DCO Rules

UNITED STATES
COMMODITY FUTURES TRADING COMMISSION

Submitter Information

Organization Name
Options Clearing Corporation

Organization Type	**Organization Acronym**
DCO	OCC
Submitted By	**Email Address**
mbrown1	mcbrown@theocc.com

Cover Sheet

Submission Number	**Submission Date**
2205-2512-3349-57	5/25/2022 12:33:49 PM ET

Submission Type
40.6(a) Rule Certification

Submission Description
Rule Certification Concerning Clearing Member Cybersecurity Attestation Program

☐ **Request Confidential Treatment**

Registered Entity Identifier Code

Rule Numbers
Rule 219

Date of Intended Implementation
6/24/2022

Documents

2022.5.25 OCC Self-Certification (Cybersecurity Attestation).pdf

Request For Confidential Treatment - Detailed Written Justification

N/A

THE FOUNDATION FOR SECURE MARKETS

Options Clearing Corporation
125 S. Franklin Street, Suite 1200
Chicago, IL 60606
312 322 6200 | theocc.com

May 25, 2022

VIA CFTC PORTAL

Christopher J. Kirkpatrick
Office of the Secretariat
Commodity Futures Trading Commission
Three Lafayette Centre
1155 21st Street, N.W.
Washington, DC 20581

Re: Rule Certification Concerning Clearing Member Cybersecurity Attestation Program

Dear Secretary Kirkpatrick:

Pursuant to Section 5c(c)(1) of the Commodity Exchange Act, as amended ("Act"), and Commodity Futures Trading Commission ("CFTC") Regulation 40.6, The Options Clearing Corporation ("OCC") hereby certifies changes to its Rules to require Clearing Members and applicants for clearing membership ("Applicants") to submit standardized, written representations regarding their cybersecurity programs and to update such representations periodically. The date of implementation of the rule is at least 10 business days following receipt of the certification by the CFTC. The proposal has also been submitted to the Securities and Exchange Commission ("SEC") under Section 19(b) of the Securities Exchange Act of 1934 ("Exchange Act") and Rule 19b-4 thereunder.

In conformity with the requirements of Regulation 40.6(a)(7), OCC states the following:

Explanation and Analysis

The purpose of the certification is to amend OCC's Rules to establish requirements in support of a cybersecurity attestation program for Clearing Members and Applicants. Proposed changes to OCC's Rulebook can be found in Exhibit A. Material proposed to be added to OCC's Rules as currently in effect is underlined. All capitalized terms not defined herein have the same meaning as set forth in the OCC By-Laws and Rules.[1]

[1] 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.

Overview

OCC is proposing to modify the Rules in order to (1) define "Cybersecurity Confirmation" as a signed, written representation that addresses the submitting firm's cybersecurity program; and (2) enhance its existing practices to require that (a) Applicants deliver a complete Cybersecurity Confirmation as part of their application materials, and (b) all Clearing Members to deliver a complete, updated Cybersecurity Confirmation at least every two years, on a date established by OCC.

The Cybersecurity Confirmation would help OCC assess the cybersecurity risks that may be introduced to it by Clearing Members and Applicants that connect to OCC's networks and systems. The proposed Cybersecurity Confirmation would allow OCC to better assess its Clearing Members' and Applicants' cybersecurity programs and frameworks and identify possible cybersecurity risk exposures. Based on this information, OCC could take action to enhance its existing controls and mitigate identified risks and potential impacts to OCC's operations.

OCC believes it is prudent to implement a standardized approach for due diligence of cybersecurity risks that it may face through its interconnections to Clearing Members. As a designated systemically important financial market utility ("SIFMU"),[2] 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 understanding of endpoint security frameworks so that its network and systems remain protected against cyberattacks.

OCC maintains a Third-Party Risk Management ("TPRM") Framework that is designed to enable OCC to identify, measure and manage potential operational, information technology and security risks arising from third-parties, including Clearing Members and Applicants.[3] Under the TPRM Framework, OCC obtains information regarding the security of an Applicant's systems and cybersecurity program prior to admitting the firm as a Clearing Member and permitting it to connect directly to OCC or through another means, such as a through a third-party service provider, service bureau, network, or the Internet. OCC obtains information regarding the security of a Clearing Member's systems and cybersecurity program on a periodic basis thereafter through risk examinations that are conducted in accordance with the TPRM Framework.

OCC's existing process for assessing cybersecurity risks that may be presented by Clearing Members and Applicants uses a questionnaire format. Responses help OCC determine whether the submitting firm (i) has established a process to notify OCC regarding security incidents; (ii) has a formal incident communication procedure integrated with its security incident response and

---

[2] 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).

[3] See Exchange Act Release No. 90797 (Dec. 23, 2020), 85 FR 86592, 86593 (Dec. 30, 2020) (File No. SR-OCC-2020-014).

escalation process; (iii) uses encryption to protect data within and outside of its network; (iv) has established appropriate access controls, including with respect to OCC systems and data; and (v) validates controls using independent, third-party auditors or information security professionals. OCC may require supporting information or documentation for any of these items. While the questionnaire is standardized, the form and content of supporting documentation requested by OCC is not. OCC's process for validating the submitting firm's information can be iterative and time-consuming.

OCC proposes to adopt a more standardized approach for due diligence of Clearing Members' and Applicants' cybersecurity programs and frameworks. OCC believes the proposed program and associated rule change would enhance the consistency of information OCC receives from submitting firms, align with industry peers and improve process effectiveness and efficiency.[4] The proposal would better enable OCC to understand which Clearing Members may present a heightened cybersecurity risk by requiring the firms to provide information in a standardized format, which OCC could better use to make decisions about potential network risks or threats. Additionally, the proposed program would harmonize OCC's cybersecurity due diligence requirements for Clearing Members and Applicants with requirements that were adopted by the National Securities Clearing Corporation, Fixed Income Clearing Corporation and Depository Trust Company (collectively, the "DTCC Clearing Agencies") and filed with the Commission.[5] The content of OCC's proposed Cybersecurity Confirmation form is substantively identical to the content of the cybersecurity confirmation form adopted by the DTCC Clearing Agencies. OCC believes an attestation-based format would be more efficient and effective than its current questionnaire-based format in ascertaining whether the submitting firm maintains appropriate policies, processes and programs with respect to cyber risk. OCC's proposed program would improve process effectiveness and efficiency for all submitting firms and OCC by standardizing the form of submissions and thereby reducing the time and effort required to demonstrate the existence of an acceptable cybersecurity framework. Additionally, approximately 90% of OCC's Clearing Members are subject to requirements that are substantively identical to the proposed program by virtue of their membership or participation at one or more of the DTCC Clearing Agencies. The proposed program would establish a uniform approach for Clearing Members and Applicants to demonstrate the adequacy of their cyber and information security programs to OCC, while also aligning with the approach adopted by the DTCC Clearing Agencies and applicable to the large majority of OCC's Clearing Members already.[6]

---

4 See infra note 7.

5 See Exchange Act Release No. 87696 (Dec. 9, 2019), 84 FR 68243, 68244 – 68245 (Dec. 13, 2019) (File No. SR-NSCC-2019-003); Exchange Act Release No. 87697 (Dec. 9, 2019), 84 FR 68266, 68267 – 68268 (Dec. 13, 2019) (File No. SR-FICC-2019-005); Exchange Act Release No. 87698 (Dec. 9, 2019), 84 FR 68269, 68270 – 68271 (Dec. 13, 2019) (File No. SR-DTC-2019-008), respectively (collectively, "Orders Approving Program").

6 See id.

OCC believes that aligning the format and content of OCC's cybersecurity attestation with that used by the DTCC Clearing Agencies would enhance process efficiency by eliminating the duplication of effort currently required for these common Clearing Members to submit different sets of materials to OCC and the DTCC Clearing Agencies regarding the firm's cybersecurity practices.[7] These process efficiencies also support program effectiveness by filtering the requested information into standardized format, which better enables OCC to review and identify areas of interest or concern for a specific firm or groups of firms. The frequency of OCC reviews under the proposed framework would also increase from every three years to every two years, which OCC believes would further enhance process effectiveness.

Proposed Rule Changes

OCC is proposing to modify its Rules to define "Cybersecurity Confirmation" and require that firms deliver a completed Cybersecurity Confirmation (a) as part of their initial application with OCC, and (b) on an ongoing basis, at least every two years. Each of these proposed changes is described in greater detail below.

OCC is proposing to adopt a definition of "Cybersecurity Confirmation" in a new Rule 219 (Cybersecurity Confirmation). Each Cybersecurity Confirmation would be required to be in writing on a form provided by OCC and signed by a designated senior executive of the submitting firm who is authorized to attest to these matters. Based on the form provided by OCC, each Cybersecurity Confirmation would include representations regarding the submitting firm's cybersecurity program and framework. In addition, submitting firm would be required to identify its designated control officer and the standards and/or frameworks it uses to guide and assess its cybersecurity program. While the proposed Cybersecurity Confirmation would identify certain standards and guidelines that would be appropriate, OCC would consider requests by Clearing Members and Applicants to allow other standards in accepting a Cybersecurity Confirmation.

The initial representations made by Clearing Members and Applicants would be made as of the date of submission to OCC. Subsequent representations made by Clearing Members would cover the two years prior to the date of the most recently provided Cybersecurity Confirmation.

OCC is proposing to require that the following representations be included in the form of Cybersecurity Confirmation:

First, the Cybersecurity Confirmation would include a representation that the submitting firm has defined and maintains a comprehensive cybersecurity program and framework that considers potential cyber threats that impact its organization and protects the confidentiality, integrity, and availability requirements of its systems and information.

---

[7] Approximately 90% of current OCC Clearing Members are also members or participants at one or more of the DTCC Clearing Agencies.

Second, the Cybersecurity Confirmation would include a representation that the submitting firm has implemented and maintains a written enterprise cybersecurity policy or policies approved by senior management or the organization's board of directors, and the organization's cybersecurity framework is in alignment with standard industry best practices and guidelines, as indicated on the form of Cybersecurity Confirmation.[8]

Third, the Cybersecurity Confirmation would include a representation that, if the submitting firm is using a third-party service provider or service bureau(s) to connect or transact business or to manage the connection with OCC, the submitting firm has an appropriate program to (a) evaluate the cyber risks and impact of these third parties, and (b) review the third-party assurance reports.

Fourth, the Cybersecurity Confirmation would include a representation that the submitting firm's cybersecurity program and framework protect the segment of its system that connects to and/or interacts with OCC.

Fifth, the Cybersecurity Confirmation would include a representation that the submitting firm has in place an established process to remediate cyber issues identified to fulfill the submitting' firm's regulatory and/or statutory requirements.

Sixth, the Cybersecurity Confirmation would include a representation that the submitting firm's cybersecurity program's and framework's risk processes are updated periodically based on a risk assessment or changes to technology, business, threat ecosystem, and/or regulatory environment.

Lastly, the Cybersecurity Confirmation would include a representation that the review of the submitting firm's cybersecurity program and framework has been conducted by one of the following: (1) the submitting firm, if it has filed and maintains a current Certification of Compliance with the Superintendent of the New York State Department of Financial Services confirming compliance with its Cybersecurity Requirements for Financial Services Companies;[9] (2) a regulator

---

[8] Examples of recognized frameworks, guidelines and standards that OCC believes are adequate include the Financial Services Sector Coordinating Council Cybersecurity Profile, the National Institute of Standards and Technology Cybersecurity Framework ("NIST CSF"), International Organization for Standardization ("ISO") standard 27001/27002 ("ISO 27001"), Federal Financial Institutions Examination Council ("FFIEC") Cybersecurity Assessment Tool, Critical Security Controls Top 20, and Control Objectives for Information and Related Technologies. OCC would identify recognized frameworks, guidelines and standards in the form of Cybersecurity Confirmation and in an Information Memorandum that OCC would issue from time to time. OCC would also consider accepting other standards upon request by a Clearing Member or Applicant.

[9] 23 N.Y. Comp. Codes R. & Regs. tit. 23, § 500 (2017). This regulation requires firms to confirm that they have a comprehensive cybersecurity program, as described in the

who assesses the program against an industry cybersecurity framework or industry standard, including those that are listed on the form of Cybersecurity Confirmation and in an Information Memorandum that is issued by OCC from time to time;[10] (3) an independent external entity with cybersecurity domain expertise in relevant industry standards and practices, including those that are listed on the form of Cybersecurity Confirmation and in an Information Memorandum that is issued by OCC from time to time;[11] or (4) an independent internal audit function reporting directly to the submitting firm's board of directors or designated board of directors committee, such that the findings of that review are shared with these governance bodies.

Together, the required representations are designed to provide OCC with evidence of each Clearing Member's and Applicant's management of cybersecurity with respect to their connectivity to OCC. By requiring these representations from Clearing Members and Applicants the proposed Cybersecurity Confirmation would provide OCC with additional information that it could use to make decisions about risks or threats, perform additional monitoring, target potential vulnerabilities and protect the OCC network.

OCC is proposing to require that a Cybersecurity Confirmation be submitted by each Applicant, as part of its application materials, and at least every two years by each Clearing Member. With respect to the requirement to deliver a Cybersecurity Confirmation at least every two years, OCC would provide each Clearing Member with notice of the date on which the Cybersecurity Confirmation would be due. Each Clearing Member would have 180 calendar days after such notification to provide OCC with its completed Cybersecurity Confirmation.

In order to implement these proposed changes, OCC would amend the Rules to include a new Rule 219 (Cybersecurity Confirmation) to require that (1) each Applicant completes and delivers a Cybersecurity Confirmation as part of its application materials; and (2) each Clearing

---

regulation, which OCC believes is sufficient to meet the objectives of the proposed Cybersecurity Confirmation.

[10] Industry cybersecurity frameworks and industry standards could include, for example, the Office of the Comptroller of the Currency or the FFIEC Cybersecurity Assessment Tool. OCC would identify acceptable industry cybersecurity frameworks and standards in the form of Cybersecurity Confirmation and in an Information Memorandum that OCC would issue from time to time. OCC would also consider accepting other industry cybersecurity frameworks and standards upon request by a Clearing Member or Applicant.

[11] A third party with cybersecurity domain expertise is one that follows and understands industry standards, practices and regulations that are relevant to the financial sector. Examples of such standards and practices include ISO 27001 certification or NIST CSF assessment. OCC would identify acceptable industry standards and practices in the form of Cybersecurity Confirmation and in an Information Memorandum that OCC would issue from time to time. OCC would also consider accepting other industry standards and practices upon request by a Clearing Member or Applicant.

Member completes and delivers a Cybersecurity Confirmation at least every two years, on a date that is 180 calendar days from the date that OCC notifies the Clearing Member of the requirement to submit a Cybersecurity Confirmation.

Consistency with DCO Core Principles

OCC reviewed the DCO core principles ("Core Principles") as set forth in the Act, the regulations thereunder, and the provisions applicable to a DCO that elects to be subject to the provisions of 17 CFR Subpart C ("Subpart C DCO"). During this review, OCC identified the following as potentially being impacted:

Participant and product eligibility. OCC believes that the proposed changes are consistent with Core Principle C,[12] which requires, in part, that each DCO establish appropriate admission and continuing eligibility standards for Clearing Members of the DCO and establish and implement procedures to verify, on an ongoing basis, the compliance of each participation and membership requirement of the DCO.[13] Core Principle C further requires that such participation and membership requirements be objective, publicly disclosed, and permit fair and open access.[14] OCC is establishing in its public Rulebook a requirement that Clearing Members and Applicants provide standardized information, in the form of the Cybersecurity Confirmation, regarding their cybersecurity programs as a condition of clearing membership. Updated Cybersecurity Confirmations would be required from each submitting firm on a regular timeline, enabling OCC to monitor the firms' cybersecurity programs on an ongoing basis. The standardization of information to be submitted would enhance OCC's ability to identify, monitor and manage potential cybersecurity risks presented by submitting firms, while enhancing process effectiveness and efficiency both for the submitting firms and OCC. OCC therefore believes that the proposed change would be consistent with the Core Principle C under the Act.[15]

Risk management. OCC believes that the proposed changes are consistent with Core Principle D.[16] CFTC Regulation 39.13[17] requires, in relevant part, that each DCO have rules that require clearing members to maintain current written risk management policies and procedures, which address the risks that such clearing members may pose to the DCO.[18] The amended OCC Rules and associated Cybersecurity Confirmation would require OCC Clearing Members and

---

12 7 U.S.C. 7a-1(c)(2)(C).

13 See id.

14 See id.

15 Id.

16 7 U.S.C. 7a-1(c)(2)(D).

17 17 CFR 39.13.

18 See 17 CFR 39.13(h)(5).

Applicants to provide OCC with information in a standardized format regarding the submitting firm's management of cybersecurity risks. OCC will review these attestations and request additional information, as necessary, in order to assess the cybersecurity programs of submitting firms and take appropriate action to address concerns identified in such reviews. In this way, OCC believes the proposed change is consistent with Core Principle D under the Act.[19]

Systems safeguards. OCC believes that the proposed changes are consistent with the requirements of Core Principle I.[20] CFTC Regulation 39.18[21] requires, in relevant part, that each DCO establish and maintain a program of risk analysis and oversight with respect to its operations and automated systems, and that such program address information security.[22] The amended OCC Rules and associated Cybersecurity Confirmation would support OCC's program of risk analysis and oversight with respect to its operations and automated systems, particularly with respect to information security. The required Cybersecurity Confirmation is designed to provide OCC with evidence of each Clearing Member's and Applicant's management of cybersecurity with respect to their connectivity to OCC, as well as additional information that OCC could use to make decisions about risks or threats, perform additional monitoring, target potential vulnerabilities and protect its network. OCC's proposed cybersecurity program is based on generally accepted standards for cybersecurity and industry best practices as implemented by other SEC-regulated SIFMUs. In these ways, OCC believes the proposed change is consistent with Core Principle I under the Act.[23]

Opposing Views

No substantive opposing views were expressed related to the rule amendments by OCC's Board members, Clearing Members or market participants.

Notice of Pending Rule Certification

OCC hereby certifies that notice of this rule filing has been given to Clearing Members of OCC in compliance with Regulation 40.6(a)(2) by posting a copy of this certification on OCC's website concurrently with the filing of this submission.

Certification

OCC hereby certifies that the rule set forth at Exhibit A of the enclosed filing complies with the Act and the CFTC's regulations thereunder.

---

19 7 U.S.C. 7a-1(c)(2)(D).

20 7 U.S.C. 7a-1(c)(2)(I).

21 See 17 CFR 39.18.

22 See 17 CFR 39.18(b)(1), (2).

23 7 U.S.C. 7a-1(c)(2)(D).

Should you have any questions regarding this matter, please do not hesitate to contact me.

Sincerely,

/s/ Mark C. Brown
Associate General Counsel

Enclosure: Exhibit A

EXHIBIT A

OCC Rules

Underlined text indicates new text

CHAPTER II – MISCELLANEOUS REQUIREMENTS

* * * * *

RULE 219 – Cybersecurity Confirmation

(a) Each Clearing Member and applicant for clearing membership shall complete and submit a form, provided by the Corporation, that confirms the existence of an information system cybersecurity program and includes required representations as determined by the Corporation ("Cybersecurity Confirmation").

(i) Each applicant for clearing membership shall submit a completed Cybersecurity Confirmation as part of its application materials.

(ii) Each Clearing Member shall submit a completed Cybersecurity Confirmation at least every two years and not later than 180 calendar days from the date that OCC notifies the Clearing Member that an attestation is required.

(b) The Cybersecurity Confirmation shall consist of representations including, but not limited to, the following:

(1) The Clearing Member or applicant for clearing membership has defined and maintains a comprehensive cybersecurity program and framework that considers potential cyber threats that impact their organization and protects the confidentiality, integrity, and availability requirements of their systems and information.

(2) The Clearing Member or applicant for clearing membership has implemented and maintains a written enterprise cybersecurity policy or policies approved by senior management or the organization's board of directors, and the organization's cybersecurity framework is in alignment with standard industry best practices and guidelines, as indicated on the form of Cybersecurity Confirmation. OCC may consider requests to recognize additional best practices and guidelines that are not indicated on the form of Cybersecurity Confirmation.

(3) If using a third-party service provider or service bureau(s) to connect or transact business or to manage the connection with the Corporation, the Clearing Member or applicant for clearing membership has an appropriate program to (A) evaluate the cyber risks and impact of these third parties, and (B) review the third-party assurance reports.

(4) The cybersecurity program and framework protect the segment of the Clearing Member's or applicant's system that connects to and/or interacts with the Corporation.

(5) The Clearing Member or applicant has in place an established process to remediate cyber issues identified to fulfill the Clearing Member's or applicant's regulatory and/or statutory requirements.

(6) The cybersecurity program's and framework's risk processes are updated periodically based on a risk assessment or changes to technology, business, threat ecosystem, and/or regulatory environment.

(7) A comprehensive review of the Clearing Member's or applicant's cybersecurity program and framework has been conducted by one of the following:

- The Clearing Member or applicant, if that organization has filed and maintains a current Certification of Compliance with the Superintendent of the New York State Department of Financial Services pursuant to 23 NYCRR 500;

- A regulator who assesses the program against a designated cybersecurity framework or industry standard, including those that are listed on the form of the Cybersecurity Confirmation and in an Information Memorandum published by the Corporation from time to time;

- An independent external entity with cybersecurity domain expertise, including those that are listed on the form of the Cybersecurity Confirmation [and in an Information Memorandum published by the Corporation from time to time]; and

- An independent internal audit function reporting directly to the board of directors or designated board of directors committee of Clearing Member or applicant, such that the findings of that review are shared with these governance bodies.

(c) The Cybersecurity Confirmation shall be signed by a designated senior executive of the Clearing Member or applicant who is authorized to attest to these matters.

* * * * *