for a Charged NMS Connection would defray expenses or why it is otherwise reasonably related to the cost to provide access to the NMS Network).

In addition, it is not clear from the information provided why it is equitable and not unfairly discriminatory for those Users that purchase access to the IP network or LCN on the proposed conditions to receive connections to the NMS Network at no additional charge, whereas other Users (e.g., those seeking connections to the NMS Network that do not satisfy the proposed conditions, or those who do not otherwise require access to the LCN or IP network) would be required to pay $10,000 initially and $11,000 or $18,000 monthly for a 10 Gb or 40 Gb connection, respectively. In particular, it is unclear the basis on which the Exchanges have determined the proposed conditions for making available a No Additional Fee NMS Network Connection, and whether that basis is reasonable, equitable, and not unfairly discriminatory as required by the Exchange Act.

Further, the Commission solicits additional comment on whether the Exchanges’ proposed fee structure for the NMS Network would impose a burden on competition that is not necessary or appropriate in furtherance of the purposes of the Act.

V. Commission’s Solicitation of Comments

The Commission requests that interested persons provide written submissions of their views, data, and arguments with respect to the issues identified above, as well as any other concerns they may have with the proposals. In particular, the Commission invites the written views of interested persons concerning whether the proposals are consistent with Sections 6(b)(4), 6(b)(5), 6(b)(8) or any other provision of the Act, or the rules and regulations thereunder. Although there do not appear to be any issues relevant to approval or disapproval that would be facilitated by an oral presentation of views, data, and arguments, the Commission will consider, pursuant to Rule 19b–4 under the Act, any request for an opportunity to make an oral presentation.

Interested persons are invited to submit written data, views, and arguments regarding whether the proposals should be approved or disapproved by January 3, 2020. Any person who wishes to file a rebuttal to any other person’s submission must file that rebuttal by January 17, 2020. 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

Paper Comments
- Send paper comments in triplicate to: Secretary, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549–1090. All submissions should refer to File Numbers SR–NYSE–2019–46, SR–NYSENAT–2019–19, SR–NYSEArca–2019–61, SR–NYSEArca–2019–34. 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 other 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 the filing also will be available for inspection and copying at the principal office of the Exchange. 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 Numbers SR–NYSE–2019–46, SR–NYSENAT–2019–19, SR–NYSEArca–2019–61, SR–NYSEArca–2019–34 and should be submitted on or before January 3, 2020.

For the Commission, by the Division of Trading and Markets, pursuant to delegated authority.\(^\text{14}\)

Jill M. Peterson,
Assistant Secretary.

[FR Doc. 2019–26846 Filed 12–12–19; 8:45 am]

BILLING CODE 8011–01–P

SECURITIES AND EXCHANGE COMMISSION


Self-Regulatory Organizations; National Securities Clearing Corporation; Order Approving a Proposed Rule Change To Require Confirmation of Cybersecurity Program

December 9, 2019.

I. Introduction

On October 15, 2019, National Securities Clearing Corporation (“NSCC”) filed with the Securities and Exchange Commission ("Commission"), pursuant to Section 19(b)(1) of the Securities Exchange Act of 1934 ("Act") \(^\text{1}\) and Rule 19b–4 thereunder, \(^\text{2}\) a proposed rule change SR–NSCC–2019–003. The proposed rule change was published for comment in the Federal Register on October 30, 2019.\(^\text{3}\) The Commission did not receive any comment letters on the proposed rule change. For the reasons discussed below, the Commission is approving the proposed rule change.

II. Description of the Proposed Rule Change

NSCC proposes to modify its Rules and Procedures (“Rules”) \(^\text{4}\) in order to (1) define the term “Cybersecurity Confirmation” as a written representation that addresses a submitting entity’s cybersecurity program (described more fully below); [FR Doc. 2019–26846 Filed 12–12–19; 8:45 am]

BILLING CODE 8011–01–P

\(^{1}\) 17 CFR 200.30–3(a)(12).


\(^{5}\) Capitalized terms not defined herein are defined in the Rules, available at http://www.dlcc.com/legal/rules-and-procedures. References to “members” in this Order include both Members and Limited Members, as such terms are defined in the Rules.
against cyberattacks. Accordingly, such entities would currently be required to follow standards established by national or international organizations focused on information security management, and they would currently maintain protocols for their senior management to verify the existence of cybersecurity programs sufficient to meet regulatory obligations. NSCC further believes that some of its members, applicants for membership, and trade data reporting organizations might also currently follow protocols substantially similar to the regulations referred to earlier in this paragraph in order to meet the evolving cybersecurity expectations of regulators and/or their own institutional customers.

Although NSCC believes that its members, applicants for membership, and trade data reporting organizations may currently maintain robust cybersecurity programs, NSCC seeks to better ensure the protection of its network by requiring its members, applicants for membership, and trade data reporting organizations to confirm that they are meeting certain cybersecurity standards in order to connect to NSCC via the SMART network or other means. Therefore, NSCC proposes to require all members, applicants for membership, and certain trade data reporting organizations to submit a written Cybersecurity Confirmation that includes specific representations regarding the submitting entity’s cybersecurity program and framework. NSCC states that the information contained in the Cybersecurity Confirmation would help NSCC to better understand the cybersecurity programs and frameworks of entities seeking to connect to NSCC, and thereby identify possible cyber risk exposures. As a result, NSCC would be better able to establish appropriate controls to mitigate such risks and their possible impacts on NSCC’s operations.

B. Proposed Changes

NSCC proposes to modify its Rules to:
(1) Provide a detailed definition of the Cybersecurity Confirmation;
(2) require NSCC’s members and applicants for membership to submit to NSCC a Cybersecurity Confirmation (both as part of an initial application for membership, and on an ongoing basis for members, at least every two years); and
(3) provide that NSCC may require a Cybersecurity Confirmation from organizations that report trade data to NSCC. Each of these proposed rule changes is described in greater detail below.

1. Cybersecurity Confirmation

NSCC proposes to define the term “Cybersecurity Confirmation” to mean a written form, in a format provided by NSCC and signed by the submitting entity’s designated senior executive with the authority to attest to the cybersecurity matters contained in the form. The form would contain specific representations regarding the submitting entity’s cybersecurity program and framework. Such representations would cover the two years prior to the date of the most recently provided Cybersecurity Confirmation. The Cybersecurity Confirmation would include the following representations:

• The submitting entity has implemented and maintains a comprehensive cybersecurity program and framework that considers potential cyber threats that impact the submitting entity’s organization, and protects the confidentiality, integrity, and availability requirements of its systems and information.
• The submitting entity has implemented and maintains a written enterprise cybersecurity policy or policies approved by the submitting entity’s senior management or board of directors, and the submitting entity’s cybersecurity framework is in alignment with standard industry best practices and guidelines.

See FSOC 2012 Report, supra note 5.
See FSOC 2012 Report, supra note 5.
The submitting entity’s cybersecurity program and framework protects the segment of its system that connects to and/or interacts with NSCC. The submitting entity has in place an established process to remediate cyber issues identified to meet its regulatory and/or statutory requirements.

The submitting entity periodically updates the risk processes of its cybersecurity program and framework based on a risk assessment or changes to technology, business, threat ecosystem, and/or regulatory environment.

The submitting entity’s cybersecurity program and framework has been reviewed by one of the following: (1) The submitting entity, 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;13 (2) a regulator who assesses the submitting entity’s cybersecurity program and framework against an industry cybersecurity framework or industry standard, including those that are listed on the Cybersecurity Confirmation form and in an Important Notice that is issued by NSCC from time to time;14 (3) an independent external entity with cybersecurity domain expertise in relevant industry standards and practices, including those that are listed on the Cybersecurity Confirmation form and in an Important Notice that is issued by NSCC from time to time;15 or (4) an independent internal audit function reporting directly to the submitting entity’s board of directors or designated board of directors committee, such that the findings of that review are shared with these governance bodies.

NSCC states that it designed the representations in the Cybersecurity Confirmation to provide information on how each submitting entity manages cybersecurity with respect to its connectivity to NSCC.16 NSCC believes that by requiring these representations from members, applicants for membership, and trade data reporting organizations, the proposed Cybersecurity Confirmation would provide useful information designed to enable NSCC to make informed decisions about risks or threats, perform additional monitoring, target potential vulnerabilities, and otherwise protect the NSCC network.17

2. Initial and Ongoing Membership Requirement

NSCC proposes to require new applicants for NSCC membership to submit a Cybersecurity Confirmation as part of their application materials. NSCC also proposes to require all NSCC members to submit a Cybersecurity Confirmation at least every two years. With respect to the requirement to submit a Cybersecurity Confirmation at least every two years, NSCC would provide all members with notice of the date on which the Cybersecurity Confirmation would be due no later than 180 calendar days prior to the due date.

3. Organizations Reporting Trade Data to NSCC

NSCC proposes to modify the Rules to provide that, when determining whether to accept trade data from an organization for comparison and trade recording,18 NSCC may require the organization to submit a Cybersecurity Confirmation. Since such organizations are not NSCC members, contracts (i.e., separate from the Rules) govern the relationships between NSCC and such organizations. NSCC states that this proposal would provide transparency regarding the steps NSCC may take when determining whether to accept trade data from such organizations.19

C. Implementation Timeframe

The proposed rule change would be effective upon Commission approval. New applicants for NSCC membership would be required to submit a Cybersecurity Confirmation as part of their application materials. The requirement to submit a Cybersecurity Confirmation would also apply to applicants whose applications are pending with NSCC at the time the Commission approves the proposed rule change. For existing NSCC members, NSCC would provide notice of the due date to submit a Cybersecurity Confirmation, not later than 180 days prior to the due date. Finally, NSCC would provide such notice to its members at least every two years going forward.

III. Discussion and Commission Findings

Section 19(b)(2)(C) of the Act20 directs the Commission to approve a proposed rule change of a self-regulatory organization if it finds that such proposed rule change is consistent with the requirements of the Act and rules and regulations thereunder applicable to such organization. After carefully considering the proposed rule change, the Commission finds that the proposed rule change is consistent with the requirements of the Act and the rules and regulations thereunder applicable to NSCC. In particular, the Commission finds that the proposed rule change is consistent with Section 17A(b)(3)(F) of the Act,21 and Rules 17Ad–22(e)(17)(i) and (e)(17)(ii) promulgated under the Act,22 for the reasons described below.

A. Consistency With Section 17A(b)(3)(F) of the Act

Section 17A(b)(3)(F) of the Act requires that the rules of a clearing agency 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

---

13 23 N.Y.C.R.R. § 23, §500 et seq. (2017). NSCC states that this regulation requires entities to confirm that they have comprehensive cybersecurity programs as described in the regulation, and NSCC believes this regime is sufficient to meet the objectives of the proposed Cybersecurity Confirmation. Notice, supra note 3, at 58184.

14 NSCC states that current industry cybersecurity frameworks and industry standards could include, for example, the Office of the Comptroller of the Currency or the FFIEC Cybersecurity Assessment Tool. NSCC would identify acceptable industry cybersecurity frameworks and standards in the Cybersecurity Confirmation form and in an Important Notice that NSCC would issue from time to time. NSCC would also consider accepting other industry cybersecurity frameworks and standards upon request. Notice, supra note 3, at 58185.

15 NSCC states that a third party with cybersecurity domain expertise is one that follows and understands applicable industry standards, practices, and regulations, such as ISO 27001 certification or NIST CSF assessment. NSCC would identify acceptable industry standards and practices in the Cybersecurity Confirmation form and in an Important Notice that NSCC would issue from time to time. NSCC would also consider accepting other industry standards and practices upon request. Notice, supra note 3, at 58185.

16 Id.

17 See Rule 7 (Comparison and Trade Recording Operation), supra note 4.

18 Notice, supra note 3, at 58185.


21 17 CFR 240.17Ad–22(e)(17)(i) and (e)(17)(ii).

22 17 CFR 240.17Ad–22(e)(17)(i) and (e)(17)(ii).
As described above, NSCC proposes to require its members, applicants for membership, and trade data reporting organizations seeking to connect to NSCC via the SMART network or other means, to submit a Cybersecurity Confirmation, confirming the existence and nature of their cybersecurity programs. The Cybersecurity Confirmation would provide NSCC with useful information regarding the cybersecurity programs of the submitting entities. By conditioning an entity’s connectivity to NSCC via the SMART network or other means on the submission of a Cybersecurity Confirmation, NSCC should be better enabled to reduce the cyber risks of electronically connecting to entities that have not confirmed the existence and nature of their cybersecurity programs. Accordingly, the proposed Cybersecurity Confirmation requirement should provide NSCC with information to better identify its exposure to cyber risks and to take steps to mitigate those risks.

If not adequately addressed, the risk of cyberattacks and other cyber vulnerabilities could affect NSCC’s network and NSCC’s ability to clear and settle securities transactions, or to safeguard the securities and funds which are in NSCC’s custody or control, or for which it is responsible. The proposed Cybersecurity Confirmation requirement is a tool designed to address those risks as described above. Therefore, the Commission finds the proposed Cybersecurity Confirmation requirement 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 NSCC or for which it is responsible, consistent with the requirements of Section 17A(b)(3)(F) of the Act.

B. Consistency With Rule 17Ad–22(e)(17)(i) Under the Act

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.

SECURITIES AND EXCHANGE COMMISSION


Self-Regulatory Organizations; NYSE Arca, Inc.; Notice of Filing and Immediate Effectiveness of Proposed Rule Change Amending the NYSE Arca Options Fees and Charges and the NYSE Arca Equities Fees and Charges Related to Co-Location Services

December 9, 2019.

Pursuant to Section 19(b)(1) of the Securities Exchange Act of 1934 (the “Act”) and Rule 19b–4 thereunder, notice is hereby given that, on