Additionally, please include the Docket ID at the top of your comments.

*Federal eRulemaking Portal:* Go to *www.regulations.gov* to submit your comments electronically. Information on how to use *Regulations.gov,* including instructions for accessing agency documents, submitting comments, and viewing the docket, is available on the site under ''FAQ'' (*https://www.regulations.gov/faq*).

*Privacy Note:* OSTP's policy is to make all comments received from members of the public available for public viewing in their entirety on the Federal eRulemaking Portal at *www.regulations.gov.* Therefore, commenters should be careful to include in their comments only information that they wish to make publicly available. OSTP requests that no proprietary information, copyrighted information, or personally identifiable information be submitted in response to this RFI.

*Instructions:* Response to this RFI is voluntary. Respondents need not reply to all questions listed. For all submissions, clearly indicate which questions are being answered. Multiple submissions from an individual, group, or institution will be considered as supplements to the original response and not as new comments. Submissions should include the name(s) of the person(s) or organization(s) filing the comment.

Any information obtained from this RFI is intended to be used by the Government on a non-attribution basis for planning and strategy development. OSTP will not respond to individual submissions. A response to this RFI will not be viewed as a binding commitment to develop or pursue the project or ideas discussed. This RFI is not accepting applications for financial assistance or financial incentives. Please note that the United States Government will not pay for response preparation, or for the use of any information contained in a response.

**FOR FURTHER INFORMATION CONTACT:** Rhema Bjorkland at *info@nnco.nano.gov* or 202–517–1050. Individuals who use telecommunication devices for the deaf and hard of hearing (TDD) may call the Federal Relay Service (FRS) at 1–800–877–8339, 24 hours a day, every day of the year, including holidays.

**SUPPLEMENTARY INFORMATION:**

*Background Information:* NEHI, on behalf of the NNI, is engaging the community early in the process to allow the public and key stakeholders to inform revisions to the NNI EHS research strategy. In preparing comments, the public is invited to view the core research areas and their associated needs as set out in the NNI 2011 Environmental, Health, and Safety (EHS) Research Strategy (*https://www.nano.gov/2011EHSStrategy*). The 2014 Progress Review on the Coordinated Implementation of the National Nanotechnology Initiative 2011 Environmental, Health, and Safety Research Strategy (*https://www.nano.gov/2014-EHS-Progress-Review*) and 2017 Highlights of Recent Research on the Environmental, Health, and Safety Implications of Engineered Nanomaterials (*https://www.nano.gov/Highlights-Federal-NanoEHS-Report*) provide additional information on the progress made in the core research areas.

*Information Requested:* Pursuant to 42 U.S.C. 6617, OSTP is soliciting public input through an RFI to obtain feedback from a wide variety of stakeholders, including individuals, industry, academia, research laboratories, nonprofits, and think tanks. OSTP is interested in public input to inform an updated nanotechnology EHS research strategy, specifically a strategy that focuses on the use of science-based risk analysis and risk management to protect public health and the environment while also fostering the technological advancements that benefit society. OSTP seeks responses to any or all of the following questions:

1. What are the research accomplishments in the following six core research areas identified in the 2011 NNI EHS Strategy? The six core research areas are (1) Nanomaterial Measurement Infrastructure, (2) Human Exposure Assessment, (3) Human Health, (4) Environment, (5) Risk Assessment and Risk Management Methods, and (6) Informatics and Modeling.

2. What research gaps remain in addressing the six NNI EHS core research areas listed in question 1?

3. The ethical, legal, and societal implications (ELSI) of nanotechnology are considered across the core research areas of the 2011 strategy. What additional ways could ELSI be more fully integrated throughout a refreshed NNI EHS research strategy?

4. What broad themes should the revised strategy adopt to integrate and connect the six research areas?

5. How should the updated NNI EHS research strategy reflect the evolution of nanotechnology beyond engineered nanomaterials to complex systems, structures, and devices?

6. The 2011 strategy focused on engineered nanomaterials and did not include incidental nanoscale materials such as nanoplastics and certain nanoscale particulate emissions such as those from 3D printing. If the updated strategy is revised to include some non-engineered or incidental nanomaterials, describe how to scope the strategy in a way that complements rather than being redundant with existing health and environmental research (*e.g.,* by excluding the large body of existing research on air pollution, which can include nanoscale particles).

Dated: March 31, 2023.

**Stacy Murphy,**

*Deputy Chief Operations Officer/Security Officer.*

[FR Doc. 2023–07074 Filed 4–4–23; 8:45 am]

**BILLING CODE 3270–F1–P**

## SECURITIES AND EXCHANGE COMMISSION

**[Release No. 34–97225; File No. SR–OCC–2023–003]**

## Self-Regulatory Organizations; The Options Clearing Corporation; Notice of Filing of Proposed Rule Change by The Options Clearing Corporation Concerning Clearing Member Cybersecurity Obligations

March 30, 2023.

Pursuant to Section 19(b)(1) of the Securities Exchange Act of 1934 (''Exchange Act'' or ''Act''),[1] and Rule 19b–4 thereunder,[2] notice is hereby given that on March 21, 2023, The Options Clearing Corporation (''OCC'' or ''Corporation'') filed with the Securities and Exchange Commission (''SEC'' or ''Commission'') the proposed rule change as described in Items I, II, and III below, which Items have been prepared primarily by OCC. The Commission is publishing this notice to solicit comments on the proposed rule change from interested persons.

### I. Clearing Agency's Statement of the Terms of Substance of the Proposed Rule Change

The proposed rule change would amend certain provisions in OCC's Rules relating to Clearing Member cybersecurity obligations to address the occurrence of a cyber-related disruption or intrusion of a Clearing Member (''Security Incident''). The proposed changes would (i) require a Clearing Member to immediately notify OCC of a Security Incident; (ii) memorialize OCC's ability to take actions reasonably necessary to mitigate any effects to its operations; and (iii) require such

[1] 15 U.S.C. 78s(b)(1).

[2] 17 CFR 240.19b–4.

Clearing Member to provide a form containing written representations addressing the incident and attesting to certain security requirements (''Reconnection Attestation'') and an associated checklist describing remediation efforts (''Reconnection Checklist'' and together, ''Reconnection Attestation and Checklist'').

The proposed changes to OCC's Rules are included as Exhibit 5 to File No. SR–OCC–2023–003. Material proposed to be added to the Rules as currently in effect is underlined and material proposed to be deleted is marked in strikethrough text. All capitalized terms not defined herein have the same meaning as set forth in the OCC By-Laws and Rules.[3]

## II. Clearing Agency's Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change

In its filing with the Commission, OCC included statements concerning the purpose of and basis for the proposed rule change and discussed any comments it received on the proposed rule change. The text of these statements may be examined at the places specified in Item IV below. OCC has prepared summaries, set forth in sections (A), (B), and (C) below, of the most significant aspects of these statements.

### *(A) Clearing Agency's Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change*

(1) Purpose

Overview

The proposed rule change would amend certain provisions in the Rules relating to Clearing Member cybersecurity obligations to address the occurrence of a Security Incident. The proposed changes would (i) require a Clearing Member to immediately notify OCC of a Security Incident; (ii) memorialize OCC's ability to take actions reasonably necessary to mitigate any effects to its operations; and (iii) require such Clearing Member to provide a Reconnection Attestation containing written representations addressing the incident and attesting to certain security requirements and an associated Reconnection Checklist describing remediation efforts. As described in more detail below, the proposed rule change is designed to help OCC assess and take appropriate action to manage the cybersecurity risks that may be introduced to OCC's information and data systems due to a Security Incident.

OCC believes it is prudent to implement a standardized approach to assess and manage the cybersecurity risks that OCC may face through its interconnections to Clearing Members. Cybersecurity incidents pose an ongoing risk to OCC, as well as market participants, as an attack on OCC can lead to the loss of data or system integrity, unauthorized disclosure of sensitive information, or an inability to conduct essential clearance and settlement functions. Moreover, as a designated systemically important financial market utility (''SIFMU''),[4] a failure or disruption to OCC could increase the risk of significant liquidity problems spreading among financial institutions or markets and thereby threaten the stability of the financial system in the United States. Given its designation as a SIFMU, OCC believes it is prudent to enhance its management of Security Incidents so that OCC's own information and data systems remain protected against cyberattacks.

The proposed rule change would amend certain provisions in the Rules relating to Clearing Member cybersecurity obligations to address the occurrence of a Security Incident. Clearing Member cybersecurity obligations are currently set out in Rule 219, which addresses requirements related to a firm's cybersecurity program. The proposed rule change would expand the scope of this Rule to incorporate provisions that address the occurrence of a Security Incident, as further described below. The current Clearing Member cybersecurity obligations in this Rule would remain unchanged.

The proposed changes would clearly describe Clearing Member obligations and OCC rights with respect to a Security Incident. The proposal would require Clearing Members to immediately notify OCC of a Security Incident. OCC's notification and reporting requirements for Clearing Members are currently set forth in various provisions of the By-Laws and the Rules and require, among other things, that Clearing Members provide OCC with such documents and information as OCC may require from time to time.[5] These existing notification and reporting requirements do not directly address Security Incidents. The proposal would amend OCC's notification and reporting requirements to adopt a specific requirement in the Rules that Clearing Members immediately notify OCC of a Security Incident and promptly confirm such notice in writing.

The proposed changes would also memorialize in the Rules OCC's ability to take actions reasonably necessary to mitigate any effects of a Security Incident to its operations. OCC's existing right to disconnect access, or to modify the scope and specifications of access, of a Clearing Member to OCC information and data systems is based in the Agreement for OCC Services, which sets forth the terms of various services that OCC may provide to Clearing Members.[6] OCC maintains various contracts and forms, including the Agreement for OCC Services, that in conjunction with OCC's By-Laws and Rules, establish and govern the relationship between OCC and each Clearing Member.[7] Pursuant to the Agreement for OCC Services, OCC may terminate electronic access to particular OCC information and data systems, or modify the scope and specifications of such access, from time to time. Codifying this ability of OCC to take actions reasonably necessary to mitigate any effects to its operations in the Rules would centralize relevant information pertaining to cybersecurity in the Rules.

The proposal would further implement a standardized approach to evaluate and manage the cybersecurity risks that OCC may face due to a Security Incident. The proposal would set out new procedures that would require a Clearing Member to submit, upon OCC's request, the Reconnection Attestation and Checklist after reporting a Security Incident, both as provided by OCC from time to time. The Rule is designed to provide OCC with a degree of flexibility in requesting the Reconnection Attestation and Checklist to consider circumstances where there may be no risk or threat to OCC, such as when a Security Incident is contained to a part of a Clearing Member's business with no relevance to OCC or its markets. The Reconnection Attestation and Checklist are designed to enable OCC to determine whether the risk or threat to OCC has been mitigated sufficiently, including whether to resume connectivity to a Clearing Member if connectivity was disconnected or modified. OCC would detail specific representations and information required of Clearing Members in the proposed Reconnection

[3] OCC's By-Laws and Rules can be found on OCC's public website: *https://www.theocc.com/Company-Information/Documents-and-Archives/By-Laws-and-Rules.*

[4] OCC was designated as a SIFMU under Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010. 12 U.S.C. 5465(e)(1).

[5] *See* Article V, Section 1, Interpretation and Policy .07 of the By-Laws and Rules 201(b), 215, 216, 217(b), 303, 306, 308 and 310(a)–(c).

[6] *See* Exchange Act Release No. 34–73577 (Nov. 12, 2014), 79 FR 68733 (Nov. 18, 2014) (File No. SR–OCC–2014–20).

[7] *Id.*

Attestation and Checklist, included in Exhibit 3 to File No. SR–OCC–2023–003. OCC believes an attestation-based format coupled with a checklist would be most effective in ascertaining a Clearing Member's response to a Security Incident, including whether the Clearing Member has appropriate security requirements and carried out suitable remediation measures, to determine any potential threats to OCC's information and data systems. The forms filter the requested information and representations into a standardized format, which would better enable OCC to review and identify areas of interest, concern, or heightened risk in respect of a Security Incident. Standardizing the form and contents of submissions would also improve efficiency for Clearing Members and OCC by reducing the potential uncertainty and time required to demonstrate an acceptable response to a Security Incident, which would facilitate OCC's ability to evaluate the potential risk or threat posed by the Security Incident and facilitate the resumption of Clearing Member connectivity.

Proposed Rule Changes

The proposed rule change would amend certain provisions in the Rules relating to Clearing Member cybersecurity obligations to address the occurrence of a Security Incident. In addition to expanding the scope of existing Rules, the proposed changes would (i) require a Clearing Member to immediately notify OCC of a Security Incident; (ii) memorialize OCC's ability to take actions reasonably necessary to mitigate any effects to its operations; and (iii) require such Clearing Member to provide a Reconnection Attestation and Checklist.

Amended Cybersecurity Obligations Provisions

The proposed changes would expand the scope of existing Rule 219 to address the occurrence of a Security Incident. Existing Rule 219, titled ''Cybersecurity Confirmation,'' currently includes requirements related to a firm's cybersecurity program and requires Clearing Members and applicants for clearing membership to submit a form, referred to as the ''Cybersecurity Confirmation,'' that confirms the existence of a cybersecurity program. To broaden the scope, OCC proposes to retitle this Rule from ''Cybersecurity Confirmation'' to ''Cybersecurity Obligations'' to address Security Incidents and centralize cybersecurity-related provisions in one section of the Rules. For clarity, OCC also proposes to add a heading to each paragraph in this Rule to summarize its content. OCC proposes to add the following headings: ''Cybersecurity Confirmation Submission'' to paragraph (a), which relates to the submission of the Cybersecurity Confirmation; ''Representations in the Cybersecurity Confirmation'' to paragraph (b), which relates to the representations in the Cybersecurity Confirmation; and ''Execution of the Cybersecurity Confirmation'' to paragraph (c), which relates to the execution of the Cybersecurity Confirmation. OCC also proposes a minor edit to replace ''OCC'' with ''the Corporation'' in paragraphs (a) and (b) for consistency. Additionally, under the proposed rule change, existing Rule 219 would be renumbered as Rule 213.[8]

Occurrence of a Security Incident

The proposed changes would address the occurrence of a Security Incident in the Rules by: (i) requiring a Clearing Member to immediately notify OCC of a Security Incident; (ii) memorializing OCC's ability to take actions reasonably necessary to mitigate any effects to its operations; and (iii) requiring such Clearing Member to provide a Reconnection Attestation and Checklist. Each of these proposed changes is described in greater detail below.

(i) Notification of a Security Incident

The proposed rule change would adopt a new paragraph (d) to amended Rule 213, titled ''Occurrence of a Security Incident,'' to address the occurrence of a Security Incident. Proposed Rule 213(d) would define Security Incident as a cyber-related disruption or intrusion of the Clearing Member, including, but not limited to, any disruption or degradation of the normal operation of the Clearing Member's systems or any unauthorized entry into the Clearing Member's systems. Proposed Rule 213(d) would require a Clearing Member to immediately notify OCC if there has been a Security Incident or if a Security Incident is occurring and to promptly confirm such notice in writing.

(ii) Memorialization of OCC's Ability To Take Action

Proposed paragraph (d) to amended Rule 213 would also memorialize OCC's ability to take actions reasonably necessary to mitigate any effects to its operations in the case of a Security Incident. The proposed language specifies that upon notice from a Clearing Member of a Security Incident, or if OCC has a reasonable basis to believe that a Security Incident has occurred, or is occurring, OCC may take actions reasonably necessary to mitigate any effects to its operations. Such actions would include the right to disconnect access, or to modify the scope and specifications of access, of the Clearing Member to OCC's information and data systems, consistent with the Agreement for OCC Services.

(iii) Requirement To Provide Reconnection Attestation and Checklist

The proposed rule change would adopt new paragraph (e) to amended Rule 213, titled ''Procedures for Connecting Following a Security Incident,'' to incorporate procedures for Clearing Members to follow in the case of a Security Incident, including in order to resume connectivity to OCC. Proposed Rule 213(e) would require a Clearing Member to complete and submit, upon OCC's request, the Reconnection Attestation and Checklist after reporting a Security Incident, both as provided by OCC from time to time. The Reconnection Attestation and Checklist would facilitate OCC's ability to determine whether the risk or threat to OCC has been mitigated sufficiently, including whether to resume connectivity to a Clearing Member if connectivity was disconnected or modified. The proposed Reconnection Attestation and Checklist are set out in more detail below.

Each Reconnection Attestation would be required to be in writing on a form provided by OCC and signed by a designated senior executive of the Clearing Member who is authorized to attest to these matters, as specified in proposed Rule 213(e)(1). Each Reconnection Attestation would contain representations addressing the incident and attesting to certain security requirements. In addition, Clearing Members would be required to describe the Security Incident. OCC is proposing to require that the following representations be included in the Reconnection Attestation in proposed Rule 213(e)(1)(A) through (E):

First, the Reconnection Attestation would include a representation that the Clearing Member has provided full, complete and accurate information in response to all requests made by OCC regarding the Security Incident, including all requests contained in the Reconnection Checklist, on a good faith, best efforts basis.

[8] OCC proposes to renumber existing Rule 219 to Rule 213 following on proposed changes to OCC's clearing membership standards, which includes removal of current rules 213 through 218. *See* Exchange Act Release No. 34–97150 (Mar. 15, 2023), 88 FR 17046 (Mar. 21, 2023) (File No. SR–OCC–2023–002).

Second, the Reconnection Attestation would include a representation that the Clearing Member has provided full, complete and accurate information regarding any OCC data or systems that were potentially compromised during the Security Incident, including any potential exposure of credentials used to access OCC's systems, and will immediately notify OCC if it later becomes aware of a previously undetected or unreported compromise of OCC data or systems during the Security Incident.

Third, the Reconnection Attestation would include a representation that the Clearing Member has determined whether the Security Incident resulted, directly or indirectly, from any controls that failed or were circumvented by its employees, contractors or agents (''Failed Controls''). The proposed language would further specify that the Clearing Member has communicated Failed Controls to OCC and is remediating or has remediated all Failed Controls.

Fourth, the Reconnection Attestation would include a representation that the Clearing Member has implemented, or will implement promptly, technical and operational changes, both preventative and detective, with the intent to prevent a recurrence of the Security Incident and has provided written summaries of such changes to OCC.

Fifth, the Reconnection Attestation would include a representation that the Clearing Member has complied and will continue to comply with all applicable laws in connection with its response to the Security Incident, including any notifications required to be provided to government agencies, OCC, and third parties.

Furthermore, each Reconnection Checklist would be required to be in writing on a form provided by OCC. A Clearing Member would describe its remediation efforts as part of the Reconnection Checklist, including relevant information related to the Security Incident and the Clearing Member's response thereto. To account for the evolving nature of Security Incidents, OCC proposes flexibility regarding the information requirements under proposed Rule 213(e)(2). Namely, the Reconnection Checklist may require information including, but not limited to, the following under this Rule:

- whether the disconnection was the result of a cybersecurity-related incident;
- the nature of the incident;
- the steps taken to contain the incident;
- the OCC data, if any, that was compromised during the incident;
- the OCC systems, if any, that were impacted during the incident;
- whether there was any risk of exposure of credentials used to access OCC systems, and if so, whether the credentials were reissued;
- the controls that were circumvented or failed that led to the incident occurring;
- the changes, preventative and detective, that were implemented to prevent a reoccurrence;
- details on how data integrity has been preserved and what data checks have been performed; [9]
- whether third-parties, including government agencies, have been notified; and
- any additional details relevant to reconnection.

Together, the required representations and information in the Reconnection Attestation and Checklist are designed to provide OCC with evidence related to a Clearing Member's response to a Security Incident, including whether the Clearing Member has appropriate security requirements and carried out suitable remediation measures, to enable OCC to better understand and manage Security Incidents. By requiring such representations and information from a Clearing Member, the Reconnection Attestation and Checklist would provide OCC with key information to make decisions about risks and threats, perform additional monitoring, and determine whether to resume connectivity to a Clearing Member, as applicable, in order to protect OCC's information and data systems.

(2) Statutory Basis

OCC believes the proposed rule changes are consistent with the requirements of the Act and the rules and regulations thereunder applicable to a registered clearing agency. In particular, OCC believes that the proposed rule changes are consistent with Section 17A(b)(3)(F) of the Act,[10] and Rules 17Ad–22(e)(17)(i) and (e)(17)(ii), each promulgated under the Act,[11] for the reasons described below.

Section 17A(b)(3)(F) of the Act requires that the rules of OCC be designed to, among other things, promote the prompt and accurate clearance and settlement of securities transactions and assure the safeguarding of securities and funds which are in the custody or control of the clearing agency or for which it is responsible.[12] As described above, the proposed amendments are designed to help OCC assess and take appropriate action to manage the cybersecurity risks that may be introduced to OCC's information and data systems due to a Security Incident. OCC proposes edits to existing Rule 219, including to titles and headings, to expand the scope to address the occurrence of a Security Incident. Existing Rule 219 would be renumbered as Rule 213 and would clearly set out the obligation of Clearing Members to notify OCC of a Security Incident and the right of OCC to take actions reasonably necessary to mitigate any effects to its operations, thereby centralizing relevant information pertaining to cybersecurity in the Rules and promoting transparency. Moreover, the proposal would implement a standardized approach to assess and manage the cybersecurity risks that OCC may face through its interconnections to Clearing Members. The proposal would include procedures for Clearing Members to follow in the case of a Security Incident, including in order to resume connectivity to OCC. The proposed changes would require a Clearing Member to submit, upon OCC's request, the Reconnection Attestation and Checklist after reporting a Security Incident, both as provided by OCC from time to time. OCC proposes to set forth specific representations and information required of Clearing Members in the Reconnection Attestation and Checklist, which are designed to provide OCC with evidence related to a Clearing Member's response to a Security Incident, including whether the Clearing Member has appropriate security requirements and carried out suitable remediation measures, to enable OCC to better understand and manage Security Incidents. The Reconnection Attestation and Checklist would provide OCC with key information to make decisions about risks and threats, perform additional monitoring, and determine whether to resume connectivity to a Clearing Member, as applicable, to protect OCC's information and data systems. Risks, threats, and potential vulnerabilities could impact OCC's ability to clear and settle securities transactions, or to safeguard the securities and funds which are in its custody or control, or for which it is responsible. Therefore, by enhancing its processes to mitigate these risks, OCC believes the proposal would promote the prompt and accurate

[9] OCC notes that the Reconnection Checklist would specifically request details on how data integrity has been preserved and what data checks have been performed ''prior to reconnecting to and sending/receiving data to/from OCC.'' *See* Exhibit 3 to File No. SR–OCC–2023–003.

[10] 15 U.S.C. 78q–1(b)(3)(F).

[11] 17 CFR 240.17Ad–22(e)(17)(i) and (e)(17)(ii).

[12] 15 U.S.C. 78q–1(b)(3)(F).

clearance and settlement of securities transactions and assure the safeguarding of securities and funds which are in the custody or control of the clearing agency or for which it is responsible, consistent with the requirements of Section 17A(b)(3)(F) of the Act.[13]

Rule 17Ad–22(e)(17)(i) under the Act requires that each covered clearing agency establish, implement, maintain and enforce written policies and procedures reasonably designed to manage the covered clearing agency's operational risks by identifying the plausible sources of operational risk, both internal and external, and mitigating their impact through the use of appropriate systems, policies, procedures, and controls.[14] The proposed Reconnection Attestation and Checklist would reduce the cybersecurity risks to OCC by requiring a Clearing Member to provide written representations addressing the incident and attesting to certain security requirements and an associated checklist describing remediation efforts. The proposed Reconnection Attestation and Checklist would filter the requested information and representations into a standardized format, which would better enable OCC to review and identify areas of interest, concern, or heightened risk in respect of a Security Incident. The representations and information in these forms would help OCC mitigate its exposure to cybersecurity risk and, thereby, decrease the operational risks to OCC. The proposed Reconnection Attestation and Checklist would identify to OCC potential sources of external operational risks that may be introduced through its interconnections to Clearing Members and enable OCC to mitigate these risks and possible impacts to OCC's operations. Based on this information, OCC would make a determination regarding the resumption of connectivity to a Clearing Member if connectivity was disconnected or modified. As a result, OCC believes the proposal is consistent with the requirements of Rule 17Ad–22(e)(17)(i) under the Act.[15]

Rule 17Ad–22(e)(17)(ii) under the Act requires that each covered clearing agency establish, implement, maintain and enforce written policies and procedures reasonably designed to manage the covered clearing agency's operational risks by ensuring, in part, that systems have a high degree of security, resiliency, and operational reliability.[16] The proposed Reconnection Attestation and Checklist would help enhance the security, resiliency, and operational reliability of OCC's information and data systems. Namely, these forms would help OCC determine whether to take action against a Clearing Member, including preventing the reconnection of a Clearing Member, that may pose an increased cyber risk to OCC by not having appropriate security requirements or taking suitable remediation measures. Clearing Members that have not adequately addressed Security Incidents may present increased risk to OCC. For example, weaknesses within a Clearing Member's environment could allow for exploitation by a malicious actor of the link between a Clearing Member and OCC. By better enabling OCC to identify these risks, the proposed rule change would allow OCC to more effectively secure its environment against potential vulnerabilities. The required representations and information in the Reconnection Attestation and Checklist would provide OCC with key information to make decisions about risks and threats, perform additional monitoring, and determine whether to resume connectivity to a Clearing Member, as applicable, to protect OCC's information and data systems. As a result, OCC believes the proposal would improve OCC's ability to ensure that its systems have a high degree of security, resiliency, and operational reliability, and, as such, is consistent with the requirements of Rule 17Ad–22(e)(17)(ii) under the Act.[17]

*(B) Clearing Agency's Statement on Burden on Competition*

Section 17A(b)(3)(I) of the Act[18] requires that the rules of a clearing agency not impose any burden on competition not necessary or appropriate in furtherance of the purposes of the Act. OCC does not believe that the proposed rule changes would impose any burden on competition not necessary or appropriate in furtherance of the purposes of the Act. As discussed above, OCC proposes to amend certain provisions in the Rules relating to Clearing Member cybersecurity obligations to address the occurrence of a Security Incident. The proposed changes would (i) require a Clearing Member to immediately notify OCC of a Security Incident; (ii) memorialize OCC's ability to take actions reasonably necessary to mitigate any effects to its operations; and (iii) require such Clearing Member to provide a Reconnection Attestation and Checklist. While the proposed changes would require Clearing Members to incur additional costs, including to complete and submit the Reconnection Attestation and Checklist, OCC does not believe the proposed changes would present an undue burden on Clearing Members. Clearing Members are already subject to the notification and reporting requirements in OCC's By-Laws and the Rules that require, among other things, that Clearing Members provide OCC with such documents and information as OCC may require from time to time.[19] Standardizing the form and contents of the proposed submissions would reduce the potential uncertainty and time required to demonstrate an acceptable response to a Security Incident. Additionally, the proposed changes would not unfairly inhibit access to OCC's services or disadvantage or favor any particular user in relationship to another user. Such changes would apply to all Clearing Members consistently and thus would not provide any Clearing Member with a competitive advantage over any other Clearing Member as the requirements would be uniform. As described above, given OCC's position in the marketplace, OCC believes it is prudent to enhance its management of Security Incidents as detailed in the proposal, so that OCC's own information and data systems remain protected against cyberattacks. For the foregoing reasons, OCC believes that the proposed rule change is in the public interest, would be consistent with the requirements of the Act applicable to clearing agencies, and would not impact or impose a burden on competition.

*(C) Clearing Agency's Statement on Comments on the Proposed Rule Change Received From Members, Participants or Others*

Written comments were not and are not intended to be solicited with respect to the proposed rule change and none have been received.

## III. Date of Effectiveness of the Proposed Rule Change and Timing for Commission Action

Within 45 days of the date of publication of this notice in the **Federal Register** or within such longer period up to 90 days (i) as the Commission may designate if it finds such longer period

[13] *Id.*

[14] 17 CFR 240.17Ad–22(e)(17)(i).

[15] *Id.*

[16] 17 CFR 240.17Ad–22(e)(17)(ii).

[17] *Id.*

[18] 15 U.S.C. 78q–1(b)(3)(I).

[19] *See* Article V, Section 1, Interpretation and Policy .07 of the By-Laws and Rules 201(b), 215, 216, 217(b), 303, 306, 308 and 310(a)–(c).

to be appropriate and publishes its reasons for so finding or (ii) as to which the self-regulatory organization consents, the Commission will:

(A) by order approve or disapprove such proposed rule change, or

(B) institute proceedings to determine whether the proposed rule change should be disapproved.

The proposal shall not take effect until all regulatory actions required with respect to the proposal are completed.

**IV. Solicitation of Comments**

Interested persons are invited to submit written data, views and arguments concerning the foregoing, including whether the proposed rule change is consistent with the Act. Comments may be submitted by any of the following methods:

*Electronic Comments*

- Use the Commission's internet comment form (*http://www.sec.gov/rules/sro.shtml*); or
- Send an email to *rule-comments@sec.gov.* Please include File Number SR–OCC–2023–003 on the subject line.

*Paper Comments*

- Send paper comments in triplicate to Vanessa Countryman, Secretary, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549–1090.

All submissions should refer to File Number SR–OCC–2023–003. This file number should be included on the subject line if email is used. To help the Commission process and review your comments more efficiently, please use only one method. The Commission will post all comments on the Commission's internet website (*http://www.sec.gov/rules/sro.shtml*). Copies of the submission, all subsequent amendments, all written statements with respect to the proposed rule change that are filed with the Commission, and all written communications relating to the proposed rule change between the Commission and any person, other than those that may be withheld from the public in accordance with the provisions of 5 U.S.C. 552, will be available for website viewing and printing in the Commission's Public Reference Room, 100 F Street, NE, Washington, DC 20549, on official business days between the hours of 10:00 a.m. and 3:00 p.m. Copies of such filing also will be available for inspection and copying at the principal office of OCC and on OCC's website at *https://www.theocc.com/Company-Information/Documents-and-Archives/By-Laws-and-Rules.*

All comments received will be posted without change. Persons submitting comments are cautioned that we do not redact or edit personal identifying information from comment submissions. You should submit only information that you wish to make available publicly.

All submissions should refer to File Number SR–OCC–2023–003 and should be submitted on or before April 26, 2023.

For the Commission, by the Division of Trading and Markets, pursuant to delegated authority.[20]

**Sherry R. Haywood,**

*Assistant Secretary.*

[FR Doc. 2023–07004 Filed 4–4–23; 8:45 am]

**BILLING CODE 8011–01–P**

---

## SECURITIES AND EXCHANGE COMMISSION

**[Release No. 34–97224; File No. SR–ICEEU–2023–009]**

## Self-Regulatory Organizations; ICE Clear Europe Limited; Notice of Filing of Proposed Rule Change Relating to Amendments of the Investment Management Procedures

March 30, 2023.

Pursuant to Section 19(b)(1) of the Securities Exchange Act of 1934 (''Act''),[1] and Rule 19b–4 thereunder,[2] notice is hereby given that on March 23, 2023, ICE Clear Europe Limited (''ICE Clear Europe'' or the ''Clearing House'') filed with the Securities and Exchange Commission (''Commission'') the proposed rule changes described in Items I, II and III below, which Items have been primarily prepared by ICE Clear Europe. The Commission is publishing this notice to solicit comments on the proposed rule change from interested persons.

**I. Clearing Agency's Statement of the Terms of Substance of the Proposed Rule Change**

ICE Clear Europe Limited (''ICE Clear Europe'' or the ''Clearing House'') proposes to modify its Investment Management Procedures[3] (the ''Investment Management Procedures'' or the ''Procedures'') to change the maximum maturities for certain investments made with amounts held by the Clearing House as regulatory capital.

**II. Clearing Agency's Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change**

In its filing with the Commission, ICE Clear Europe included statements concerning the purpose of and basis for the proposed rule change and discussed any comments it received on the proposed rule change. The text of these statements may be examined at the places specified in Item IV below. ICE Clear Europe has prepared summaries, set forth in sections (A), (B), and (C) below, of the most significant aspects of such statements.

*(A) Clearing Agency's Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change*

(a) Purpose

ICE Clear Europe is proposing to amend the Investment Management Procedures in the Table of Authorised Investments and Concentration Limits for ICEU's Regulatory Capital (the ''Table'') to change the maximum maturity of certain investments in sovereign and government agency bonds. In particular, the maximum maturity on the purchase of U.S. Sovereign Bonds, UK Sovereign Bonds, EU Sovereign Bonds, U.S. Government Agency Bonds, UK Government Agency Bonds, and EU Government Agency Bonds would be amended from 90 days to 13 months. The amendments would align the maximum maturity for such investments with the existing maximum maturity for permitted investments in the same instrument that are made with cash provided by Clearing Members (''CMs'') (*e.g.,* as margin or guaranty fund contribution) and the Clearing House's own contribution to the guaranty fund. By extending the maximum maturity, ICE Clear Europe would have the flexibility to invest its regulatory capital in longer term sovereign and government bonds. ICE Clear Europe believes that such flexibility is important in light of current and expected market conditions, including to assist ICE Clear Europe in avoiding having to invest or reinvest in shorter duration instruments during potential periods of market volatility, such as those that may arise in connection with U.S. debt ceiling developments.

(b) Statutory Basis

ICE Clear Europe believes that the proposed amendments to the Investment Management Procedures are consistent with the requirements of

---

[20] 17 CFR 200.30–3(a)(12).

[1] 15 U.S.C. 78s(b)(1).

[2] 17 CFR 240.19b–4.

[3] Capitalized terms used but not defined herein have the meanings specified in the ICE Clear Europe Clearing Rules and the Investment Management Procedures.