SECURITIES AND EXCHANGE COMMISSION
(Release No. 34-95237; File No. SR-NSCC-2022-004)

July 8, 2022

Self-Regulatory Organizations; National Securities Clearing Corporation; Order Approving a Proposed Rule Change to Require Applicants and Members to Maintain or Upgrade Their Network or Communications Technology

I. INTRODUCTION

On May 11, 2022, National Securities Clearing Corporation ("NSCC") filed with the Securities and Exchange Commission ("Commission") proposed rule change SR-NSCC-2022-004 ("Proposed Rule Change") pursuant to Section 19(b)(1) of the Securities Exchange Act of 1934 ("Act")[1] and Rule 19b-4 thereunder.[2] The Proposed Rule Change was published for comment in the Federal Register on May 31, 2022.[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

A. Background

NSCC proposes to modify its Rules and Procedures ("Rules")[4] to require its Members, Limited Members, Sponsored Members, and applicants for membership (collectively, "members") to upgrade and maintain their network technology, and

---

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

2 17 CFR 240.19b-4.

3 Securities Exchange Act Release No. 94977 (May 24, 2022), 87 Fed. Reg. 32485 (May 31, 2022) (SR-NSC-2022-004) ("Notice of Filing").

4 NSCC's Rules are available at https://dtcc.com/~/media/Files/Downloads/legal/rules/nscc_rules.pdf.

communications technology or protocols, to meet standards that NSCC would identify and publish via Important Notice on its website, as described more fully below.

NSCC provides clearance, settlement, risk management, central counterparty services, and a guarantee of completion for virtually all broker-to-broker trades involving equity securities, corporate and municipal debt securities, American depository receipts, exchange traded funds, and unit investment trusts.[5] In light of its critical role in the marketplace, NSCC was designated a Systemically Important Financial Market Utility ("SIFMU") under Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010.[6] Due to NSCC's unique position in the marketplace, a failure or a disruption at NSCC could, among other things, 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.[7]

NSCC's Rules currently do not require, either as part of an application for membership or as an ongoing membership requirement, any level or version for network technology, such as a web browser or other technology, or any level or version of communications technology or protocols, such as email encryption, secure messaging, or file transfers, that members may use to connect to or communicate with NSCC.[8]

---

5 See Financial Stability Oversight Counsel 2012 Annual Report, Appendix A ("FSOC 2012 Report"), available at http://www.treasury.gov/initiatives/fsoc/Documents/2012%20Annual%20Report.pdf.

6 12 U.S.C. 5465(e)(1). See FSOC 2012 Report, supra note 5.

7 See FSOC 2012 Report, Appendix A, supra note 5.

8 Notice of Filing, supra note 3, at 32486.

Therefore, NSCC currently maintains multiple network and communications methods and protocols to interact with its members.[9] This includes some outdated communication technologies in order to support members that continue to use such older technologies.[10] NSCC believes that continuing to use such outdated technologies could render communications between NSCC and some of its members vulnerable to cyber risks.[11] Additionally, members' use of outdated technology delays NSCC's implementation of its own internal system upgrades, which by doing so, risks losing connectivity between NSCC and a number of its members.[12] Finally, NSCC states that it currently expends additional resources, both in personnel and equipment, to maintain outdated communications channels.[13]

To mitigate the foregoing security concerns and resource inefficiencies, NSCC proposes to require its members to upgrade and maintain network technology, communication technology, and protocol standards, in accordance with applicable technology standards that NSCC would identify and publish via Important Notice on its website from time to time.[14] NSCC would base these requirements on standards set forth by widely accepted organizations such as the National Institute of Standards and

---

9 Id.

10 Id.

11 Id.

12 Id.

13 Id.

14 Id.

Technology ("NIST") and the Internet Engineer Task Force ("IETF").[15]

To implement the proposed changes, NSCC would revise its Rules to require members to maintain or upgrade their network technology, communications technology, or protocols on the systems that connect to NSCC, to the version NSCC requires, within the time period NSCC requires.[16] Consistent with the guidance from NIST and other standards organizations, NSCC would require the use of TLS 1.2, Secure FTP ("SFTP"), and other modern technology and communication standards and protocols, by its members for communication with NSCC.[17] NSCC would publish such requirements via

---

15 Id. NIST is part of the U.S. Department of Commerce. The IETF is an open standards organization that develops and promotes voluntary Internet standards, in particular, the technical standards that comprise the Internet protocol suite (TCP/IP). For example, NIST Special Publication 800-52 revision 2, specifies servers that support government-only applications shall be configured to use Transport Layer Security ("TLS") 1.2 and should be configured to use TLS 1.3 as well. See https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf. (TLS, the successor of the now-deprecated Secure Sockets Layer ("SSL"), is a cryptographic protocol designed to provide communications security over a computer network.) These servers should not be configured to use TLS 1.1 and shall not use TLS 1.0, SSL 3.0, or SSL 2.0. Additionally, the IETF formally deprecated TLS versions 1.0 and 1.1 in March of 2021, stating that "[t]hese versions lack support for current and recommended cryptographic algorithms and mechanisms, and various government and industry profiles of applications using TLS now mandate avoiding these old TLS versions.... Removing support for older versions from implementations reduces the attack surface, reduces opportunity for misconfiguration, and streamlines library and product maintenance." See https://datatracker.ietf.org/doc/rfc8996/. NSCC would also require members to discontinue using File Transfer Protocol ("FTP"), which NSCC believes to be an insecure protocol because it transfers user authentication data (username and password) and file data as plain-text (not encrypted) over the network. Notice of Filing, supra note 3, at 32486.

16 Notice of Filing, supra note 3, at 32486-87.

17 Id.

Important Notice on its website.[18] NSCC also proposes to amend its Rules to provide that failure to perform a necessary technology upgrade within the required timeframe would subject members to a monetary fine.[19]

III. DISCUSSION AND COMMISSION FINDINGS

Section 19(b)(2)(C) of the Act[20] 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 the rules and regulations thereunder applicable to such organization. After careful consideration, the Commission finds that the Proposed Rule Change is consistent with the requirements of the Act and the rules and regulations applicable to NSCC. In particular, the Commission finds that the Proposed Rule Change is consistent with Sections 17A(b)(3)(F)[21] and (b)(3)(G)[22] of the Act and Rules 17Ad-22(e)(17)[23] and (e)(21)[24] thereunder.

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

---

18 Id.

19 Notice of Filing, supra note 3, at 32487.

20 15 U.S.C. 78s(b)(2)(C).

21 15 U.S.C. 78q-1(b)(3)(F).

22 15 U.S.C. 78q-1(b)(3)(G).

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

24 17 CFR 240.17Ad-22(e)(21)(iv).

which are in the custody or control of the clearing agency or for which it is responsible.[25]

As described above, NSCC proposes to require its members to upgrade and maintain network technology, and communication technology and protocol standards, that meet the standards identified by NSCC and published via Important Notice to NSCC's website from time to time. NSCC would use standards set forth by widely accepted organizations such as NIST and the IETF as the requirements. The proposed requirements would enable NSCC to avoid communicating with its members using outdated technologies that present security vulnerabilities to NSCC. Specifically, as an initial matter, the proposed requirements would enable NSCC to discontinue using communication technologies such as TLS 1.0, TLS 1.1, SSL 2.0, SSL 3.0, and FTP, which have been deemed not secure by organizations such as NIST and/or the IETF. Removing support for such outdated technologies would reduce NSCC's potential exposure to cyberattacks and other cyber vulnerabilities.

If not adequately addressed, the risk of cyberattacks and other cyber vulnerabilities could affect NSCC's network and, in turn, 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. NSCC designed the proposed requirements for members to upgrade their communications technology to address those risks, as described above. Accordingly, the Commission finds the proposed technology requirements on NSCC's members 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

---

[25] 15 U.S.C. 78q-1(b)(3)(F).

with the requirements of Section 17A(b)(3)(F) of the Act.[26]

B. Consistency with Section 17A(b)(3)(G) of the Act

Section 17A(b)(3)(G) of the Act requires the rules of a clearing agency to provide that its participants shall be appropriately disciplined for violation of any provision of the rules of the clearing agency by fine or other fitting sanction.[27] As noted above, NSCC proposes to require its members to upgrade and maintain network technology, communication technology, and protocol standards, in accordance with applicable technology standards that NSCC would identify and publish via Important Notice on its website. The proposed requirements would enable NSCC to avoid communicating with its members using outdated technologies that present security vulnerabilities to NSCC. If not adequately addressed, such vulnerabilities could affect NSCC's network and its ability to operate. NSCC also proposes to amend its Rules to provide that failure to perform a necessary technology upgrade within the required timeframe would subject members to a monetary fine. Because the proposed monetary fine should incentivize NSCC's members to upgrade and maintain secure communications technology, thereby reducing NSCC's operational risks, the Commission finds the proposed rule change is consistent with the requirements of Section 17A(b)(3)(G) of the Act.[28]

---

26 Id.

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

28 Id. Additionally, by including the monetary fine provision in its Rules, NSCC would enable its members to better identify and evaluate the material costs they might incur by participating in NSCC, consistent with Rule 17Ad-22(e)(23)(ii). under the Act, which requires a covered clearing agency to establish, implement, maintain, and enforce written policies and procedures reasonably designed to provide sufficient information to enable participants to identify and evaluate the

C. Consistency with Rule 17Ad-22(e)(17) 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.[29] NSCC's operational risks include cyber risks to its electronic systems.

As described above, NSCC and its members connect electronically to communicate with one another. However, NSCC's Rules currently do not require any level or version for network technology, such as a web browser or other technology, or any level or version of communications technology or protocols, such as email encryption, secure messaging, or file transfers, that members may use to connect to or communicate with NSCC. As a result, NSCC maintains some outdated communication technologies in order to support members that continue to use such older technologies. Continuing to use such outdated technologies could render communications between NSCC and some of its members vulnerable to cyber risks.

To mitigate the foregoing cyber risks, NSCC proposes to require its members to upgrade and maintain network technology, and communication technology and protocol standards that meet the standards identified by NSCC from time to time. The proposed technology requirements should reduce NSCC's cyber risk by requiring members to

---

risks, fees, and other material costs they incur by participating in the covered clearing agency. See 17 CFR 240.17Ad-22(e)(23)(ii).

[29] 17 CFR 240.17Ad-22(e)(17)(i).

upgrade and maintain communications technology based on standards set forth by widely accepted organizations such as NIST and the IETF, thereby decreasing the operational risks presented to NSCC. Because the proposed technology requirements would help NSCC mitigate plausible sources of external operational risk, the Commission finds the proposed changes are consistent with the requirements of Rule 17Ad-22(e)(17)(i) under the Act.[30]

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.[31] As noted above, NSCC's operational risks include cyber risks.

As described above, NSCC's Rules currently do not require any level or version for network technology, such as a web browser or other technology, or any level or version of communications technology or protocols, such as email encryption, secure messaging, or file transfers, that members may use to connect to or communicate with NSCC. NSCC designed the proposed technology requirements to reduce cyber risks by requiring its members to upgrade and maintain communications technology based on standards set forth by widely accepted organizations such as NIST and the IETF. Requiring NSCC's members to use only secure communications technology would reduce NSCC's cyber risks and thereby strengthen the security, resiliency, and operational reliability of NSCC's network and other systems. Because the proposed

---

30 Id.

31 17 CFR 240.17Ad-22(e)(17)(ii).

technology requirements would enhance NSCC's ability to ensure that its systems have a high degree of security, resiliency, and operational reliability, the Commission finds the Proposed Rule Change is consistent with the requirements of Rule 17Ad-22(e)(17)(ii) under the Act.[32]

D. Consistency with Rule 17Ad-22(e)(21) Under the Act

Rule 17Ad-22(e)(21)(iv) under the Act requires that each covered clearing agency establish, implement, maintain and enforce written policies and procedures reasonably designed to have the covered clearing agency's management regularly review the efficiency and effectiveness of its use of technology and communication procedures.[33]

As mentioned above, NSCC maintains multiple network and communication methods to interact with its members, including certain outdated communication technologies necessary to support members that continue to use such older technologies. NSCC believes that continuing to use such outdated technologies could render communications between NSCC and some of its members vulnerable to cyber risks. Additionally, members' use of outdated technology delays NSCC's implementation of its own internal system upgrades, which by doing so, risks losing connectivity between NSCC and a number of its members. Finally, NSCC states that it currently expends unnecessary resources to maintain outdated communications channels. In other words, NSCC has subjected its network communication methods to review for efficiency and effectiveness. As a result, to enhance the efficiency and effectiveness of its technology and communication procedures, NSCC proposes to require its members to upgrade and

---

32 Id.

33 17 CFR 240.17Ad-22(e)(21)(iv).

maintain network technology, communication technology, and protocol standards, in accordance with applicable technology standards that NSCC would identify and publish via Important Notice on its website. Because the Proposed Rule Change is an outgrowth of NSCC's review of the efficiency and effectiveness of its technology and communication procedures, the Commission finds the Proposed Rule Change is consistent with the requirements of Rule 17Ad-22(e)(21)(iv) under the Act.[34]

IV. CONCLUSION

On the basis of the foregoing, the Commission finds that the Proposed Rule Change is consistent with the requirements of the Act and in particular with the requirements of Section 17A of the Act[35] and the rules and regulations promulgated thereunder.

---

34 Id.

35 15 U.S.C. 78q-1.

IT IS THEREFORE ORDERED, pursuant to Section 19(b)(2) of the Act[36] that Proposed Rule Change SR-NSCC-2022-004, be, and hereby is, APPROVED.[37]

For the Commission, by the Division of Trading and Markets, pursuant to delegated authority.[38]

J. Matthew DeLesDernier,
Assistant Secretary.

---

36 15 U.S.C. 78s(b)(2).

37 In approving the Proposed Rule Change, the Commission considered the proposals' impact on efficiency, competition, and capital formation. 15 U.S.C. 78c(f).

38 17 CFR 200.30-3(a)(12).