alternatives, the Commission believes that establishing different compliance or reporting requirements for small advisers, or exempting small advisers from the proposed rule, or any part thereof, would be inappropriate under these circumstances. Because the protections of the Advisers Act are intended to apply equally to clients of both large and small firms, it would be inconsistent with the purposes of the Advisers Act to specify differences for small entities under proposed rule 204–6 and proposed Form ADV–C, as well as corresponding changes to rule 204–2. As discussed above, we believe that the proposed rule and Form ADV–C would result in multiple benefits to clients. For example, having this reporting would help us in our efforts to protect investors in connection with cybersecurity incidents by providing prompt notice of these incidents. It would also help us better assess the potential effect of the cybersecurity incident on the adviser and its covered clients and whether there is the potential for client and investor harm. We believe that these benefits should apply to clients of smaller firms as well as larger firms. As mentioned above, establishing different conditions for large and small advisers even though advisers of every type and size rely on technology systems and networks and thus face increasing cybersecurity risks would negate these benefits.

Regarding the second alternative, we believe the current proposal for rule 204–6 and Form ADV–C is clear and that further clarification, consolidation, or simplification of the compliance requirements is not necessary. As discussed above, proposed rule 204–6 would require advisers to report to the Commission through Form ADV–C, any significant cybersecurity incidents within 48 hours after having a reasonable basis to conclude that any such incident has occurred.[331] These proposals would provide a new, clear opportunity in the existing regulatory framework for reporting to the Commission with respect to significant cybersecurity incidents.

Regarding the third alternative, we determined to use a combination of performance and design standards. Our proposal requires all advisers, including small advisers, to report using Form ADV–C promptly, but in no event more than 48 hours after, having a reasonable basis to believe a significant cybersecurity incident has occurred. Once the adviser makes the determination that an incident would meet the definition of a significant cybersecurity incident, it is required to report on Form ADV–C within 48 hours. We believe this requirement should apply to all advisers, regardless of size, given that all types of advisers are susceptible to cybersecurity incidents, and obtaining such information from all advisers would help to ensure that the Commission has accurate and timely information with respect to adviser and fund cybersecurity incidents to better allocate resources when evaluating and responding to these incidents.

We also considered an alternative that would have increased the scope of the proposed rule's performance standards

[330] *See* proposed rule 38a–2; *see also supra* section II.A.

[331] *See* proposed rule 204–6; *see also supra* section II.B.

and removed the 48-hour threshold, solely relying on the word ''promptly.'' However, we believe providing a specific time period would provide advisers, including small advisers, with the opportunity to confirm its determination and prepare the report while still providing the Commission with timely notice about the incident.

1. Proposed Amendments to Form ADV and Rule 204–3

The RFA directs the Commission to consider significant alternatives that would accomplish our stated objectives, while minimizing any significant adverse effect on small entities. We considered the following alternatives for small entities in relation to the proposed amendments to Form ADV and rule 204–3: (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 amendments for such small entities; (3) the use of design rather than performance standards; and (4) an exemption from coverage of the proposed amendments, or any part thereof, for such small entities.

Regarding the first and fourth alternatives, the Commission believes that establishing different compliance or reporting requirements for small advisers, or exempting small advisers from the proposed amendments, or any part thereof, would be inappropriate under these circumstances. Because the protections of the Advisers Act are intended to apply equally to clients of both large and small firms, it would be inconsistent with the purposes of the Advisers Act to specify differences for small entities under the proposed amendments to Form ADV and rule 204–3. As discussed above, we believe that the proposed amendments would result in multiple benefits to clients. For example, the proposed amendments to Form ADV would improve the ability of clients and prospective clients to evaluate and understand relevant cybersecurity risks and incidents that advisers and their personnel face and their potential effect on the advisers' services. Also, requiring advisers to deliver interim brochure amendments to existing clients promptly if the adviser adds or materially revises disclosure of a cybersecurity incident, would enhance investor protection by enabling clients to take protective or remedial measures as appropriate. Clients and investors may also be able to determine whether their engagement of an adviser remains appropriate and consistent with their investment objectives better. We believe that these benefits should apply to clients of smaller firms as well as larger firms. Establishing different conditions for large and small advisers even though all advisers, regardless of type and size, face cybersecurity risks would negate these benefits.

Regarding the second alternative, we believe the current proposed amendments are clear and that further clarification, consolidation, or simplification of the compliance requirements is not necessary. As discussed above, the proposed amendments to Form ADV would require advisers to disclose information regarding cybersecurity risks that could materially affect the advisory relationship.[332] The proposed amendments to rule 204–3 would also require prompt delivery of interim brochure supplements if an adviser adds or materially revises disclosure related to a cybersecurity incident.[333] The proposed amendments to Form ADV would provide for advisers to present clear and meaningful cybersecurity disclosure to their clients and prospective clients, and the proposed amendments to rule 204–3 would assist in providing clients updated cybersecurity disclosures.

Regarding the third alternative, we determined to use a mix of performance and design standards, regardless of size, with respect to the proposed amendments. We believe the amendments already appropriately use performance rather than design standards in many instances. The proposed amendments to Form ADV do not contain any specific limitations or restrictions on the disclosure of cybersecurity risks and incidents. As discussed above, given the number and varying types of advisers, as well as the types of cybersecurity risks and incidents that may be present or occur at a particular adviser, respectively, we believe firms need the ability to tailor their disclosures according to their own circumstances. The proposed amendments to rule 204–3 do not change the performance standard already present in rule 204–3. Advisers may, with client consent, deliver their brochures and supplements, along with any updates, to clients electronically.[334] Advisers may also incorporate their supplements into the brochure or provide them separately.

G. Solicitation of Comments

We encourage written comments on the matters discussed in this IRFA. We solicit comment on the number of small entities subject to the proposed rule 206(4)–9, proposed rule 38a–2, proposed rule 204–6, proposed Form ADV–C, and proposed amendments to rule 204–2, rule 204–3, Form ADV, and the fund registration forms. We also solicit comment on the potential effects discussed in this analysis; and whether this proposal could have an effect on small entities that has not been considered. We request that commenters describe the nature of any effect on small entities and provide empirical data to support the extent of such effect.

VI. Consideration of Impact on the Economy

For purposes of the Small Business Regulatory Enforcement Fairness Act of 1996, or ''SBREFA,''773 we 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. We request 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.

VII. Statutory Authority

The Commission is proposing rule 38a–2 under the authority set forth in sections 31(a) and 38(a) of the Investment Company Act [15 U.S.C. 80a–30(a), and 80a–37(a)]. The Commission is proposing amendments to rule 204–2 under the Advisers Act under the authority set forth in sections 204 and 211 of the Advisers Act of 1940 [15 U.S.C. 80b–4 and 80b–11]. The Commission is proposing amendments to rule 204–3 under the Advisers Act under the authority set forth in sections 203(d), 206(4), 211(a) and 211(h) of the Advisers Act of 1940 [15 U.S.C. 80b–3(d), 10b–6(4) and 80b–11(a) and (h)]. The Commission is proposing rule 204–6, rule 206(4)–9, and Form ADV–C under the Advisers Act under the authority set forth in sections 203(d),

[332] *See supra* section II.C.

[333] *See* proposed rule 204–3; *see also supra* section II.C.

[334] Use of Electronic Media by Broker-Dealers, Transfer Agents, and Investment Advisers for Delivery of Information, Investment Advisers Act Release No. 1562 (May 9, 1996) [61 FR 24644 (May 15, 1996)].

206(4), and 211(a) of the Advisers Act of 1940 [15 U.S.C. 80b–3(d), 10b–6(4) and 80b–11(a)]. The Commission is proposing amendments to Form N–1A, Form N–2, Form N–3, Form N–4, Form N–6, Form N–8B–2, and Form S–6 under the authority set forth in sections 8, 30, and 38 of the Investment Company Act [15 U.S.C. 80a–8, 80a–29, and 80a–37] and sections 6, 7(a), 10 and 19(a) of the Securities Act [15 U.S.C. 77f, 77g(a), 77j, 77s(a)]. The Commission is proposing amendments to Form ADV under section 19(a) of the Securities Act [15 U.S.C. 77s(a)], sections 23(a) and 28(e)(2) of the Exchange Act [15 U.S.C. 78w(a) and 78bb(e)(2)], section 319(a) of the Trust Indenture Act of 1939 [15 U.S.C. 7sss(a)], section 38(a) of the Investment Company Act [15 U.S.C. 80a–37(a)], and sections 203(c)(1), 204, and 211(a) of the Advisers Act of 1940 [15 U.S.C. 80b–3(c)(1), 80b–4, and 80b–11(a)]. The Commission is proposing amendments to rule 232.11 and 232.405 under the authority set forth in section 23 of the Exchange Act [15 U.S.C. 78w]. The Commission is proposing amendments to rule 230.485 and rule 230.497 under the authority set forth in sections 10 and 19 of the Securities Act [15 U.S.C. 77j and 77s].

List of Subjects

17 CFR Part 230

Investment companies, Reporting and recordkeeping requirements, Securities.

17 CFR Part 232

Administrative practice and procedure, Reporting and recordkeeping requirements, Securities.

17 CFR Part 239

Reporting and recordkeeping requirements, Securities.

17 CFR Parts 270 and 274

Investment companies, Reporting and recordkeeping requirements, Securities.

17 CFR Parts 275 and 279

Reporting and recordkeeping requirements, Securities.

Text of Proposed Rules and Rule and Form Amendments

For the reasons set forth in the preamble, the Commission is proposing to amend title 17, chapter II of the Code of Federal Regulations as follows:

PART 230—GENERAL RULES AND REGULATIONS, SECURITIES ACT OF 1933

■ 1. The authority citation for part 230 continues to read, in part, as follows:

Authority: 15 U.S.C. 77b, 77b note, 77c, 77d, 77f, 77g, 77h, 77j, 77r, 77s, 77z–3, 77sss, 78c, 78d, 78j, 78*l,* 78m, 78n, 78o, 78o–7 note, 78t, 78w, 78*ll*(d), 78mm, 80a–8, 80a–24, 80a–28, 80a–29, 80a–30, and 80a–37, and Pub. L. 112–106, sec. 201(a), sec. 401, 126 Stat. 313 (2012), unless otherwise noted.

* * * * *

Sections 230.400 to 230.499 issued under secs. 6, 8, 10, 19, 48 Stat. 78, 79, 81, and 85, as amended (15 U.S.C. 77f, 77h, 77j, 77s).

* * * * *

■ 2. Amend § 230.485 by revising paragraph (c)(3) to read as follows:

§ 230.485 Effective date of post-effective amendments filed by certain registered investment companies.

* * * * *

(c) * * *

(3) A registrant's ability to file a post-effective amendment, other than an amendment filed solely for purposes of submitting an Interactive Data File, under paragraph (b) of this section is automatically suspended if a registrant fails to submit any Interactive Data File (as defined in § 232.11 of this chapter) required by the Form on which the registrant is filing the post-effective amendment. A suspension under this paragraph (c)(3) shall become effective at such time as the registrant fails to submit an Interactive Data File as required by the relevant Form. Any such suspension, so long as it is in effect, shall apply to any post-effective amendment that is filed after the suspension becomes effective, but shall not apply to any post-effective amendment that was filed before the suspension became effective. Any suspension shall apply only to the ability to file a post-effective amendment pursuant to paragraph (b) of this section and shall not otherwise affect any post-effective amendment. Any suspension under this paragraph (c)(3) shall terminate as soon as a registrant has submitted the Interactive Data File required by the relevant Form.

* * * * *

■ 3. Amend § 230.497 by revising paragraphs (c) and (e) to read as follows:

§ 230.497 Filing of investment company prospectuses—number of copies.

* * * * *

(c) For investment companies filing on §§ 239.15A and 274.11A of this chapter (Form N–1A), §§ 239.17a and 274.11b of this chapter (Form N–3), §§ 239.17b and 274.11c of this chapter (Form N–4), or §§ 239.17c and 274.11d of this chapter (Form N–6), within five days after the effective date of a registration statement or the commencement of a public offering after the effective date of a registration statement, whichever occurs later, 10 copies of each form of prospectus and form of Statement of Additional Information used after the effective date in connection with such offering shall be filed with the Commission in the exact form in which it was used. Investment companies filing on Forms N–1A, N–3, N–4, or N–6 must submit an Interactive Data File (as defined in § 232.11 of this chapter) if required by the Form on which the registrant files its registration statement.

* * * * *

(e) For investment companies filing on §§ 239.15A and 274.11A of this chapter (Form N–1A), §§ 239.17a and 274.11b of this chapter (Form N–3), §§ 239.17b and 274.11c of this chapter (Form N–4), or §§ 239.17c and 274.11d of this chapter (Form N–6), after the effective date of a registration statement, no prospectus that purports to comply with Section 10 of the Act (15 U.S.C. 77j) or Statement of Additional Information that varies from any form of prospectus or form of Statement of Additional Information filed pursuant to paragraph (c) of this section shall be used until five copies thereof have been filed with, or mailed for filing to the Commission. Investment companies filing on Forms N–1A, N–3, N–4, or N–6 must submit an Interactive Data File (as defined in § 232.11 of this chapter) if required by the Form on which the registrant files its registration statement.

* * * * *

PART 232—REGULATION S–T—GENERAL RULES AND REGULATIONS FOR ELECTRONIC FILINGS

■ 4. The authority citation for part 232 continues to read, in part, as follows:

Authority: 15 U.S.C. 77c, 77f, 77g, 77h, 77j, 77s(a), 77z–3, 77sss(a), 78c(b), 78*l,* 78m, 78n, 78o(d), 78w(a), 78*ll,* 80a–6(c), 80a–8, 80a–29, 80a–30, 80a–37, 7201 *et seq.;* and 18 U.S.C. 1350, unless otherwise noted.

* * * * *

■ 5. Amend § 232.11 by revising the definition of ''Related Official Filing'' to read as follows:

§ 232.11 Definition of terms used in this part.

* * * * *

Related Official Filing. The term *Related Official Filing* means the ASCII or HTML format part of the official filing with which all or part of an Interactive Data File appears as an exhibit or, in the case of a filing on Form N–1A (§§ 239.15A and 274.11A of this chapter), Form N–2 (§§ 239.14 and 274.11a–1 of this chapter), Form N–3 (§§ 239.17a and 274.11b of this chapter), Form N–4 (§§ 239.17b and 274.11c of this chapter), Form N–6 (§§ 239.17c and

274.11d of this chapter), Form N–8B–2 (§ 274.12 of this chapter), Form S–6 (§ 239.16 of this chapter), and Form N–CSR (§§ 249.331 and 274.128 of this chapter), and, to the extent required by § 232.405 [Rule 405 of Regulation S–T] for a business development company as defined in § 2(a)(48) of the Investment Company Act of 1940 (15 U.S.C. 80a–2(a)(48)), Form 10–K (§ 249.310 of this chapter), Form 10–Q (§ 249.308a of this chapter), and Form 8–K (§ 249.308 of this chapter), the ASCII or HTML format part of an official filing that contains the information to which an Interactive Data File corresponds.

* * * * *

■ 6. Amend § 232.405 by revising the introductory text, paragraphs (a)(2), (a)(3) introductory text, (a)(3)(i) introductory text, and (3)(ii), (a)(4), (b)(1) introductory text, (b)(2), (b)(3)(iii), Note 1 to § 232.405(b)(1), and Note 2 to § 232.405 to read as follows:

§ 232.405 Interactive Data File submissions.

This section applies to electronic filers that submit Interactive Data Files. Section 229.601(b)(101) of this chapter (Item 601(b)(101) of Regulation S–K), paragraph (101) of Part II—Information Not Required to be Delivered to Offerees or Purchasers of Form F–10 (§ 239.40 of this chapter), paragraph 101 of the Instructions as to Exhibits of Form 20–F (§ 249.220f of this chapter), paragraph B.(15) of the General Instructions to Form 40–F (§ 249.240f of this chapter), paragraph C.(6) of the General Instructions to Form 6–K (§ 249.306 of this chapter), General Instruction C.3.(g) of Form N–1A (§§ 239.15A and 274.11A of this chapter), General Instruction I of Form N–2 (§§ 239.14 and 274.11a–1 of this chapter), General Instruction C.3.(h) of Form N–3 (§§ 239.17a and 274.11b of this chapter), General Instruction C.3.(h) of Form N–4 (§§ 239.17b and 274.11c of this chapter), General Instruction C.3.(h) of Form N–6 (§§ 239.17c and 274.11d of this chapter), General Instruction 2.(l) of Form N–8B–2 (§ 274.12 of this chapter), General Instruction 5 of Form S–6 (§ 239.16 of this chapter), and General Instruction C.4 of Form N–CSR (§§ 249.331 and 274.128 of this chapter) specify when electronic filers are required or permitted to submit an Interactive Data File (§ 232.11), as further described in note 1 to this section. This section imposes content, format, and submission requirements for an Interactive Data File, but does not change the substantive content requirements for the financial and other disclosures in the Related Official Filing (§ 232.11).

(a) * * *

(2) Be submitted only by an electronic filer either required or permitted to submit an Interactive Data File as specified by § 229.601(b)(101) of this chapter (Item 601(b)(101) of Regulation S–K), paragraph (101) of Part II—Information Not Required to be Delivered to Offerees or Purchasers of Form F–10 (§ 239.40 of this chapter), paragraph 101 of the Instructions as to Exhibits of Form 20–F (§ 249.220f of this chapter), paragraph B.(15) of the General Instructions to Form 40–F (§ 249.240f of this chapter), paragraph C.(6) of the General Instructions to Form 6–K (§ 249.306 of this chapter), General Instruction C.3.(g) of Form N–1A (§§ 239.15A and 274.11A of this chapter), General Instruction I of Form N–2 (§§ 239.14 and 274.11a–1 of this chapter), General Instruction C.3.(h) of Form N–3 (§§ 239.17a and 274.11b of this chapter), General Instruction C.3.(h) of Form N–4 (§§ 239.17b and 274.11c of this chapter), General Instruction C.3.(h) of Form N–6 (§§ 239.17c and 274.11d of this chapter), General Instruction 2.(l) of Form N–8B–2 (§ 274.12 of this chapter), General Instruction 5 of Form S–6 (§ 239.16 of this chapter), or General Instruction C.4 of Form N–CSR (§§ 249.331 and 274.128 of this chapter), as applicable;

(3) Be submitted using Inline XBRL:

(i) If the electronic filer is not a management investment company registered under the Investment Company Act of 1940 (15 U.S.C. 80a et seq.), a separate account as defined in Section 2(a)(14) of the Securities Act (15 U.S.C. 77b(a)(14)) registered under the Investment Company Act of 1940, a business development company as defined in Section 2(a)(48) of the Investment Company Act of 1940 (15 U.S.C. 80a–2(a)(48)), or a unit investment trust as defined in Section 4(2) of the Investment Company Act of 1940 (15 U.S.C. 80a–4), and is not within one of the categories specified in paragraph (f)(1)(i) of this section, as partly embedded into a filing with the remainder simultaneously submitted as an exhibit to:

* * * * *

(ii) If the electronic filer is a management investment company registered under the Investment Company Act of 1940 (15 U.S.C. 80a *et seq.*), or a separate account (as defined in Section 2(a)(14) of the Securities Act (15 U.S.C. 77b(a)(14)) registered under the Investment Company Act of 1940, a business development company as defined in Section 2(a)(48) of the Investment Company Act of 1940 (15 U.S.C. 80a–2(a)(48)), or a unit investment trust as defined in Section 4(2) of the Investment Company Act of 1940 (15 U.S.C. 80a–4) and is not within one of the categories specified in paragraph (f)(1)(ii) of this section, as partly embedded into a filing with the remainder simultaneously submitted as an exhibit to a filing that contains the disclosure this section requires to be tagged; and

(4) Be submitted in accordance with the EDGAR Filer Manual and, as applicable, either Item 601(b)(101) of Regulation S–K (§ 229.601(b)(101) of this chapter), paragraph (101) of Part II—Information Not Required to be Delivered to Offerees or Purchasers of Form F–10 (§ 239.40 of this chapter), paragraph 101 of the Instructions as to Exhibits of Form 20–F (§ 249.220f of this chapter), paragraph B.(15) of the General Instructions to Form 40–F (§ 249.240f of this chapter), paragraph C.(6) of the General Instructions to Form 6–K (§ 249.306 of this chapter), General Instruction C.3.(g) of Form N–1A (§§ 239.15A and 274.11A of this chapter), General Instruction I of Form N–2 (§§ 239.14 and 274.11a–1 of this chapter), General Instruction C.3.(h) of Form N–3 (§§ 239.17a and 274.11b of this chapter), General Instruction C.3.(h) of Form N–4 (§§ 239.17b and 274.11c of this chapter), General Instruction C.3.(h) of Form N–6 (§§ 239.17c and 274.11d of this chapter); General Instruction 2.(l) of Form N–8B–2 (§ 274.12 of this chapter); General Instruction 5 of Form S–6 (§ 239.16 of this chapter); or General Instruction C.4 of Form N–CSR (§§ 249.331 and 274.128 of this chapter).

(b) * * *

(1) If the electronic filer is not a management investment company registered under the Investment Company Act of 1940 (15 U.S.C. 80a *et seq.*), a separate account (as defined in Section 2(a)(14) of the Securities Act (15 U.S.C. 77b(a)(14)) registered under the Investment Company Act of 1940, a business development company as defined in Section 2(a)(48) of the Investment Company Act of 1940 (15 U.S.C. 80a–2(a)(48)), or a unit investment trust as defined in Section 4(2) of the Investment Company Act of 1940 (15 U.S.C. 80a–4), an Interactive Data File must consist of only a complete set of information for all periods required to be presented in the corresponding data in the Related Official Filing, no more and no less, from all of the following categories:

* * * * *

Note 1 to § 232.405(b)(1): It is not permissible for the Interactive Data File to present only partial face financial statements, such as by excluding

comparative financial information for prior periods.

(2) If the electronic filer is an open-end management investment company registered under the Investment Company Act of 1940, a separate account (as defined in section 2(a)(14) of the Securities Act) registered under the Investment Company Act of 1940 (15 U.S.C. 80a *et seq.*), or a unit investment trust as defined in Section 4(2) of the Investment Company Act of 1940 (15 U.S.C. 80a–4), an Interactive Data File must consist of only a complete set of information for all periods required to be presented in the corresponding data in the Related Official Filing, no more and no less, from the information set forth in:

(i) Items 2, 3, 4, and 10(a)(4) of §§ 239.15A and 274.11A of this chapter (Form N–1A);

(ii) Items 2, 4, 5, 11, 16A, 18 and 19 of §§ 239.17a and 274.11b of this chapter (Form N–3);

(iii) Items 2, 4, 5, 10, 16A, and 17 of §§ 239.17b and 274.11c of this chapter (Form N–4);

(iv) Items 2, 4, 5, 10, 11, 16A and 18 of §§ 239.17c and 274.11d of this chapter (Form N–6); or

(v) Item 9A of § 274.12 of this chapter (Form N–8B–2), including to the extent required by § 239.16 of this chapter (Form S–6); as applicable.

(3) * * *

(iii) As applicable, all of the information provided in response to Items 3.1, 4.3, 8.2.b, 8.2.d, 8.3.a, 8.3.b, 8.5.b, 8.5.c, 8.5.e, 10.1.a–d, 10.2.a–c, 10.2.e, 10.3, 10.5, and 13 of Form N–2 in any registration statement or post-effective amendment thereto filed on Form N–2; or any form of prospectus filed pursuant to § 230.424 of this chapter (Rule 424 under the Securities Act); or, if a Registrant is filing a registration statement pursuant to General Instruction A.2 of Form N–2, any filing on Form N–CSR, Form 10–K, Form 10–Q, or Form 8–K to the extent such information appears therein.

* * * * *

Note 2 to § 232.405: Section 229.601(b)(101) of this chapter (Item 601(b)(101) of Regulation S–K) specifies the circumstances under which an Interactive Data File must be submitted and the circumstances under which it is permitted to be submitted, with respect to § 239.11 of this chapter (Form S–1), § 239.13 of this chapter (Form S–3), § 239.25 of this chapter (Form S–4), § 239.18 of this chapter (Form S–11), § 239.31 of this chapter (Form F–1), § 239.33 of this chapter (Form F–3), § 239.34 of this chapter (Form F–4), § 249.310 of this chapter (Form 10–K), § 249.308a of this chapter (Form 10–Q), and § 249.308 of this chapter (Form 8–K). Paragraph (101) of Part II—Information not Required to be Delivered to Offerees or Purchasers of § 239.40 of this chapter (Form F–10) specifies the circumstances under which an Interactive Data File must be submitted and the circumstances under which it is permitted to be submitted, with respect to Form F–10. Paragraph 101 of the Instructions as to Exhibits of § 249.220f of this chapter (Form 20–F) specifies the circumstances under which an Interactive Data File must be submitted and the circumstances under which it is permitted to be submitted, with respect to Form 20–F. Paragraph B.(15) of the General Instructions to § 249.240f of this chapter (Form 40–F) and Paragraph C.(6) of the General Instructions to § 249.306 of this chapter (Form 6–K) specify the circumstances under which an Interactive Data File must be submitted and the circumstances under which it is permitted to be submitted, with respect to § 249.240f of this chapter (Form 40–F) and § 249.306 of this chapter (Form 6–K). Section 229.601(b)(101) (Item 601(b)(101) of Regulation S–K), paragraph (101) of Part II—Information not Required to be Delivered to Offerees or Purchasers of Form F–10, paragraph 101 of the Instructions as to Exhibits of Form 20–F, paragraph B.(15) of the General Instructions to Form 40–F, and paragraph C.(6) of the General Instructions to Form 6–K all prohibit submission of an Interactive Data File by an issuer that prepares its financial statements in accordance with 17 CFR 210.6–01 through 210.6–10 (Article 6 of Regulation S–X). For an issuer that is a management investment company or separate account registered under the Investment Company Act of 1940 (15 U.S.C. 80a *et seq.*), a business development company as defined in Section 2(a)(48) of the Investment Company Act of 1940 (15 U.S.C. 80a–2(a)(48)), or a unit investment trust as defined in Section 4(2) of the Investment Company Act of 1940 (15 U.S.C. 80a–4), General Instruction C.3.(g) of Form N–1A (§§ 239.15A and 274.11A of this chapter), General Instruction I of Form N–2 (§§ 239.14 and 274.11a–1 of this chapter), General Instruction C.3.(h) of Form N–3 (§§ 239.17a and 274.11b of this chapter), General Instruction C.3.(h) of Form N–4 (§§ 239.17b and 274.11c of this chapter), General Instruction C.3.(h) of Form N–6 (§§ 239.17c and 274.11d of this chapter), General Instruction 2.(l) of Form N–8B–2 (§ 274.12 of this chapter), General Instruction 5 of Form S–6 (§ 239.16 of this chapter), and General Instruction C.4 of Form N–CSR (§§ 249.331 and 274.128 of this chapter), as applicable, specifies the circumstances under which an Interactive Data File must be submitted.

PART 239—FORMS PRESCRIBED UNDER THE SECURITIES ACT OF 1933

■ 7. The authority citation for part 239 continues to read, in part, as follows:

Authority: 15 U.S.C. 77c, 77f, 77g, 77h, 77j, 77s, 77z–2, 77z–3, 77sss, 78c, 78*l,* 78m, 78n, 78o(d), 78o–7 note, 78u–5, 78w(a), 78*ll,* 78mm, 80a–2(a), 80a–3, 80a–8, 80a–9, 80a–10, 80a–13, 80a–24, 80a–26, 80a–29, 80a–30, and 80a–37; and sec. 107, Pub. L. 112–106, 126 Stat. 312, unless otherwise noted.

* * * * *

■ 8. Amend Form S–6 (referenced in §§ 239.16) by adding General Instruction 5 as follows:

Note: The text of Form S–6 does not, and these amendments will not, appear in the *Code of Federal Regulations.*

Form S–6

* * * * *

General Instructions

* * * * *

Instruction 5. Interactive Data

(a) An Interactive Data File as defined in rule 11 of Regulation S–T [17 CFR 232.11] is required to be submitted to the Commission in the manner provided by rule 405 of Regulation S–T [17 CFR 232.405] for any registration statement or post-effective amendment thereto on Form S–6 that includes or amends information provided in response to item 9A of Form N–8B–2 (as provided pursuant to Instruction 1.(a) of the Instructions as to the Prospectus of this Form).

(1) Except as required by paragraph (a)(2), the Interactive Data File must be submitted as an amendment to the registration statement to which the Interactive Data File relates. The amendment must be submitted on or before the date the registration statement or post-effective amendment that contains the related information becomes effective.

(2) In the case of a post-effective amendment to a registration statement filed pursuant to paragraphs (b)(1)(i), (ii), (v), or (vii) of rule 485 under the Securities Act [17 CFR 230.485(b)], the Interactive Data File must be submitted either with the filing, or as an amendment to the registration statement to which the Interactive Data Filing relates that is submitted on or before the date the post-effective amendment that

contains the related information becomes effective.

(b) All interactive data must be submitted in accordance with the specifications in the EDGAR Filer Manual.

* * * * *

PART 270—RULES AND REGULATIONS, INVESTMENT COMPANY ACT OF 1940

■ 9. The authority citation for part 270 continues to read, in part, as follows:

Authority: 15 U.S.C. 80a–1 *et seq.,* 80a–34(d), 80a–37, 80a–39, and Pub. L. 111–203, sec. 939A, 124 Stat. 1376 (2010), unless otherwise noted.

* * * * *

■ 10. Section 270.38a–2 is added to read as follows:

§ 270.38a–2 Cybersecurity policies and procedures of certain investment companies.

(a) *Cybersecurity policies and procedures.* Each fund must adopt and implement written policies and procedures that are reasonably designed to address cybersecurity risks, including policies and procedures that:

(1) *Risk assessment.* (i) Require periodic assessments of cybersecurity risks associated with fund information systems and fund information residing therein including requiring the fund to:

(A) Categorize and prioritize cybersecurity risks based on an inventory of the components of the fund information systems and fund information residing therein and the potential effect of a cybersecurity incident on the fund; and

(B) Identify the fund's service providers that receive, maintain, or process fund information, or are otherwise permitted to access fund information systems and any fund information residing therein, and assess the cybersecurity risks associated with the fund's use of these service providers.

(ii) Require written documentation of any risk assessments.

(2) *User security and access.* Require controls designed to minimize user-related risks and prevent the unauthorized access to fund information systems and fund information residing therein including:

(i) Requiring standards of behavior for individuals authorized to access fund information systems and any fund information residing therein, such as an acceptable use policy;

(ii) Identifying and authenticating individual users, including implementing authentication measures that require users to present a combination of two or more credentials for access verification;

(iii) Establishing procedures for the timely distribution, replacement, and revocation of passwords or methods of authentication;

(iv) Restricting access to specific fund information systems or components thereof and fund information residing therein solely to individuals requiring access to such systems and information as is necessary for them to perform their responsibilities and functions on behalf of the fund; and

(v) Securing remote access technologies.

(3) *Information protection.*

(i) Require measures designed to monitor fund information systems and protect fund information from unauthorized access or use, based on a periodic assessment of the fund information systems and fund information that resides on the systems that takes into account:

(A) The sensitivity level and importance of fund information to its business operations;

(B) Whether any fund information is personal information;

(C) Where and how fund information is accessed, stored and transmitted, including the monitoring of fund information in transmission;

(D) Fund information systems access controls and malware protection; and

(E) The potential effect a cybersecurity incident involving fund information could have on the fund and its shareholders, including the ability for the fund to continue to provide services.

(ii) Require oversight of service providers that receive, maintain, or process fund information, or are otherwise permitted to access fund information systems and any fund information residing therein and through that oversight document that such service providers, pursuant to a written contract between the fund and any such service provider, are required to implement and maintain appropriate measures, including the practices described in paragraphs (a)(1), (2), (3)(i), (4), and (5) of this section, that are designed to protect fund information and fund information systems.

(4) *Cybersecurity threat and vulnerability management.* Require measures to detect, mitigate, and remediate any cybersecurity threats and vulnerabilities with respect to fund information systems and the fund information residing therein.

(5) *Cybersecurity incident response and recovery.* (i) Require measures to detect, respond to, and recover from a cybersecurity incident, including policies and procedures that are reasonably designed to ensure:

(A) Continued operations of the fund;

(B) The protection of fund information systems and fund information residing therein;

(C) External and internal cybersecurity incident information sharing and communications; and

(D) Reporting of a significant fund cybersecurity incident by the fund's adviser under § 275.204–6 (Rule 204–6 under the Investment Advisers Act of 1940).

(ii) Require written documentation of any cybersecurity incident, including the fund's response to and recovery from such an incident.

(b) *Annual review.* A fund must, at least annually, review and assess the design and effectiveness of the cybersecurity policies and procedures required by paragraph (a) of this section, including whether they reflect changes in cybersecurity risk over the time period covered by the review.

(c) *Board oversight.* A fund must:

(1) Obtain the initial approval of the fund's board of directors, including a majority of the directors who are not interested persons of the fund, of the fund's policies and procedures; and

(2) Provide, for review by the fund's board of directors, a written report prepared no less frequently than annually by the fund that, at a minimum, 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.

(d) *Unit investment trusts.* If the fund is a unit investment trust, the fund's principal underwriter or depositor must:

(i) Approve the fund's policies and procedures; and

(ii) Receive all written reports required by paragraph (c) of this section.

(e) *Recordkeeping.* The fund must maintain:

(1) A copy of the policies and procedures that are in effect, or at any time within the past five years were in effect, in an easily accessible place;

(2) Copies of written reports provided to the board of directors pursuant to paragraph (c)(2) of this section (or, if the fund is a unit investment trust, to the fund's principal underwriter or depositor, pursuant to paragraph (d) of this section) for at least five years after the end of the fiscal year in which the documents were provided, the first two years in an easily accessible place;

(3) Any records documenting the review pursuant to paragraph (c)(2) of

this section for at least five years after the end of the fiscal year in which the annual review was conducted, the first two years in an easily accessible place;

(4) Any report provided to the Commission pursuant to paragraph (a)(5) of this section for at least five years after the provision of the report, the first two years in an easily accessible place;

(5) Records documenting the occurrence of any cybersecurity incident, including records related to any response and recovery from such incident pursuant to paragraph (a)(5) of this section, for at least five years after the date of the incident, the first two years in an easily accessible place; and

(6) Records documenting the risk assessment pursuant to paragraph (a)(1) of this section for at least five years after the date of the assessment, the first two years in an easily accessible place.

(f) *Definitions.* For purposes of this section:

Cybersecurity incident means an unauthorized occurrence on or conducted through a fund's information systems that jeopardizes the confidentiality, integrity, or availability of a fund's information systems or any fund information residing therein.

Cybersecurity risk means financial, operational, legal, reputational, and other adverse consequences that could result from cybersecurity incidents, threats, and vulnerabilities.

Cybersecurity threat means any potential occurrence that may result in an unauthorized effort to adversely affect the confidentiality, integrity or availability of a fund's information systems or any fund information residing therein.

Cybersecurity vulnerability means a vulnerability in a fund's information systems, information system security procedures, or internal controls, including vulnerabilities in their design, configuration, maintenance, or implementation that, if exploited, could result in a cybersecurity incident.

Fund means a registered investment company or a business development company.

Fund information means any electronic information related to the fund's business, including personal information, received, maintained, created, or processed by the fund.

Fund information systems means the information resources owned or used by the fund, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of fund information to maintain or support the fund's operations.

Personal information means any information that can be used, alone or in conjunction with any other information, to identify an individual, such as name, date of birth, place of birth, telephone number, street address, mother's maiden name, Social Security number, driver's license number, electronic mail address, account number, account password, biometric records or other nonpublic authentication information.

Significant fund cybersecurity incident means a cybersecurity incident, or a group of related cybersecurity incidents, that significantly disrupts or degrades the fund's ability to maintain critical operations, or leads to the unauthorized access or use of fund information, where the unauthorized access or use of such information results in substantial harm to the fund or to an investor whose information was accessed.

PART 274—FORMS PRESCRIBED UNDER THE INVESTMENT COMPANY ACT OF 1940

■ 11. The authority citation for part 274 is revised to read as follows:

Authority: 15 U.S.C. 77f, 77g, 77h, 77j, 77s, 78c(b), 78*l*, 78m, 78n, 78o(d), 80a–8, 80a–24, 80a–26, 80a–29, 80a–37, otherwise noted.

■ 12. Amend Form N–1A (referenced in §§ 239.15A and 274.11A) by revising General Instruction C.3.(g)(i) and (ii), and adding Item 10(a)(4). The revisions read as follows:

Note: The text of Form N–1A does not, and these amendments will not, appear in the *Code of Federal Regulations.*

Form N–1A

* * * * *

General Instructions

* * * * *

C. Preparation of the Registration Statement

* * * * *

3. * * *

* * * * *

(g) Interactive Data File

(i) An Interactive Data File (rule 232.11 of Regulation S–T [17 CFR 232.11]) is required to be submitted to the Commission in the manner provided by rule 405 of Regulation S–T [17 CFR 232.405] for any registration statement or post-effective amendment thereto on Form N–1A that includes or amends information provided in response to Items 2, 3, 4, or 10(a)(4).

* * * * *

(ii) An Interactive Data File is required to be submitted to the Commission in the manner provided by rule 405 of Regulation S–T for any form of prospectus filed pursuant to paragraphs (c) or (e) of rule 497 under the Securities Act [17 CFR 230.497(c) or (e)] that includes information provided in response to Items 2, 3, 4, or 10(a)(4) that varies from the registration statement. All interactive data must be submitted with the filing made pursuant to rule 497.

* * * * *

Part A—INFORMATION REQUIRED IN A PROSPECTUS

* * * * *

Item 10. Management, Organization, and Capital Structure

* * * * *

(4) *Significant Fund Cybersecurity Incidents.* Provide a description of any significant fund cybersecurity incident as defined by rule 38a–2 of the Investment Company Act (17 CFR 270.38a–2) that has or is currently affecting the Fund or its service providers.

Instructions

1. The disclosure must include all significant fund cybersecurity incidents that have occurred within the last 2 fiscal years, as well as any currently ongoing.

2. The description of each incident must include the following information to the extent known: The entity or entities affected; when the incident was discovered and whether it is ongoing; whether any data was stolen, altered, or accessed or used for any other unauthorized purpose; the effect of the incident on the Fund's operations; and whether the Fund or service provider has remediated or is currently remediating the incident.

* * * * *

■ 13. Amend Form N–2 (referenced in §§ 239.14 and 274.11a–1) by revising General Instruction I.2 and 3, Item 13 is to read as follows:

Note: The text of Form N–2 does not, and these amendments will not, appear in the *Code of Federal Regulations.*

Form N–2

* * * * *

General Instructions

* * * * *

I. Interactive Data

* * * * *

2. An Interactive Data File is required to be submitted to the Commission in

the manner provided by Rule 405 of Regulation S–T for any registration statement or post-effective amendment thereto filed on Form N–2 or for any form of prospectus filed pursuant to Rule 424 under the Securities Act [17 CFR 230.424] that includes or amends information provided in response to Items 3.1, 4.3, 8.2.b, 8.2.d, 8.3.a, 8.3.b, 8.5.b, 8.5.c, 8.5.e, 10.1.a–d, 10.2.a–c, 10.2.e, 10.3, 10.5, or 13. The Interactive Data File must be submitted either with the filing, or as an amendment to the registration statement to which it relates, on or before the date the registration statement or post-effective amendment that contains the related information becomes effective. Interactive Data Files must be submitted with the filing made pursuant to Rule 424.

3. If a Registrant is filing a registration statement pursuant to General Instruction A.2, an Interactive Data File is required to be submitted to the Commission in the manner provided by Rule 405 of Regulation S–T for any of the documents listed in General Instruction F.3.(a) or General Instruction F.3.(b) that include or amend information provided in response to Items 3.1, 4.3, 8.2.b, 8.2.d, 8.3.a, 8.3.b, 8.5.b, 8.5.c, 8.5.e, 10.1.a–d, 10.2.a–c, 10.2.e, 10.3, 10.5, or 13. All interactive data must be submitted with the filing of the document(s) listed in General Instruction F.3.(a) or General Instruction F.3.(b).

* * * * *

Part A—INFORMATION REQUIRED IN A PROSPECTUS

* * * * *

Item 13. Significant Fund Cybersecurity Incidents

Provide a description of any significant fund cybersecurity incident as defined by rule 38a–2 of the Investment Company Act (17 CFR 270.38a–2) that has or is currently affecting the Registrant, any subsidiary of the Registrant, or the Registrant's service providers.

Instructions.

1. The disclosure must include all significant fund cybersecurity incidents that have occurred within the last 2 fiscal years, as well as any currently ongoing.

2. The description of each incident must include the following information to the extent known: The entity or entities affected; when the incident was discovered and whether it is ongoing; whether any data was stolen, altered, or accessed or used for any other unauthorized purpose; the effect of the incident on the Registrant's operations; and whether the Registrant, any subsidiary of the Registrant, or any service provider of the Registrant has remediated or is currently remediating the incident.

■ 14. Amend Form N–3 (referenced in §§ 239.17a and 274.11b) by revising General Instruction C.3(h)(i) and (ii) and adding new Item 16A to reads as follows:

Note: The text of Form N–3 does not, and these amendments will not, appear in the *Code of Federal Regulations.*

Form N–3

* * * * *

GENERAL INSTRUCTIONS

* * * * *

C. Preparation of the Registration Statement

* * * * *

3. Additional Matters

* * * * *

(h) *Interactive Data*

(i) An Interactive Data File (see rule 232.11 of Regulation S–T [17 CFR 232.11]) is required to be submitted to the Commission in the manner provided by rule 405 of Regulation S–T [17 CFR 232.405] for any registration statement or post-effective amendment thereto on Form N–3 that includes or amends information provided in response to Items 2, 4, 5, 11, 16A, 18, or 19 with regards to Contracts that are being sold to new investors.

* * * * *

(ii) An Interactive Data File is required to be submitted to the Commission in the manner provided by rule 405 of Regulation S–T for any form of prospectus filed pursuant to paragraphs (c) or (e) of rule 497 under the Securities Act [17 CFR 230.497(c) or (e)] that includes information provided in response to Items 2, 4, 5, 11, 16A, 18 or 19 that varies from the registration statement with regards to Contracts that are being sold to new investors. All interactive data must be submitted with the filing made pursuant to rule 497.

* * * * *

PART A—INFORMATION REQUIRED IN A PROSPECTUS

* * * * *

Item 16A. Significant Fund Cybersecurity Incidents

Provide a description of any significant fund cybersecurity incident as defined by rule 38a–2 of the Investment Company Act (17 CFR 270.38a–2) that has or is currently affecting the Registrant, Insurance Company or the Registrant's service providers.

Instructions.

1. The disclosure must include all significant fund cybersecurity incidents that have occurred within the last 2 fiscal years, as well as any currently ongoing.

2. The description of each incident must include the following information to the extent known: The entity or entities affected; when the incident was discovered and whether it is ongoing; whether any data was stolen, altered, or accessed or used for any other unauthorized purpose; the effect of the incident on the Registrant's operations; and whether the Registrant, Insurance Company, or any service provider of the Registrant has remediated or is currently remediating the incident.

* * * * *

■ 15. Amend Form N–4 (referenced in §§ 239.17b and 274.11c) by revising General Instruction C.3(h)(i) and (ii) and adding new Item 16A to read as follows:

Note: The text of Form N–4 does not, and these amendments will not, appear in the *Code of Federal Regulations.*

Form N–4

* * * * *

GENERAL INSTRUCTIONS

* * * * *

C. Preparation of the Registration Statement

* * * * *

3. Additional Matters

* * * * *

(h) Interactive Data

(i) An Interactive Data File (see rule 232.11 of Regulation S–T [17 CFR 232.11]) is required to be submitted to the Commission in the manner provided by rule 405 of Regulation S–T [17 CFR 232.405] for any registration statement or post-effective amendment thereto on Form N–4 that includes or amends information provided in response to Items 2, 4, 5, 10, 16A, or 17 with regards to Contracts that are being sold to new investors.

* * * * *

(ii) An Interactive Data File is required to be submitted to the Commission in the manner provided by rule 405 of Regulation S–T for any form of prospectus filed pursuant to paragraphs (c) or (e) of rule 497 under the Securities Act [17 CFR 230.497(c) or (e)] that includes information provided in response to Items 2, 4, 5, 10, 16A, or 17 that varies from the registration

statement with regards to Contracts that are being sold to new investors. All interactive data must be submitted with the filing made pursuant to rule 497.

* * * * *

PART A—INFORMATION REQUIRED IN A PROSPECTUS

* * * * *

Item 16A. Significant Fund Cybersecurity Incidents

Provide a description of any significant fund cybersecurity incident as defined by rule 38a–2 of the Investment Company Act (17 CFR 270.38a–2) that has or is currently affecting the Registrant, Depositor, or the Registrant's service providers.

Instructions.

1. The disclosure must include all significant fund cybersecurity incidents that have occurred within the last 2 fiscal years, as well as any currently ongoing.

2. The description of each incident must include the following information to the extent known: The entity or entities affected; when the incident was discovered and whether it is ongoing; whether any data was stolen, altered, or accessed or used for any other unauthorized purpose; the effect of the incident on the Registrant's operations; and whether the Registrant, Depositor, or any service provider of the Registrant has remediated or is currently remediating the incident.

* * * * *

■ 16. Amend Form N–6 (referenced in §§ 239.17c and 274.11d) by revising General Instruction C.3(h)(i) and (ii) and adding new Item 16A to read as follows:

Note: The text of Form N–6 does not, and these amendments will not, appear in the *Code of Federal Regulations.*

Form N–6

* * * * *

GENERAL INSTRUCTIONS

* * * * *

C. Preparation of the Registration Statement

* * * * *

3. Additional Matters

* * * * *

(h) Interactive Data

(i) An Interactive Data File (see rule 232.11 of Regulation S–T [17 CFR 232.11]) is required to be submitted to the Commission in the manner provided by rule 405 of Regulation S–T [17 CFR 232.405] for any registration statement or post-effective amendment thereto on Form N–6 that includes or amends information provided in response to Items 2, 4, 5, 10, 11, 16A, or 18 with regards to Contracts that are being sold to new investors.

* * * * *

(ii) An Interactive Data File is required to be submitted to the Commission in the manner provided by rule 405 of Regulation S–T for any form of prospectus filed pursuant to paragraphs (c) or (e) of rule 497 under the Securities Act [17 CFR 230.497(c) or (e)] that includes information provided in response to Items 2, 4, 5, 10, 11, 16A, or 18 that varies from the registration statement with regards to Contracts that are being sold to new investors. All interactive data must be submitted with the filing made pursuant to rule 497.

* * * * *

PART A—INFORMATION REQUIRED IN A PROSPECTUS

* * * * *

Item 16A. Significant Fund Cybersecurity Incidents

Provide a description of any significant fund cybersecurity incident as defined by rule 38a–2 of the Investment Company Act (17 CFR 270.38a–2) that has or is currently affecting the Registrant, the Depositor or the Registrant's service providers.

Instructions.

1. The disclosure must include all significant fund cybersecurity incidents that have occurred within the last 2 fiscal years, as well as any currently ongoing.

2. The description of each incident must include the following information to the extent known: The entity or entities affected; when the incident was discovered and whether it is ongoing; whether any data was stolen, altered, or accessed or used for any other unauthorized purpose; the effect of the incident on the Registrant's operations; and whether the Registrant, Depositor, or any service provider of the Registrant has remediated or is currently remediating the incident.

■ 17. Amend Form N–8B–2 (referenced in § 274.12) by adding new General Instruction 2.(*l*) and new Item 9A to read as follows:

Note: The text of Form N–8B–2 does not, and these amendments will not, appear in the *Code of Federal Regulations.*

FORM N–8B–2

* * * * *

GENERAL INSTRUCTIONS FOR FORM N–8B–2

* * * * *

2. Preparation and Filing of Registration Statement

* * * * *

(l) Interactive Data

(1) An Interactive Data File as defined in rule 11 of Regulation S–T [17 CFR 232.11] is required to be submitted to the Commission in the manner provided by rule 405 of Regulation S–T [17 CFR 232.405] for any registration statement on Form N–8B–2 that includes information provided in response to Item 9A pursuant to Instruction 2. The Interactive Data File must be submitted with the filing to which it relates on the date such filing becomes effective.

(2) All interactive data must be submitted in accordance with the specifications in the EDGAR Filer Manual.

* * * * *

I. ORGANIZATION AND GENERAL INFORMATION

* * * * *

9A. Provide a description of any significant fund cybersecurity incident as defined by rule 38a–2 of the Investment Company Act of 1940 (17 CFR 270.38a–2) that has or is currently affecting the trust, the depositor, or the trust's service providers.

Instructions:

(a) The disclosure must include all significant fund cybersecurity incidents that have occurred within the last 2 fiscal years, as well as any currently ongoing.

(b) The description of each incident must include the following information to the extent known: the entity or entities affected; when the incident was discovered and whether it is ongoing; whether any data was stolen, altered, or accessed or used for any other unauthorized purpose; the effect of the incident on the trust's operations; and whether the trust, the depositor, or any service provider of the trust has remediated or is currently remediating the incident.

* * * * *

PART 275—RULES AND REGULATIONS, INVESTMENT ADVISERS ACT OF 1940

■ 18. The authority citation for part 275 continues to read, in part, as follows:

Authority: 15 U.S.C. 80b–2(a)(11)(G), 80b–2(a)(11)(H), 80b–2(a)(17), 80b–3, 80b–4, 80b–4a, 80b–6(4), 80b–6a, and 80b–11, unless otherwise noted.

* * * * *

Section 275.204–2 is also issued under 15 U.S.C. 80b–6.

* * * * *

■ 19. Amend § 275.204–2 by:

■ a. Revising paragraph (a)(17)(i);

■ b. Removing the period at the end of paragraph (a)(17)(iii) and adding a semicolon in its place; and

■ c. Adding paragraphs (a)(17)(iv) through (vii).

The additions read as follows:

§ 275.204–2 Books and records to be maintained by investment advisers.

(a) * * *

(17) * * *

(i) A copy of the investment adviser's policies and procedures formulated pursuant to §§ 275.206(4)–7(a) and 275.206(4)–9 that are in effect, or at any time within the past five years were in effect;

* * * * *

(iv) A copy of the investment adviser's written report documenting the investment adviser's annual review of the cybersecurity policies and procedures conducted pursuant to § 275.206(4)–9(b) in the last five years;

(v) A copy of any Form ADV–C, and amendments filed by the adviser under § 275.204–6 in the last five years;

(vi) Records documenting the occurrence of any cybersecurity incident, as defined in § 275.206(4)–9(c), occurring in the last five years, including records related to any response and recovery from such an incident; and

(vii) Records documenting any risk assessment conducted pursuant to the cybersecurity policies and procedures required by § 275.206(4)–9(a)(1) in the last five years.

* * * * *

■ 20. Amend § 275.204–3 by revising paragraph (b)(4) to read as follows:

§ 275.204–3 Delivery of brochures and brochure supplements.

* * * * *

(b) * * *

(4) Deliver the following to each client promptly after you create an amended brochure or brochure supplement, as applicable, if the amendment adds disclosure of an event or incident, or materially revises information already disclosed about an event or incident: in response to Item 9 of Part 2A of Form ADV or Item 3 of Part 2B of Form ADV (Disciplinary Information), or Item 20.B of Part 2A of Form ADV (Cybersecurity Risks and Incidents);

(i) The amended brochure or brochure supplement, as applicable, along with a statement describing the material facts relating to the change in disciplinary information or information about a significant cybersecurity incident; or

(ii) A statement describing the material facts relating to the change in disciplinary information or information about a significant cybersecurity incident.

* * * * *

■ 21. Section 275.204–6 is added to read as follows:

§ 275.204–6 Cybersecurity incident reporting.

(a) Every investment adviser registered or required to be registered under section 203 of the Act (15 U.S.C. 80b–3) shall:

(1) Report to the Commission any significant adviser cybersecurity incident or significant fund cybersecurity incident, promptly, but in no event more than 48 hours, after having a reasonable basis to conclude that any such incident has occurred or is occurring by filing Form ADV–C electronically on the Investment Adviser Registration Depository (IARD).

(2) Amend any previously filed Form ADV–C promptly, but in no event more than 48 hours after:

(i) Any information previously reported to the Commission on Form ADV–C pertaining to a significant adviser cybersecurity incident or a significant fund cybersecurity becoming materially inaccurate;

(ii) Any new material information pertaining to a significant adviser cybersecurity incident or a significant fund cybersecurity incident previously reported to the Commission on Form ADV–C being discovered; or

(iii) Any significant adviser cybersecurity incident or significant fund cybersecurity incident being resolved or any internal investigation pertaining to such an incident being closed.

(b) For the purposes of this section:

Adviser information and *cybersecurity incident* have the same meanings as in § 275.206(4)–9 (Rule 206(4)–9 under the Investment Advisers Act of 1940).

Significant adviser cybersecurity incident means a cybersecurity incident, or a group of related cybersecurity incidents, that significantly disrupts or degrades the adviser's ability, or the ability of a private fund client of the adviser, to maintain critical operations, or leads to the unauthorized access or use of adviser information, where the unauthorized access or use of such information results in:

(i) Substantial harm to the adviser; or

(ii) Substantial harm to a client, or an investor in a private fund, whose information was accessed.

Significant fund cybersecurity incident has the same meaning as in § 270.38a–2 of this chapter (Rule 38a–2 under the Investment Company Act of 1940).

■ 22. Section 275.206(4)–9 is added to read as follows:

§ 275.206(4)–9 Cybersecurity policies and procedures of investment advisers.

(a) *Cybersecurity policies and procedures.* As a means reasonably designed to prevent fraudulent, deceptive, or manipulative acts, practices, or courses of business within the meaning of section 206(4) of the Act (15 U.S.C. 80b6(4)), it is unlawful for any investment adviser registered or required to be registered under section 203 of the Investment Advisers Act of 1940 (15 U.S.C. 80b–3) to provide investment advice to clients unless the adviser adopts and implements written policies and procedures that are reasonably designed to address the adviser's cybersecurity risks, including policies and procedures that:

(1) *Risk assessment.*

(i) Require periodic assessments of cybersecurity risks associated with adviser information systems and adviser information residing therein, including requiring the adviser to:

(A) Categorize and prioritize cybersecurity risks based on an inventory of the components of the adviser information systems and adviser information residing therein and the potential effect of a cybersecurity incident on the adviser; and

(B) Identify the adviser's service providers that receive, maintain, or process adviser information, or are otherwise permitted to access adviser information systems and any adviser information residing therein, and assess the cybersecurity risks associated with the adviser's use of these service providers.

(ii) Require written documentation of any risk assessments.

(2) *User security and access.* Require controls designed to minimize user-related risks and prevent unauthorized access to adviser information systems and adviser information residing therein, including:

(i) Requiring standards of behavior for individuals authorized to access adviser information systems and any adviser information residing therein, such as an acceptable use policy;

(ii) Identifying and authenticating individual users, including implementing authentication measures that require users to present a combination of two or more credentials for access verification;

(iii) Establishing procedures for the timely distribution, replacement, and revocation of passwords or methods of authentication;

(iv) Restricting access to specific adviser information systems or components thereof and adviser information residing therein solely to individuals requiring access to such systems and information as is necessary for them to perform their responsibilities and functions on behalf of the adviser; and

(v) Securing remote access technologies.

(3) *Information protection.*

(i) Require measures designed to monitor adviser information systems and protect adviser information from unauthorized access or use, based on a periodic assessment of the adviser information systems and adviser information that resides on the systems that takes into account:

(A) The sensitivity level and importance of adviser information to its business operations;

(B) Whether any adviser information is personal information;

(C) Where and how adviser information is accessed, stored and transmitted, including the monitoring of adviser information in transmission;

(D) Adviser information systems access controls and malware protection; and

(E) The potential effect a cybersecurity incident involving adviser information could have on the adviser and its clients, including the ability for the adviser to continue to provide investment advice.

(ii) Require oversight of service providers that receive, maintain, or process adviser information, or are otherwise permitted to access adviser information systems and any adviser information residing therein and through that oversight document that such service providers, pursuant to a written contract between the adviser and any such service provider, are required to implement and maintain appropriate measures, including the practices described in paragraphs (a)(1), (2), (3)(i), (4), and (5) of this section, that are designed to protect adviser information and adviser information systems.

(4) *Cybersecurity threat and vulnerability management.* Require measures to detect, mitigate, and remediate any cybersecurity threats and vulnerabilities with respect to adviser information systems and the adviser information residing therein;

(5) *Cybersecurity incident response and recovery.*

(i) Require measures to detect, respond to, and recover from a cybersecurity incident, including policies and procedures that are reasonably designed to ensure:

(A) Continued operations of the adviser;

(B) The protection of adviser information systems and the adviser information residing therein;

(C) External and internal cybersecurity incident information sharing and communications; and

(D) Reporting of significant cybersecurity incidents under § 275.204–6 (Rule 204–6).

(ii) Require written documentation of any cybersecurity incident, including the adviser's response to and recovery from such an incident.

(b) *Annual review.* An adviser must, at least annually:

(1) Review and assess the design and effectiveness of the cybersecurity policies and procedures required by paragraph (a) of this section, including whether they reflect changes in cybersecurity risk over the time period covered by the review; and

(2) Prepare a written report that, at a minimum, 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) *Definitions.* For purposes of this section:

Adviser information means any electronic information related to the adviser's business, including personal information, received, maintained, created, or processed by the adviser.

Adviser information systems means the information resources owned or used by the adviser, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of adviser information to maintain or support the adviser's operations.

Cybersecurity incident means an unauthorized occurrence on or conducted through an adviser's information systems that jeopardizes the confidentiality, integrity, or availability of an adviser's information systems or any adviser information residing therein.

Cybersecurity risk means financial, operational, legal, reputational, and other consequences that could result from cybersecurity incidents, threats, and vulnerabilities.

Cybersecurity threat means any potential occurrence that may result in an unauthorized effort to adversely affect the confidentiality, integrity, or availability of an adviser's information systems or any adviser information residing therein.

Cybersecurity vulnerability means a vulnerability in an adviser's information systems, information system security procedures, or internal controls, including vulnerabilities in their design, configuration, maintenance, or implementation that, if exploited, could result in a cybersecurity incident.

Personal information means:

(i) Any information that can be used, alone or in conjunction with any other information, to identify an individual, such as name, date of birth, place of birth, telephone number, street address, mother's maiden name, Social Security number, driver's license number, electronic mail address, account number, account password, biometric records or other nonpublic authentication information; or

(ii) Any other non-public information regarding a client's account.

PART 279—FORMS PRESCRIBED UNDER THE INVESTMENT ADVISERS ACT OF 1940

■ 23. The authority citation for part 279 continues to read as follows:

Authority: The Investment Advisers Act of 1940, 15 U.S.C. 80b–1 *et seq.,* Pub. L. 111203, 124 Stat. 1376.

■ 24. Amend Form ADV (referenced in § 279.1) by:

■ a. Adding Item 20 to Part 2A; and

■ b. Revising the instructions to the form, in the section entitled ''Form ADV: Glossary of Terms.''

The addition and revision read as follows:

Note: The text of Form ADV does not, and this amendment will not, appear in the *Code of Federal Regulations.*

FORM ADV (Paper Version)

UNIFORM APPLICATION FOR INVESTMENT ADVISER REGISTRATION

PART 2: Uniform Requirements for the Investment Adviser Brochure and Brochure Supplements

* * * * *

Item 20. Cybersecurity Risks and Incidents

A. *Risks.* Describe the *cybersecurity risks* that could materially affect the advisory services you offer. Describe how you assess, prioritize, and address cybersecurity risks created by the nature and scope of your business.

B. *Incidents.* Provide a description of any *cybersecurity incident* that that has occurred within the last two fiscal years that has significantly disrupted or degraded your ability to maintain

critical operations, or has led to the unauthorized access or use of *adviser information,* resulting in substantial harm to you or your clients. The description of each incident must include the following information to the extent known: The entity or entities affected; when the incident was discovered and whether it is ongoing; whether any data was stolen, altered or accessed or used for any other unauthorized purpose; the effect of the incident on the adviser's operations; and whether the adviser, or service provider, has remediated or is currently remediating the incident.

* * * * *

APPENDIX B: FORM ADV GLOSSARY OF TERMS

Adviser information means any electronic information related to the adviser's business, including personal information, received, maintained, created, or processed by the adviser.

Adviser information systems means the adviser information resources owned or used by the adviser, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of adviser information to maintain or support the adviser's operations.

Cybersecurity incident means an unauthorized occurrence on or conducted through an adviser's information systems that jeopardizes the confidentiality, integrity, or availability of an adviser's information systems or any adviser information residing therein.

Cybersecurity risk means financial, operational, legal, reputational, and other consequences that could result from cybersecurity incidents, threats, and vulnerabilities.

Cybersecurity threat means any potential occurrence that may result in an unauthorized effort to adversely affect the confidentiality, integrity, or availability of an adviser's information systems or any adviser information residing therein.

Cybersecurity vulnerability means a vulnerability in an adviser's information systems, information system security procedures, or internal controls, including vulnerabilities in their design, configuration, maintenance, or implementation that, if exploited, could result in a cybersecurity incident.

Personal information means:

(1) Any information that can be used, alone or in conjunction with any other information, to identify an individual, such as name, date of birth, place of birth, telephone number, street address, mother's maiden name, Social Security number, driver's license number, electronic mail address, account number, account password, biometric records or other nonpublic authentication information; or

(2) Any other non-public information regarding a client's account.

* * * * *

■ 25. Section 279.10 is added to read as follows:

§ 279.10 Form ADV–C, investment adviser cybersecurity incident reporting.

This form shall be filed pursuant to § 275.204–6 of this chapter (Rule 204–6) by investment advisers registered or required to register under section 203 of the Act (15 U.S.C. 80b–3).

By the Commission.

Dated: February 9, 2022.

Vanessa A. Countryman,

Secretary.

Note: The following appendix will not, appear in the *Code of Federal Regulations.*

FORM ADV–C

INVESTMENT ADVISER CYBERSECURITY INCIDENT REPORT PURSUANT TO RULE 204–6 [17 CFR 275.206(4)–6]

You must submit this Form ADV–C if you are registered with the Commission as an investment adviser within 48 hours after having a reasonable basis to conclude that a *significant adviser cybersecurity incident* or a *significant fund cybersecurity incident* (collectively, ''*significant cybersecurity incident*'') has occurred or is occurring in accordance with rule 204–6 under the Investment Advisers Act of 1940.

Check the box that indicates what you would like to do (check all that apply):

○ Submit an initial report for a significant cybersecurity incident.

○ Submit an amended report for a significant cybersecurity incident.

○ Submit a final amended report for a significant cybersecurity incident.

(1) Investment Advisers Act SEC File Number: 801-

(2) Your full legal name of investment adviser (if you are a sole proprietor, state last, first, middle name):

(3) Name under which your primarily conduct your advisory business, if different from above:

(4) Address of principal place of business (number, street, city, state, zip code):

(5) Contact information for an individual with respect to the *significant cybersecurity incident* being reported: (Name, title, address if different from above, phone, email address)

(6) Adviser reporting a:

☐ *Significant adviser cybersecurity incident*

(a) If so, does the *significant adviser cybersecurity incident* involve any *private funds*?

☐ Yes

☐ No

(1) If yes, list the *private fund ID number(s)*

☐ *Significant fund cybersecurity incident*

(b) If so, list each investment company registered under the Investment Company Act of 1940 or company that has elected to be a business development company pursuant to section 54 of that Act involved and their SEC file number(s) (811 or 814 number) and the series ID number of the specific fund if more than one series under the SEC file number.

(7) Approximate date(s) the *significant cybersecurity incident* occurred, if known:

(8) Approximate date the *significant cybersecurity incident* was discovered:

(9) Is the *significant cybersecurity incident* ongoing?

☐ Yes

☐ No

(a) If not, approximate date the *significant cybersecurity incident* was resolved or any internal investigation pertaining to such incident was closed.

(10) Has law enforcement or a government agency (other than the Commission) been notified about the *significant cybersecurity incident*?

☐ Yes

☐ No

(a) If yes, which law enforcement or government agencies have been notified?

(11) Describe the nature and scope of the *significant cybersecurity incident,* including any effect on the relevant entity's critical operations:

(12) Describe the actions taken or planned to respond to and recover from the *significant cybersecurity* incident:

(13) Was any data was stolen, altered, or accessed or used for any other unauthorized purpose?

☐ Yes

☐ No

☐ Unknown

(a) If yes, describe the nature and scope of such information, including whether it was *adviser information* or *fund information.*

(14) Was any *personal information* lost, stolen, modified, deleted,

destroyed, or accessed without authorization as a result of the *significant cybersecurity incident*?

☐ Yes
☐ No
☐ Unknown

(a) If yes, describe the nature and scope of such information.

(b) If yes, has notification been provided to persons whose *personal information* was lost, stolen, damaged, or accessed without authorization?

☐ Yes
☐ No

(i) If not, are such notifications planned?

☐ Yes
☐ No

(15) Has disclosure about the *significant cybersecurity incident* been made to the adviser's clients and/or to investors in any investment company registered under the Investment Company Act of 1940 or company that has elected to be a business development company pursuant to section 54 of that Act, or *private funds* advised by the adviser involved?

☐ Yes
☐ No

(a) If yes, when was such disclosure made?

(b) If not, explain why such disclosure has not be made?

(16) Is the *significant cybersecurity incident* covered under a cybersecurity insurance policy maintained by you or any investment company registered under the Investment Company Act of 1940 or company that has elected to be a business development company pursuant to section 54 of that Act, or any private fund?

☐ Yes
☐ No
☐ Unknown

(a) If yes, has the insurance company issuing the cybersecurity insurance policy been contacted about the significant cybersecurity incident?

☐ Yes
☐ No

Definitions

For the purposes of this Form:

Adviser information and *adviser information systems* have the same meanings as in rule 206(4)–9 under the Investment Advisers Act of 1940.

Fund information, fund information systems, and *significant fund cybersecurity incident* have the same meaning as in rule 38a–2 under the Investment Company Act of 1940.

Private fund has the same meaning as in section 202(a)(29) of the Investment Advisers Act of 1940.

Personal information has the same meaning in rule 206(4)–9 under the Advisers Act of 1940 or rule 38a–2 under the Investment Company Act of 1940, as applicable.

Significant adviser cybersecurity incident has the meaning as in rule 204–6 under the Advisers Act of 1940.

[FR Doc. 2022–03145 Filed 3–8–22; 8:45 am]

BILLING CODE 8011–01–P