SECURITIES AND EXCHANGE COMMISSION
(Release No. 34-95068; File No. SR-OCC-2022-008)

June 8, 2022

Clearing Agency; The Options Clearing Corporation; Notice of Filing and Immediate Effectiveness of Proposed Rule Change Concerning Adoption of a Cybersecurity Attestation Program

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 May 25, 2022, The Options Clearing Corporation ("OCC") filed with the Securities and Exchange Commission ("Commission") the proposed rule change as described in Items I, II, and III below, which Items have been prepared primarily by OCC. OCC filed the proposed rule change pursuant to Section 19(b)(3)(A)[3] of the Act and Rule 19b-4(f)(6)[4] thereunder.

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

The proposed rule change would amend the OCC's Rules to (1) define "Cybersecurity Confirmation" as a signed, written representation that addresses the submitting firm's cybersecurity program; and (2) enhance the OCC application requirements and ongoing requirements for applicants for clearing membership ("Applicants") and Clearing Members to require (a) each Applicant to provide a completed Cybersecurity Confirmation as part of its application materials, and (b) each Clearing Member to deliver to OCC a complete, updated Cybersecurity Confirmation at least every two years, as described in greater detail below. The proposed changes to

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

2 17 CFR 240.19b-4.

3 15 U.S.C. 78s(b)(3)(A).

4 17 CFR 240.19b-4(f)(6).

OCC's Rules are included as Exhibit 5 of File No. SR-OCC-2022-008. 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.[5]

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

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) all 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.

5 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.

As described in more detail below, 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"),[6] 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.[7] 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

---

6 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).

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

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 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 rule change would enhance the consistency of information OCC receives from submitting firms, align with industry peers and improve process effectiveness and efficiency.[8] 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,

[8] See infra note 10.

which OCC could better use to make decisions about potential network risks or threats. Additionally, the proposed rule change 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.[9] The content of OCC's proposed Cybersecurity Confirmation form, included at Exhibit 3, 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 rule change would improve process effectiveness and efficiency for all submitting firms and OCC. As noted above, OCC's existing process for evaluating Clearing Members' cybersecurity programs uses a question-and-answer format that tends toward an iterative process for gathering responses and supporting documentation. OCC's proposal would enhance process efficiency for all submitting firms by standardizing the form of submissions and thereby reducing the time and effort required to demonstrate the existence of an acceptable cybersecurity framework. In addition, the large majority of OCC Clearing Members are required to make attestations regarding their cybersecurity programs that are substantively identical to OCC's proposal. OCC believes that aligning

---

[9] 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").

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.[10] 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.

OCC Clearing Members may currently be subject to regulations that are designed, in part, to enhance the safeguards used by these entities to protect themselves against cyberattacks.[11] In order to comply with such regulations, Clearing Members and Applicants would be required to follow standards established by national or international organizations focused on information security management, and would have already established protocols to allow their senior management to verify that they have sufficient

---

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

[11] For example, depending on the type of entity, Clearing Members or Applicants may be subject to one or more of the following regulations: (1) Regulation S-ID, which requires "financial institutions" or "creditors" under the rule to adopt programs to identify and address the risk of identity theft of individuals (17 CFR 248.201 - 202); (2) Regulation S-P, which requires broker-dealers, investment companies, and investment advisers to adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information (17 CFR 248.1 - 30); and (3) Rule 15c3-5 under the Securities Exchange Act of 1934 ("Act"), known as the "Market Access Rule," which requires broker-dealers to establish, document, and maintain a system for regularly reviewing the effectiveness of its management controls and supervisory procedures (17 CFR 240.15c3-5).

cybersecurity programs in place to fulfill existing regulatory obligations. Other Clearing Members have established and follow substantially similar protocols because of evolving expectations by regulators or by institutional customers as to the sufficiency of their cyber safeguards. Additionally, approximately 90% of OCC's Clearing Members are subject to requirements that are substantively identical to the proposed rule change by virtue of their membership or participation at one or more of the DTCC Clearing Agencies. The proposed rule change 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.[12]

Proposed Rule Changes

OCC is proposing to modify its Rules to (1) define "Cybersecurity Confirmation;" and (2) 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 rule changes is described in greater detail below.

(a) *Proposed Cybersecurity Confirmation*

OCC is proposing to adopt a definition of "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 contain representations regarding the submitting

12 See Orders Approving Program, supra note 9.

firm's cybersecurity program and framework. In addition, Clearing Members and Applicants 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.

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.[13]

---

[13] 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

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 programs 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

---

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.

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;[14] (2) a regulator 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;[15] (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;[16] 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.

---

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

15 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.

16 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.

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 amend the Rules to include a definition of "Cybersecurity Confirmation," as described above, in a new Rule 219 (Cybersecurity Confirmation).

(b) *Initial and Ongoing Requirement*

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 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.

Implementation Timeframe

OCC proposes the rule changes to be effective immediately upon filing. Notwithstanding their immediate effectiveness, OCC would not make the proposed rule changes operative until 30 days after the date of the filing, or such shorter time as the Commission may designate. Upon implementation, the proposed requirement that that [sic] all Applicants deliver a Cybersecurity Confirmation with their application materials would apply to applications that have been submitted at that time but have not yet been approved or rejected. Following the effective date of the proposed rule change, OCC would notify each Clearing Member of the date on which its Cybersecurity Confirmation would be due. Each Clearing Member would then have 180 calendar days after such notification to provide OCC with its completed Cybersecurity Confirmation.

(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,[17] and Rules 17Ad-22(e)(17)(i) and (e)(17)(ii), each promulgated under the Act,[18] 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.[19] As described above, the proposed requirement that Clearing Members and Applicants

17 15 U.S.C. 78q-1(b)(3)(F).

18 17 CFR 240.17Ad-22(e)(17)(i) and (e)(17)(ii).

19 15 U.S.C. 78q-1(b)(3)(F).

provide a Cybersecurity Confirmation regarding their cybersecurity program which includes the representations described above would provide OCC with evidence of each Clearing Member's or Applicant's management of endpoint security and would enhance the protection of OCC against cyberattacks. The proposed Cybersecurity Confirmation would provide OCC with information that it could use to make decisions about risks or threats, perform additional monitoring, target potential vulnerabilities, and protect the OCC network. The proposed Cybersecurity Confirmation would enable OCC to further identify its exposure and enable it to take steps to mitigate risks. These requirements would help reduce risk to OCC's network with respect to its communications with Clearing Members and their submission of instructions and transactions to OCC by requiring all Clearing Members connecting to OCC to have appropriate cybersecurity programs in place. 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 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.[20]

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

---

[20] Id.

plausible sources of operational risk, both internal and external, and mitigating their impact through the use of appropriate systems, policies, procedures, and controls.[21] The proposed Cybersecurity Confirmation would reduce cybersecurity risks to OCC by requiring all Clearing Members and Applicants to confirm they have defined and maintain cybersecurity programs that meet standard industry best practices and guidelines. The proposed representations in the Cybersecurity Confirmations would help OCC to mitigate its exposure to cybersecurity risk and, thereby, decrease the operational risks to OCC. The proposed Cybersecurity Confirmations would identify to OCC potential sources of external operational risks and enable it to mitigate these risks and possible impacts to OCC's operations. As a result, OCC believes the proposal is consistent with the requirements of Rule 17Ad-22(e)(17)(i) under the Act.[22]

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.[23] The proposed Cybersecurity Confirmation would enhance the security, resiliency, and operational reliability of the endpoint security with respect to OCC's network or other connectivity because, as noted above, by making the Cybersecurity Confirmation an application requirement and an ongoing membership requirement, OCC would be able to prevent the connection by any Applicant, and take action against any Clearing Member, that may pose an increased cyber risk to OCC by not having a defined and ongoing

---

21 17 CFR 240.17Ad-22(e)(17)(i).

22 Id.

23 17 CFR 240.17Ad-22(e)(17)(ii).

cybersecurity program that meets appropriate standards. Clearing Members and Applicants that are not in alignment with a recognized framework, guideline, or standard that OCC believes is adequate to guide and assess such organization's cybersecurity program[24] may present increased risk to 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. OCC's controls are strengthened when OCC's Clearing Members have similar technology risk management controls and programs within their computing environment. Control weaknesses within a Clearing Member's environment could allow for malicious or unauthorized usage of the link between OCC and the Clearing Member. 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.[25]

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

OCC believes that the propose rule change could burden competition because it would require any Applicants that do not already have cybersecurity programs that meet the standards set out in the Cybersecurity Confirmation to incur additional costs including, but not limited to, establishing a cybersecurity program and framework, engaging an internal audit function or appropriate third party to review that program and framework, and remediating any findings from such review. In addition, those Clearing

---

24 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.

25 Id.

Members and Applicants that do not connect directly to OCC's network, but connect through a third party service provider or service bureau, would have the additional burden of evaluating the cyber risks and impact of these third parties and reviewing the third party's assurance reports.

As discussed above, all Clearing Members and Applicants are required to provide OCC with information concerning their program(s) for information security, encryption, incident notification, access controls, and control validations. OCC assesses this information prior to determining whether to permit the firm to access OCC's network and systems and on an ongoing basis thereafter. The proposed Cybersecurity Confirmation would establish new due diligence expectations with respect to firms' submission of required information. The set of standards against which OCC currently evaluates Clearing Member and Applicant cybersecurity programs is one of the acceptable standards and/or frameworks that OCC would recognize under the proposed attestation framework. OCC has completed security assessments for each of its Clearing Members and based on the firms' responses, OCC expects that all existing Clearing Members' cybersecurity programs currently align to at least one of the standards and/or frameworks that would be recognized under the proposed framework. Accordingly, OCC believes that any potential competitive burden would be limited to future Applicants that may have to implement process changes in order to meet the Cybersecurity Confirmation requirements.[26] OCC believes that any burden on competition for future Applicants that

---

[26] The proposed rule change would permit Clearing Members or Applicants to align their programs to one of several recognized standards and/or frameworks. OCC does not view this proposed optionality as burdening competition since it affords the Clearing Members and Applicants additional discretion they do not have today.

could be created by the proposed changes would be both necessary and appropriate in furtherance of the purposes of the Act, as permitted by Section 17A(b)(3)(I) of the Act, for the reasons described below.[27]

First, OCC believes the proposed rule change would be necessary in furtherance of the Act, specifically Section 17A(b)(3)(F) of the Act, because the Rules must be designed to 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.[28] By requiring that Clearing Members and Applicants provide a Cybersecurity Confirmation, the proposed rule change would allow OCC to better understand, assess, and, therefore, mitigate the cyber risks that OCC could face through its connections to its Clearing Members. As described above, these risks could impact OCC's ability to clear and settle securities transactions, or to safeguard the securities and funds which are in OCC's custody or control, or for which it is responsible. Enhancing its processes as described above would help to mitigate these risks, and therefore OCC believes the proposal is necessary in furtherance of the requirements of Section 17A(b)(3)(F) of the Act.[29]

The proposed changes are also necessary in furtherance of the purposes of Rules 17Ad-22(e)(17)(i) and (e)(17)(ii) under the Act.[30] The proposed Cybersecurity Confirmations would better enable OCC to identify potential sources of external operational risks and establish appropriate controls that would mitigate these risks and

---

27 15 U.S.C. 78q-1(b)(3)(I).

28 15 U.S.C. 78q-1(b)(3)(F).

29 Id.

30 17 CFR 240.17Ad-22(e)(17)(i) and (e)(17)(ii).

their possible impacts to OCC's operations. The proposed changes would also improve OCC's ability to ensure that its systems have a high degree of security, by enabling OCC to better identify the cybersecurity risks that may be presented to it by Clearing Members.

Second, OCC believes that the proposed rule change would be appropriate in furtherance of the purposes of the Act. The proposed rule change would apply equally to all Clearing Members and Applicants. As described above, OCC believes that all of its current Clearing Members may already be subject to one or more regulatory requirements or clearing agency rules that include the implementation of a cybersecurity program, and these firms would already follow a widely recognized framework, guideline, or standard to guide and assess their organization's cybersecurity program to comply with these regulations. OCC has assessed its current Clearing Members' programs and believes that all of them align to at least one of the recognized standards and/or frameworks listed in the Cybersecurity Confirmation. Therefore, OCC believes any burden that may be imposed by the proposed rule change would be appropriate.

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. Additionally, the proposed Cybersecurity Confirmation would provide differing options to conduct the review of the Clearing Member's or Applicant's cybersecurity program. As such, OCC has endeavored to design the Cybersecurity Confirmation in a way that is reasonable and does not require one approach for meeting its requirements, and which aligns with the due diligence requirements for cybersecurity programs and frameworks that were adopted by the DTCC Clearing Agencies.

Finally, OCC is proposing to provide Clearing Members with 180 calendar days' notice before the deadline to submit a completed Cybersecurity Confirmation. This notice period would allow Clearing Members to address any impact this change may have on their business. Applicants would be required to provide the Cybersecurity Confirmation as part of their application materials upon the effective date of this proposed rule change. The proposal is designed to provide all impacted Clearing Members with time to review their cybersecurity programs with respect to the required representations, and identify, if necessary, internal or third-party cybersecurity reviewers.

For the reasons described above, OCC believes any burden on competition that may result from the proposed rule change would be both necessary and appropriate in furtherance of the purposes of the Act, as permitted by Section 17A(b)(3)(I) of the Act.[31]

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

Written comments on the proposed rule change 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

Because the foregoing proposed rule change does not:

(i) significantly affect the protection of investors or the public interest;

(ii) impose any significant burden on competition; and

(iii) become operative for 30 days from the date on which it was filed, or such shorter time as the Commission may designate, it has become effective pursuant to Section 19(b)(3)(A)[32] of the Act and Rule 19b-4(f)(6)[33] thereunder.

---

31 15 U.S.C. 78q-1(b)(3)(I).

At any time within 60 days of the filing of the proposed rule change, the Commission summarily may temporarily suspend such rule change if it appears to the Commission that such action is necessary or appropriate in the public interest, for the protection of investors, or otherwise in furtherance of the purposes of the Act.

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 e-mail to rule-comments@sec.gov. Please include File Number SR-OCC-2022-008 on the subject line.

Paper Comments:

- Send paper comments in triplicate to Elizabeth M. Murphy, Secretary, Securities and Exchange Commission, 100 F Street, NE, Washington, DC 20549-1090.

All submissions should refer to File Number SR-OCC-2022-008. This file number should be included on the subject line if e-mail 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

---

[32] 15 U.S.C. 78s(b)(3)(A).

[33] 17 CFR 240.19b-4(f)(6).

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 Section, 100 F Street, N.E., 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; the Commission does not edit personal identifying information from submissions. You should submit only information that you wish to make available publicly.

All submissions should refer to File Number SR-OCC-2022-008 and should be submitted on or before [insert date 21 days from publication in the Federal Register].

For the Commission by the Division of Trading and Markets, pursuant to delegated authority.[34]

J. Matthew DeLesDernier
Assistant Secretary

[34] 17 CFR 200.30-3(a)(12).