

SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

For complete Form 19b-4 instructions please refer to the EFFF website.

Form 19b-4 Information *

Add Remove View

The self-regulatory organization must provide all required information, presented in a clear and comprehensible manner, to enable the public to provide meaningful comment on the proposal and for the Commission to determine whether the proposal is consistent with the Act and applicable rules and regulations under the Act.

Exhibit 1 - Notice of Proposed Rule Change *

Add Remove View

The Notice section of this Form 19b-4 must comply with the guidelines for publication in the Federal Register as well as any requirements for electronic filing as published by the Commission (if applicable). The Office of the Federal Register (OFR) offers guidance on Federal Register publication requirements in the Federal Register Document Drafting Handbook, October 1998 Revision. For example, all references to the federal securities laws must include the corresponding cite to the United States Code in a footnote. All references to SEC rules must include the corresponding cite to the Code of Federal Regulations in a footnote. All references to Securities Exchange Act Releases must include the release number, release date, Federal Register cite, Federal Register date, and corresponding file number (e.g., SR-[SRO]-xx-xx). A material failure to comply with these guidelines will result in the proposed rule change being deemed not properly filed. See also Rule 0-3 under the Act (17 CFR 240.0-3)

Exhibit 1A- Notice of Proposed Rule Change, Security-Based Swap Submission, or Advance Notice by Clearing Agencies *

Add Remove View

The Notice section of this Form 19b-4 must comply with the guidelines for publication in the Federal Register as well as any requirements for electronic filing as published by the Commission (if applicable). The Office of the Federal Register (OFR) offers guidance on Federal Register publication requirements in the Federal Register Document Drafting Handbook, October 1998 Revision. For example, all references to the federal securities laws must include the corresponding cite to the United States Code in a footnote. All references to SEC rules must include the corresponding cite to the Code of Federal Regulations in a footnote. All references to Securities Exchange Act Releases must include the release number, release date, Federal Register cite, Federal Register date, and corresponding file number (e.g., SR-[SRO]-xx-xx). A material failure to comply with these guidelines will result in the proposed rule change, security-based swap submission, or advance notice being deemed not properly filed. See also Rule 0-3 under the Act (17 CFR 240.0-3)

Exhibit 2 - Notices, Written Comments, Transcripts, Other Communications

Add Remove View

Exhibit Sent As Paper Document

Copies of notices, written comments, transcripts, other communications. If such documents cannot be filed electronically in accordance with Instruction F, they shall be filed in accordance with Instruction G.

Exhibit 3 - Form, Report, or Questionnaire

Add Remove View

Exhibit Sent As Paper Document

Copies of any form, report, or questionnaire that the self-regulatory organization proposes to use to help implement or operate the proposed rule change, or that is referred to by the proposed rule change.

Exhibit 4 - Marked Copies

Add Remove View

The full text shall be marked, in any convenient manner, to indicate additions to and deletions from the immediately preceding filing. The purpose of Exhibit 4 is to permit the staff to identify immediately the changes made from the text of the rule with which it has been working.

Exhibit 5 - Proposed Rule Text

Add Remove View

The self-regulatory organization may choose to attach as Exhibit 5 proposed changes to rule text in place of providing it in Item I and which may otherwise be more easily readable if provided separately from Form 19b-4. Exhibit 5 shall be considered part of the proposed rule change.

Partial Amendment

Add Remove View

If the self-regulatory organization is amending only part of the text of a lengthy proposed rule change, it may, with the Commission's permission, file only those portions of the text of the proposed rule change in which changes are being made if the filing (i.e. partial amendment) is clearly understandable on its face. Such partial amendment shall be clearly identified and marked to show deletions and additions.

1. Text of the Proposed Rule Change

(a) The proposed rule change of National Securities Clearing Corporation (“NSCC”) is annexed hereto as Exhibit 5 and consists of modifications to NSCC’s Rules and Procedures (“Rules”)¹ in order to (1) define “Cybersecurity Confirmation” as a signed, written representation that addresses the submitting firm’s cybersecurity program; (2) enhance the NSCC application requirements and ongoing requirements for Members to (a) require that a Cybersecurity Confirmation be provided as part of the application materials for all Members, and (b) require that all Members deliver to NSCC a complete, updated Cybersecurity Confirmation at least every two years; and (3) provide that NSCC may require a Cybersecurity Confirmation from organizations that report trade data to NSCC for comparison and trade recording, as described in greater detail below.

(b) Not applicable.

(c) Not applicable.

2. Procedures of the Self-Regulatory Organization

The proposed rule change was approved by the Risk Committee of the Board of Directors of NSCC at a meeting duly called and held on December 19, 2017.

3. Self-Regulatory Organization’s Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change

(a) Purpose

(i) Overview

NSCC 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; (2) enhance the NSCC application requirements and ongoing requirements for Members to (a) require that a Cybersecurity Confirmation be provided as part of the application materials for all Members, and (b) require that all Members deliver to NSCC a complete, updated Cybersecurity Confirmation at least every two years; and (3) provide that NSCC may require a Cybersecurity Confirmation from organizations that report trade data to NSCC for comparison and trade recording.

The proposed change would require all Members and applicants to deliver to NSCC a signed, written Cybersecurity Confirmation, which includes representations regarding the submitting firm’s cybersecurity program and framework. The Cybersecurity Confirmation would be required to be (1) delivered with the application materials for every applicant for membership, and (2) updated and re-delivered at least every two years by all Members. NSCC is

¹ Capitalized terms not defined herein are defined in the Rules, available at <http://www.dtcc.com/legal/rules-and-procedures>. References to “Members” in this filing include both Members and Limited Members, as such terms are defined in the Rules.

also proposing to modify the Rules to provide that it may require any organization from which it may accept trade data for comparison and trade recording to deliver a Cybersecurity Confirmation.

As described in more detail below, the Cybersecurity Confirmation would help NSCC to assess the cybersecurity risks that may be introduced to it by Members and other entities that connect to NSCC either through the Securely Managed and Reliable Technology (“SMART”) network² or through other connections. The proposed Cybersecurity Confirmation would allow NSCC to better understand its Members’ cybersecurity programs and frameworks and identify possible cybersecurity risk exposures. Based on this information, NSCC would be able to establish appropriate controls to mitigate these risks and their possible impacts to NSCC’s operations.

(ii) Background of Proposal

NSCC believes it is prudent to better understand the cybersecurity risks that it may face through its interconnections to Members. As a designated systemically important financial market utility, or “SIFMU,” NSCC occupies a unique position in the marketplace such that a failure or a disruption to NSCC 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.³ Given its designation as a SIFMU, NSCC believes it is prudent to develop an enhanced endpoint security framework designed so that its SMART network or other connectivity is adequately protected against cyberattacks.

Currently, NSCC does not obtain any information regarding the security of a firm’s systems or cybersecurity program prior to permitting that firm to connect either directly to the SMART network or to NSCC through another means, such as through a third party service provider, service bureau, network, or the Internet. Given NSCC’s critical role in the marketplace, NSCC is proposing to address the risks that could be posed by these connections.

² The SMART network is a technology managed by NSCC’s parent company, The Depository Trust & Clearing Corporation (“DTCC”), that connects a nationwide complex of networks, processing centers and control facilities. This network extends between NSCC’s and its Members’ operating premises. DTCC operates on a shared services model with respect to NSCC and DTCC’s other subsidiaries pursuant to intercompany agreements under which it is generally DTCC that provides a relevant service to its subsidiaries, including NSCC.

³ NSCC and its affiliates, The Depository Trust Company (“DTC”) and Fixed Income Clearing Corporation (“FICC”), were designated SIFMUs under Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010. 12 U.S.C. 5465(e)(1).

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.⁴ In order to comply with such regulations, 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 cybersecurity programs in place to fulfill existing regulatory obligations. Other 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. NSCC believes that it should require confirmation of the cybersecurity standards utilized by its Members and applicants that connect to its network.

The proposed Cybersecurity Confirmation would require Members and applicants to represent that they have established adequate controls and security to help limit (1) cybersecurity risks to NSCC and to the other Members' networks and (2) access by unauthorized third parties while the firm is connected to NSCC either directly through the SMART network or through other connectivity such as a service provider, service bureau, network, or the Internet.

(iii) *Proposed Rule Changes*

NSCC is proposing to modify its Rules to (1) define "Cybersecurity Confirmation;" (2) require that firms deliver a completed Cybersecurity Confirmation (a) as part of their initial application with NSCC, and (b) on an ongoing basis, 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) *Proposed Cybersecurity Confirmation*

NSCC is proposing to adopt a definition of "Cybersecurity Confirmation." Each Cybersecurity Confirmation would be required to be in writing on a form provided by NSCC 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 NSCC, each Cybersecurity Confirmation would contain representations regarding the submitting firm's cybersecurity program and framework. Such

⁴ For example, depending on the type of entity, Members 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).

representations by the submitting firm would cover the two years prior to the date of the most recently provided Cybersecurity Confirmation.

NSCC 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 the 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 the submitting firm's senior management or board of directors, and the organization's cybersecurity framework is in alignment with standard industry best practices and guidelines.⁵

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 NSCC, 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 their system that connects to and/or interacts with NSCC.

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

⁵ Examples of recognized frameworks, guidelines and standards that NSCC 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. NSCC would identify recognized frameworks, guidelines and standards in the form of Cybersecurity Confirmation and in an Important Notice that NSCC would issue from time to time. NSCC would also consider accepting other standards upon request by a Member or applicant.

on a risk assessment or changes to technology, business, threat ecosystem, and/or regulatory environment.

And, finally, 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;⁶ (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 Important Notice that is issued by NSCC from time to time;⁷ (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 Important Notice that is issued by NSCC from time to time;⁸ 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 NSCC with evidence of each Member's or applicant's management of cybersecurity with respect to their connectivity to NSCC. By requiring these representations from Members and applicants, the proposed Cybersecurity Confirmation would provide NSCC with information that it could use to make decisions about risks or threats, perform additional monitoring, target potential vulnerabilities, and protect the NSCC network.

⁶ 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 NSCC believes is sufficient to meet the objectives of the proposed Cybersecurity Confirmation.

⁷ 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 form of Cybersecurity Confirmation 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 by a Member or applicant.

⁸ 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. NSCC would identify acceptable industry standards and practices in the form of Cybersecurity Confirmation 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 by a Member or applicant.

NSCC is proposing to amend Rule 1 (Definitions and Descriptions) of the Rules to include a definition of “Cybersecurity Confirmation” as described above.

(2) *Initial and Ongoing Membership Requirement*

NSCC is proposing to require that a Cybersecurity Confirmation be submitted to NSCC by any applicant, as part of their application materials, and at least every two years by all Members. With respect to the requirement to deliver a Cybersecurity Confirmation at least every two years, NSCC would provide all Members with notice of the date on which such Cybersecurity Confirmations would be due no later than 180 calendar days prior to such due date.

In order to implement these proposed changes, NSCC would amend Rule 2A (Initial Membership Requirements), Section 1.C of the Rules to require applicants to complete and deliver a Cybersecurity Confirmation as part of their application materials. Further, NSCC would amend Rule 2B (Ongoing Membership Requirements and Monitoring), Section 2.A of the Rules to require each Member to complete and deliver a Cybersecurity Confirmation at least every two years, on a date that is set by NSCC and following notice that is provided no later than 180 calendar days prior to such due date.

(3) *Organizations Reporting Trade Data to NSCC*

NSCC is also proposing to modify the Rules to provide that, when determining whether to accept trade data from an organization for comparison and trade recording, as provided for under Rule 7 (Comparison and Trade Recording Operation) of the Rules, NSCC may require such organization to provide a Cybersecurity Confirmation. These organizations are not Members of NSCC and, as such, NSCC’s relationship with these organizations is governed by a contract that is separate from the Rules. Therefore, this change would provide transparency regarding the steps NSCC may take when determining whether to accept trade data from another organization.

To implement this change, NSCC would amend Rule 7 (Comparison and Trade Recording Operation), Section 6 of the Rules to provide that NSCC may require organizations that deliver trade data to NSCC as described in that Rule to provide a Cybersecurity Confirmation before agreeing to accept such trade data.

(iv) *Implementation Timeframe*

Subject to approval by the Securities and Exchange Commission (“Commission”), the proposed rule change would become effective immediately. The proposed requirement that applicants deliver a Cybersecurity Confirmation with their application materials would be implemented immediately and 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, NSCC would provide Members with notice of the due date of their Cybersecurity Confirmations, no later than 180 days prior to such due date, and would provide such notice at least every two years going forward.

(b) Statutory Basis

NSCC 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, NSCC believes that the proposed rule changes are consistent with Section 17A(b)(3)(F) of the Act,⁹ and Rules 17Ad-22(e)(17)(i) and (e)(17)(ii), each promulgated under the Act,¹⁰ for the reasons described below.

Section 17A(b)(3)(F) of the Act requires that the rules of NSCC 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.¹¹

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

Risks, threats and potential vulnerabilities could impact NSCC'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 implementing a tool that would help to mitigate these risks, NSCC 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.¹²

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

⁹ 15 U.S.C. 78q-1(b)(3)(F).

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

¹¹ 15 U.S.C. 78q-1(b)(3)(F).

¹² Id.

appropriate systems, policies, procedures, and controls.¹³ The proposed Cybersecurity Confirmation would reduce cybersecurity risks to NSCC by requiring all 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 NSCC to mitigate its exposure to cybersecurity risk and, thereby, decrease the operational risks to NSCC that are presented by connections to NSCC through the SMART network or otherwise. The proposed Cybersecurity Confirmations would identify to NSCC potential sources of external operational risks and enable it to mitigate these risks and their possible impacts to NSCC's operations. As a result, NSCC believes the proposal is consistent with the requirements of Rule 17Ad-22(e)(17)(i) under the Act.¹⁴

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.¹⁵ The proposed Cybersecurity Confirmation would enhance the security, resiliency, and operational reliability of the endpoint security with respect to the SMART network or other connectivity because, as noted above, by making the Cybersecurity Confirmation an application requirement and an ongoing membership requirement, NSCC would be able to prevent the connection by any applicant, and take action against any Member, that may pose an increased cyber risk to NSCC by not having a defined and ongoing cybersecurity program that meets appropriate standards. Members or applicants that are not in alignment with a recognized framework, guideline, or standard that NSCC believes is adequate to guide and assess such organization's cybersecurity program may present increased risk to NSCC. By enabling NSCC to identify these risks, the proposed changes would allow NSCC to more effectively secure its environment against potential vulnerabilities. NSCC's controls are strengthened when NSCC's Members, and other organizations that connect to NSCC, have similar technology risk management controls and programs within their computing environment. Control weaknesses within a Member's environment could allow for malicious or unauthorized usage of the link between NSCC and the Member. As a result, NSCC believes the proposal would improve NSCC'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.¹⁶

4. Self-Regulatory Organization's Statement on Burden on Competition

NSCC believes the proposed rule change could have an impact on competition. Specifically, NSCC believes that the proposed rule change could burden competition because it would require Members and applicants that do not already have cybersecurity programs that

¹³ 17 CFR 240.17Ad-22(e)(17)(i).

¹⁴ Id.

¹⁵ 17 CFR 240.17Ad-22(e)(17)(ii).

¹⁶ Id.

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 Members and applicants that do not connect directly to the SMART 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.

NSCC believes the above described burden on competition that 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.¹⁷

First, NSCC 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.¹⁸ By requiring Members and applicants to provide a Cybersecurity Confirmation, the proposed rule change would allow NSCC to better understand, assess, and, therefore, mitigate the cyber risks that NSCC could face through its connections to its Members. As described above, these risks could impact 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. Implementing a tool as described above would help to mitigate these risks, and therefore NSCC believes the proposal is necessary in furtherance of the requirements of Section 17A(b)(3)(F) of the Act.¹⁹

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.²⁰ The proposed Cybersecurity Confirmations would identify to NSCC potential sources of external operational risks and allow it to establish appropriate controls that would mitigate these risks and their possible impacts to NSCC's operations. The proposed changes would also improve NSCC's ability to ensure that its systems have a high degree of security, by enabling NSCC to identify the cybersecurity risks that may be presented to it by Members and other entities that connect to NSCC.

Second, NSCC 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 Members and applicants. As described above, NSCC believes Members may already be subject to one or more regulatory requirements 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

¹⁷ 15 U.S.C. 78q-1(b)(3)(I).

¹⁸ 15 U.S.C. 78q-1(b)(3)(F).

¹⁹ Id.

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

regulations. Therefore, NSCC believes any burden that may be imposed by the proposed rule change would be appropriate.

Further, while the proposed Cybersecurity Confirmation would identify certain standards and guidelines that would be appropriate, NSCC would consider requests by applicants and Members to allow other standards in accepting a Cybersecurity Confirmation. Additionally, the proposed Cybersecurity Confirmation would provide differing options to conduct the review of the applicant's or Member's cybersecurity program. As such, NSCC has endeavored to design the Cybersecurity Confirmation in a way that is reasonable and does not require one approach for meeting its requirements.

Finally, NSCC is proposing to provide Members with a minimum of 180 calendar days' notice before the deadline for providing a Cybersecurity Confirmation. This notice would allow 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. This implementation schedule is designed to be fair and not disproportionately impact any Members more than others. The proposal is designed to provide all impacted 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, NSCC 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.²¹

5. Self-Regulatory Organization's Statement on Comments on the Proposed Rule Change Received from Members, Participants, or Others

NSCC has not solicited or received any written comments relating to this proposal. NSCC will notify the Commission of any written comments received.

6. Extension of Time Period for Commission Action

NSCC does not consent to an extension of the time period specified in Section 19(b)(2) of the Act²² for Commission action.

7. Basis for Summary Effectiveness Pursuant to Section 19(b)(3) or for Accelerated Effectiveness Pursuant to Section 19(b)(2) or Section 19(b)(7)(D)

(a) Not applicable.

(b) Not applicable.

²¹ 15 U.S.C. 78q-1(b)(3)(I).

²² 15 U.S.C. 78s(b)(2).

(c) Not applicable.

(d) Not applicable.

8. Proposed Rule Change Based on Rules of Another Self-Regulatory Organization or of the Commission

While the proposal is not based on the rules of another self-regulatory organization or of the Commission, NSCC's affiliates, DTC and FICC, have each filed similar proposals concurrently with this filing to adopt comparable rule changes.

9. Security-Based Swap Submissions Filed Pursuant to Section 3C of the Act

Not applicable.

10. Advance Notices Filed Pursuant to Section 806(e) of the Payment, Clearing and Settlement Supervision Act

Not applicable.

11. Exhibits

Exhibit 1 – Not applicable.

Exhibit 1A – Notice of proposed rule change for publication in the Federal Register.

Exhibit 2 – Not applicable.

Exhibit 3 – NSCC Cybersecurity Confirmation form.

Exhibit 4 – Not applicable.

Exhibit 5 – Proposed changes to the Rules.

EXHIBIT 1A

SECURITIES AND EXCHANGE COMMISSION
(Release No. 34-[_____]; File No. SR-NSCC-2019-003)

[DATE]

Self-Regulatory Organizations; National Securities Clearing Corporation; Notice of Filing of Proposed Rule Change to Require Confirmation of Cybersecurity 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 October __, 2019, National Securities Clearing Corporation (“NSCC”) 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 by the clearing agency. 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 consists of modifications to NSCC’s Rules and Procedures (“Rules”)³ in order to (1) define “Cybersecurity Confirmation” as a signed, written representation that addresses the submitting firm’s cybersecurity program; (2) enhance the NSCC application requirements and ongoing requirements for Members to (a) require that a Cybersecurity Confirmation be provided as part of the application

¹ 15 U.S.C. 78s(b)(1).

² 17 CFR 240.19b-4.

³ Capitalized terms not defined herein are defined in the Rules, available at <http://www.dtcc.com/legal/rules-and-procedures>. References to “Members” in this filing include both Members and Limited Members, as such terms are defined in the Rules.

materials for all Members, and (b) require that all Members deliver to NSCC a complete, updated Cybersecurity Confirmation at least every two years; and (3) provide that NSCC may require a Cybersecurity Confirmation from organizations that report trade data to NSCC for comparison and trade recording, as described in greater detail below.

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

In its filing with the Commission, the clearing agency 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. The clearing agency 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

1. Purpose

(i) Overview

NSCC 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; (2) enhance the NSCC application requirements and ongoing requirements for Members to (a) require that a Cybersecurity Confirmation be provided as part of the application materials for all Members, and (b) require that all Members deliver to NSCC a complete, updated Cybersecurity Confirmation at least every two years; and (3) provide that NSCC may require a Cybersecurity Confirmation from organizations that report trade data to NSCC for comparison and trade recording.

The proposed change would require all Members and applicants to deliver to NSCC a signed, written Cybersecurity Confirmation, which includes representations regarding the submitting firm's cybersecurity program and framework. The Cybersecurity Confirmation would be required to be (1) delivered with the application materials for every applicant for membership, and (2) updated and re-delivered at least every two years by all Members. NSCC is also proposing to modify the Rules to provide that it may require any organization from which it may accept trade data for comparison and trade recording to deliver a Cybersecurity Confirmation.

As described in more detail below, the Cybersecurity Confirmation would help NSCC to assess the cybersecurity risks that may be introduced to it by Members and other entities that connect to NSCC either through the Securely Managed and Reliable Technology ("SMART") network⁴ or through other connections. The proposed Cybersecurity Confirmation would allow NSCC to better understand its Members' cybersecurity programs and frameworks and identify possible cybersecurity risk exposures. Based on this information, NSCC would be able to establish appropriate controls to mitigate these risks and their possible impacts to NSCC's operations.

(ii) *Background of Proposal*

NSCC believes it is prudent to better understand the cybersecurity risks that it may face through its interconnections to Members. As a designated systemically

⁴ The SMART network is a technology managed by NSCC's parent company, The Depository Trust & Clearing Corporation ("DTCC"), that connects a nationwide complex of networks, processing centers and control facilities. This network extends between NSCC's and its Members' operating premises. DTCC operates on a shared services model with respect to NSCC and DTCC's other subsidiaries pursuant to intercompany agreements under which it is generally DTCC that provides a relevant service to its subsidiaries, including NSCC.

important financial market utility, or “SIFMU,” NSCC occupies a unique position in the marketplace such that a failure or a disruption to NSCC 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.⁵ Given its designation as a SIFMU, NSCC believes it is prudent to develop an enhanced endpoint security framework designed so that its SMART network or other connectivity is adequately protected against cyberattacks.

Currently, NSCC does not obtain any information regarding the security of a firm’s systems or cybersecurity program prior to permitting that firm to connect either directly to the SMART network or to NSCC through another means, such as through a third party service provider, service bureau, network, or the Internet. Given NSCC’s critical role in the marketplace, NSCC is proposing to address the risks that could be posed by these connections.

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.⁶

⁵ NSCC and its affiliates, The Depository Trust Company and Fixed Income Clearing Corporation, were designated SIFMUs under Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010. 12 U.S.C. 5465(e)(1).

⁶ For example, depending on the type of entity, Members 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 Act, known as the “Market Access Rule,” which requires broker-dealers to establish,

In order to comply with such regulations, 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 cybersecurity programs in place to fulfill existing regulatory obligations. Other 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. NSCC believes that it should require confirmation of the cybersecurity standards utilized by its Members and applicants that connect to its network.

The proposed Cybersecurity Confirmation would require Members and applicants to represent that they have established adequate controls and security to help limit (1) cybersecurity risks to NSCC and to the other Members' networks and (2) access by unauthorized third parties while the firm is connected to NSCC either directly through the SMART network or through other connectivity such as a service provider, service bureau, network, or the Internet.

(iii) *Proposed Rule Changes*

NSCC is proposing to modify its Rules to (1) define "Cybersecurity Confirmation;" (2) require that firms deliver a completed Cybersecurity Confirmation (a) as part of their initial application with NSCC, and (b) on an ongoing basis, at least every two years; and (3) provide that NSCC may require a Cybersecurity Confirmation

document, and maintain a system for regularly reviewing the effectiveness of its management controls and supervisory procedures (17 CFR 240.15c3-5).

from organizations that report trade data to NSCC. Each of these proposed rule changes is described in greater detail below.

(1) *Proposed Cybersecurity Confirmation*

NSCC is proposing to adopt a definition of “Cybersecurity Confirmation.” Each Cybersecurity Confirmation would be required to be in writing on a form provided by NSCC 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 NSCC, each Cybersecurity Confirmation would contain representations regarding the submitting firm’s cybersecurity program and framework. Such representations by the submitting firm would cover the two years prior to the date of the most recently provided Cybersecurity Confirmation.

NSCC 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 the 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 the submitting firm’s senior management or board of directors,

and the organization's cybersecurity framework is in alignment with standard industry best practices and guidelines.⁷

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 NSCC, 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 their system that connects to and/or interacts with NSCC.

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.

⁷ Examples of recognized frameworks, guidelines and standards that NSCC 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. NSCC would identify recognized frameworks, guidelines and standards in the form of Cybersecurity Confirmation and in an Important Notice that NSCC would issue from time to time. NSCC would also consider accepting other standards upon request by a Member or applicant.

And, finally, 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;⁸ (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 Important Notice that is issued by NSCC from time to time;⁹ (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 Important Notice that is issued by NSCC from time to time;¹⁰ or (4) an independent internal audit

⁸ 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 NSCC believes is sufficient to meet the objectives of the proposed Cybersecurity Confirmation.

⁹ 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 form of Cybersecurity Confirmation 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 by a Member or applicant.

¹⁰ 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. NSCC would identify acceptable industry standards and practices in the form of Cybersecurity Confirmation 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 by a Member or applicant.

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

NSCC is proposing to amend Rule 1 (Definitions and Descriptions) of the Rules to include a definition of "Cybersecurity Confirmation" as described above.

(2) *Initial and Ongoing Membership Requirement*

NSCC is proposing to require that a Cybersecurity Confirmation be submitted to NSCC by any applicant, as part of their application materials, and at least every two years by all Members. With respect to the requirement to deliver a Cybersecurity Confirmation at least every two years, NSCC would provide all Members with notice of the date on which such Cybersecurity Confirmations would be due no later than 180 calendar days prior to such due date.

In order to implement these proposed changes, NSCC would amend Rule 2A (Initial Membership Requirements), Section 1.C of the Rules to require applicants to complete and deliver a Cybersecurity Confirmation as part of their application materials. Further, NSCC would amend Rule 2B (Ongoing Membership Requirements and Monitoring), Section 2.A of the Rules to require each Member to complete and deliver a

Cybersecurity Confirmation at least every two years, on a date that is set by NSCC and following notice that is provided no later than 180 calendar days prior to such due date.

(3) *Organizations Reporting Trade Data to NSCC*

NSCC is also proposing to modify the Rules to provide that, when determining whether to accept trade data from an organization for comparison and trade recording, as provided for under Rule 7 (Comparison and Trade Recording Operation) of the Rules, NSCC may require such organization to provide a Cybersecurity Confirmation. These organizations are not Members of NSCC and, as such, NSCC's relationship with these organizations is governed by a contract that is separate from the Rules. Therefore, this change would provide transparency regarding the steps NSCC may take when determining whether to accept trade data from another organization.

To implement this change, NSCC would amend Rule 7 (Comparison and Trade Recording Operation), Section 6 of the Rules to provide that NSCC may require organizations that deliver trade data to NSCC as described in that Rule to provide a Cybersecurity Confirmation before agreeing to accept such trade data.

(iv) *Implementation Timeframe*

Subject to approval by the Commission, the proposed rule change would become effective immediately. The proposed requirement that applicants deliver a Cybersecurity Confirmation with their application materials would be implemented immediately and 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, NSCC would provide Members with notice of the due date of their Cybersecurity

Confirmations, no later than 180 days prior to such due date, and would provide such notice at least every two years going forward.

2. Statutory Basis

NSCC 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, NSCC believes that the proposed rule changes are consistent with Section 17A(b)(3)(F) of the Act,¹¹ and Rules 17Ad-22(e)(17)(i) and (e)(17)(ii), each promulgated under the Act,¹² for the reasons described below.

Section 17A(b)(3)(F) of the Act requires that the rules of NSCC 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.¹³

As described above, the proposed requirement that Members and applicants provide a Cybersecurity Confirmation regarding their cybersecurity program that includes the representations described above would provide NSCC with evidence of each Member's or applicant's management of endpoint security with respect to the SMART network or other connectivity and would enhance the protection of NSCC against cyberattacks. The proposed Cybersecurity Confirmation would provide NSCC with information that it could use to make decisions about risks or threats, perform additional monitoring, target potential vulnerabilities, and protect the NSCC network. The proposed

¹¹ 15 U.S.C. 78q-1(b)(3)(F).

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

¹³ 15 U.S.C. 78q-1(b)(3)(F).

Cybersecurity Confirmation would give NSCC the ability to further identify its exposure and enable it to take steps to mitigate risks. These requirements would help reduce risk to NSCC's network with respect to its communications with Members and their submission of instructions and transactions to NSCC by requiring all entities connecting to NSCC to have appropriate cybersecurity programs in place.

Risks, threats and potential vulnerabilities could impact NSCC'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 implementing a tool that would help to mitigate these risks, NSCC 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.¹⁴

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.¹⁵ The proposed Cybersecurity Confirmation would reduce cybersecurity risks to NSCC by requiring all Members and applicants to confirm they have defined and maintain cybersecurity programs that meet standard industry best practices and guidelines. The

¹⁴ Id.

¹⁵ 17 CFR 240.17Ad-22(e)(17)(i).

proposed representations in the Cybersecurity Confirmations would help NSCC to mitigate its exposure to cybersecurity risk and, thereby, decrease the operational risks to NSCC that are presented by connections to NSCC through the SMART network or otherwise. The proposed Cybersecurity Confirmations would identify to NSCC potential sources of external operational risks and enable it to mitigate these risks and their possible impacts to NSCC's operations. As a result, NSCC believes the proposal is consistent with the requirements of Rule 17Ad-22(e)(17)(i) under the Act.¹⁶

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.¹⁷ The proposed Cybersecurity Confirmation would enhance the security, resiliency, and operational reliability of the endpoint security with respect to the SMART network or other connectivity because, as noted above, by making the Cybersecurity Confirmation an application requirement and an ongoing membership requirement, NSCC would be able to prevent the connection by any applicant, and take action against any Member, that may pose an increased cyber risk to NSCC by not having a defined and ongoing cybersecurity program that meets appropriate standards. Members or applicants that are not in alignment with a recognized framework, guideline, or standard that NSCC believes is adequate to guide and assess such organization's cybersecurity program may present increased risk to NSCC. By enabling NSCC to identify these risks, the proposed changes

¹⁶ Id.

¹⁷ 17 CFR 240.17Ad-22(e)(17)(ii).

would allow NSCC to more effectively secure its environment against potential vulnerabilities. NSCC's controls are strengthened when NSCC's Members, and other organizations that connect to NSCC, have similar technology risk management controls and programs within their computing environment. Control weaknesses within a Member's environment could allow for malicious or unauthorized usage of the link between NSCC and the Member. As a result, NSCC believes the proposal would improve NSCC'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.¹⁸

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

NSCC believes the proposed rule change could have an impact on competition. Specifically, NSCC believes that the proposed rule change could burden competition because it would require Members and 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 Members and applicants that do not connect directly to the SMART 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.

¹⁸ Id.

NSCC believes the above described burden on competition that 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.¹⁹

First, NSCC 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.²⁰ By requiring Members and applicants to provide a Cybersecurity Confirmation, the proposed rule change would allow NSCC to better understand, assess, and, therefore, mitigate the cyber risks that NSCC could face through its connections to its Members. As described above, these risks could impact 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. Implementing a tool as described above would help to mitigate these risks, and therefore NSCC believes the proposal is necessary in furtherance of the requirements of Section 17A(b)(3)(F) of the Act.²¹

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.²² The proposed Cybersecurity

¹⁹ 15 U.S.C. 78q-1(b)(3)(I).

²⁰ 15 U.S.C. 78q-1(b)(3)(F).

²¹ Id.

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

Confirmations would identify to NSCC potential sources of external operational risks and allow it to establish appropriate controls that would mitigate these risks and their possible impacts to NSCC's operations. The proposed changes would also improve NSCC's ability to ensure that its systems have a high degree of security, by enabling NSCC to identify the cybersecurity risks that may be presented to it by Members and other entities that connect to NSCC.

Second, NSCC 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 Members and applicants. As described above, NSCC believes Members may already be subject to one or more regulatory requirements 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. Therefore, NSCC believes any burden that may be imposed by the proposed rule change would be appropriate.

Further, while the proposed Cybersecurity Confirmation would identify certain standards and guidelines that would be appropriate, NSCC would consider requests by applicants and Members to allow other standards in accepting a Cybersecurity Confirmation. Additionally, the proposed Cybersecurity Confirmation would provide differing options to conduct the review of the applicant's or Member's cybersecurity program. As such, NSCC has endeavored to design the Cybersecurity Confirmation in a way that is reasonable and does not require one approach for meeting its requirements.

Finally, NSCC is proposing to provide Members with a minimum of 180 calendar days' notice before the deadline for providing a Cybersecurity Confirmation. This notice

would allow 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. This implementation schedule is designed to be fair and not disproportionately impact any Members more than others. The proposal is designed to provide all impacted 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, NSCC 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.²³

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

NSCC has not solicited or received any written comments relating to this proposal. NSCC will notify the Commission of any written comments 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 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.

²³ 15 U.S.C. 78q-1(b)(3)(I).

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-NSCC-2019-003 on the subject line.

Paper Comments:

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

All submissions should refer to File Number SR-NSCC-2019-003. 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 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 the filing also will be available for inspection and copying at the principal office of NSCC and on DTCC's website (<http://dtcc.com/legal/sec-rule-filings.aspx>). 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-NSCC-2019-003 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.²⁴

Secretary

²⁴ 17 CFR 200.30-3(a)(12).

**CONFIRMATION OF A CLIENT CYBERSECURITY PROGRAM
NSCC**

National Securities Clearing Corporation
The Depository Trust & Clearing Corporation
55 Water Street
New York, NY 10041

Client Legal Entity Name: _____ (“The Company”)

Attention: Control Officer Name: _____

**Which standards and/or frameworks are you using to guide and assess your institution's cybersecurity program?
Please select all that apply.**

<input type="checkbox"/>	FSSCC Profile	Financial Services Sector Coordinating Council Cybersecurity Profile
<input type="checkbox"/>	NIST CSF	The National Institute of Standards and Technology Cybersecurity Framework
<input type="checkbox"/>	ISO 27001/27002	International Organization for Standardization Standard 27001/27002
<input type="checkbox"/>	FFIEC CAT	Federal Financial Institutions Examination Council Cybersecurity Assessment Tool
<input type="checkbox"/>	CSC 20	Critical Security Controls Top 20
<input type="checkbox"/>	COBIT	Control Objectives for Information and Related Technologies
<input type="checkbox"/>	Other	

Are you using a third party service provider or service bureau to access National Securities Clearing Corporation (“NSCC”)?

CONFIRMATION

The Company has designated the senior executive indicated below with sufficient authority to be responsible and accountable for overseeing and executing the cybersecurity program within the organization.

- The Company has defined and maintains a comprehensive cybersecurity program and framework that considers potential cyber threats that impact the organization and protects the confidentiality, integrity and availability requirements of The Company’s systems and information.
- The Company has implemented and maintains a written enterprise cybersecurity policy or policies approved by senior management or The Company’s board of directors, and The Company’s cybersecurity framework is in alignment with standard industry best practices and guidelines as indicated: (FSSCC Profile, NIST CSF, ISO 27001/27002, FFIEC CAT, CSC 20, COBIT).
- If using a third party service provider or service bureau(s) to connect or transact business or to manage the connection with NSCC, The Company has an appropriate program to evaluate the cyber risks and impact of these third parties, and to review the third party assurance reports.

- The Company's cybersecurity program and framework protect the segment of The Company's system that connects to and/or interacts with NSCC.
- There is an established process to remediate cyber issues identified to fulfill regulatory and/or statutory requirements.
- The Company'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 regulatory environment.
- A comprehensive review of the cybersecurity program and framework has been conducted by one of the following:
 - The Company, which has filed and maintains a current Certification of Compliance with the Superintendent of the New York State Department of Financial Services (NYSDFS) pursuant to 23 NYCRR 500
 - A regulator who assesses the program against a designated cybersecurity framework or industry standard (OCC: Office of the Comptroller and the FFIEC CAT)
 - An independent external entity with cybersecurity domain expertise (SOC2 Certification, ISO 27001 Certification, NIST CSF assessment)
 - An independent internal audit function reporting directly to the board of directors or designated board of directors committee of The Company, such that the findings of that review are shared with these governance bodies

I am the designated senior executive authorized to attest to the above on behalf of The Company.

CONTROL OFFICER:

First Name: _____

Last Name: _____

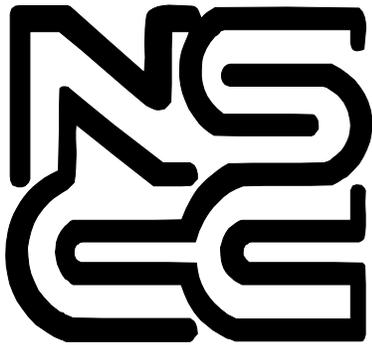
Phone: _____

Email: _____

Title _____

Date _____

Signature: _____



NATIONAL
SECURITIES
CLEARING
CORPORATION

RULES & PROCEDURES

TEXT OF PROPOSED RULE CHANGE

Bold and underlined text indicates proposed added language.

~~Bold and strikethrough text~~ indicates proposed deleted language.

RULE 1. DEFINITIONS AND DESCRIPTIONS

Cybersecurity Confirmation

The term “Cybersecurity Confirmation” means a written document provided to the Corporation by all Members, Limited Members and applicants for membership that confirms the existence of an information system cybersecurity program and includes the representations listed below.

Each Cybersecurity Confirmation shall (1) be on a form provided by the Corporation; (2) be signed by a designated senior executive of the Member, Limited Member or applicant who is authorized to attest to these matters; and (3) include the following representations, made with respect to the two years prior to the date of the Cybersecurity Confirmation:

- 1. The Member, Limited Member or applicant 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 Member, Limited Member or applicant 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.**
- 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 Member, Limited Member or applicant 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 Member’s, Limited Member’s or applicant’s system that connects to and/or interacts with the Corporation.**
- 5. The Member, Limited Member or applicant has in place an established process to remediate cyber issues identified to fulfill the Member’s, Limited 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 Member's, Limited Member's or applicant's cybersecurity program and framework has been conducted by one of the following:

- The Member, Limited 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 Important Notice issued 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 Important Notice issued 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 the Member, Limited Member or applicant, such that the findings of that review are shared with these governance bodies.**

RULE 2A. INITIAL MEMBERSHIP REQUIREMENTS

SEC. 1. ELIGIBILITY FOR MEMBERSHIP

In furtherance of the Corporation's rights and authority to establish standards for membership, the Corporation shall establish, as it deems necessary or appropriate, standards of financial responsibility, operational capability, experience and competence for membership applicable to Members and to Limited Members. The Corporation shall also establish guidelines for the application of such membership standards.

C. Application Documents

Each applicant shall, as required by the Corporation from time to time, complete and deliver to the Corporation an Applicant Questionnaire in such form as prescribed by the Corporation from time to time and shall provide such other reports, opinions, financial and other information as the Corporation may determine are appropriate for each membership type.

As part of its membership application, Eeach applicant (as determined by the Corporation with regard to membership type) shall complete and deliver to the Corporation **(1) a FATCA Certification as part of its membership application, and (2) a Cybersecurity Confirmation.**

RULE 2B. ONGOING MEMBERSHIP REQUIREMENTS AND MONITORING

SEC. 2. DATA TO BE FILED WITH THE CORPORATION

A. Reports and Information

Each Member, Mutual Fund/Insurance Services Member, Fund Member, and Insurance Carrier/Retirement Services Member (each hereinafter in this rule referred to collectively as “participants”) shall submit to the Corporation the following reports and information as applicable to such participant, together with all addenda and amendments applicable thereto, within the time periods prescribed by the Corporation from time to time. (Unless specifically set forth below, the time periods prescribed by the Corporation are set forth in the form of notices posted at the Corporation’s Website. Pursuant to Section 7 of Rule 45, it is the participant’s responsibility to retrieve all notices daily from the Website.):

(g) with respect to a participant that has provided to the SEC any notice required pursuant to paragraph (e) of the SEC’s Rule 15c3-1 shall notify the Corporation of the provision of such notice, and shall furnish the Corporation with a copy of such notice, by the Close of Business on the day that it so provides such notice to the SEC.

Each Member and Limited Member shall complete and deliver to the Corporation a Cybersecurity Confirmation at least every two years, on a date that is set by the Corporation and following notice that is provided no later than 180 calendar days prior to such due date.

The Corporation may from time to time require the submission of additional reports and other information as it may deem necessary or advisable. Reports and information provided to the Corporation pursuant to this Rule shall be provided in the form and to the persons or departments specified by the Corporation from time to time and the provisions of Rule 45 shall not apply thereto.

RULE 7. COMPARISON AND TRADE RECORDING OPERATION
(INCLUDING SPECIAL REPRESENTATIVE/INDEX RECEIPT AGENT

SEC. 6. The Corporation may determine, in its discretion, to accept, from self-regulatory organizations, as defined in the Securities Exchange Act of 1934, and/or derivatives clearing organizations that are registered or deemed to be registered with the Commodity Futures Trading Commission pursuant to the Commodity Exchange Act (either directly or through subsidiary or affiliated organizations¹) and/or service bureaus, initial, or supplemental trade data on behalf of Members for trade recording and input into the Corporation's Comparison Operation (with respect to debt securities) or compared trade data, on behalf of Members for input into the Corporation's Accounting Operation provided that a Member is a party to the trade or transaction. **In determining whether to accept trade data from an organization, as described in this Section 6, the Corporation may require such organization to provide a Cybersecurity Confirmation, as described in Rule 2B, Section 2A.**

Such data shall be in a form acceptable to the Corporation, in its discretion, and within such time frames as the Corporation may, in its discretion, require. The Corporation shall deem the report of any such data by any such organization to have been authorized by the Member on whose behalf the data shall have been reported. Data reported by any such organization(s) to the Corporation shall not be deemed to be reported by the Member to the Corporation until such data is accepted by the Corporation.
