

8011-01p
SECURITIES AND EXCHANGE COMMISSION
(Release No. 34-94975; File No. SR-DTC-2022-004)

May 24, 2022

Self-Regulatory Organizations; The Depository Trust Company; Notice of Filing of a Proposed Rule Change to Require Applicants and Members to Maintain or Upgrade Their Network or Communications Technology

Pursuant to Section 19(b)(1) of the Securities Exchange Act of 1934 (“Act”)¹ and Rule 19b-4 thereunder,² notice is hereby given that on May 11, 2022, The Depository Trust Company (“DTC”) 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 of DTC consists of modifications to Rules³ to revise certain provisions in the Rules relating to the requirement of applicants for DTC membership, Participants and Pledges, (collectively, “Participants”) of DTC, to require that each Participant upgrade its network technology, and communications technology or protocols to meet standards that DTC shall publish from time to time, as described in greater detail below.

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 https://dtcc.com/~media/Files/Downloads/legal/rules/DTC_rules.pdf.

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

DTC is proposing to adopt a requirement that each Participant provide documentation demonstrating that the Participant's network technology, and communication technology or protocols meet the standards that DTC is currently requiring. The determination to require changes or upgrades is incorporated into DTC's procedures and includes an evaluation of the external threat landscape, threats to DTC's technology infrastructure and information assets, industry cybersecurity priorities, a review of the root causes of incidents, and an evaluation of the current state of the network infrastructure as expressed using third-party assessments. For existing Participants and Pledgees, a new requirement is being proposed to require such Participants to upgrade their network technology, and communication technology or protocols within the timeframe published by DTC. The proposed changes are described in greater detail below.

(i) ***Background of the Requirement***

Currently, DTC does not require, either as part of its 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 are being used to connect to or communicate with DTC. In the current environment, DTC maintains multiple network and communications methods and protocols, some either obsolete or many years older than the current standard in order to support Participants using these older technologies, which leaves communications between DTC and its Participants vulnerable to interception or the introduction of unknown entries, and requires DTC to expend additional resources, both in personnel and equipment, to maintain older communications channels. In addition, Participant's use of older technology delays the implementation by DTC to upgrade its internal systems, which, by doing so, risks losing connectivity with a number of Participants. Given DTC's critical role in the marketplace, this is a risk that needs to be addressed.

DTC believes that it should require current network technology, and current communication technology and protocol standards for Participants connecting to its network. For example, The National Institute of Standards and Technology or NIST⁴ Special Publication 800-52 revision 2, specifies servers that support government-only

⁴ The National Institute of Standards and Technology ("NIST") is part of the U.S. Department of Commerce.

applications shall be configured to use TLS⁵ 1.2 and should be configured to use TLS 1.3 as well. These servers should not be configured to use TLS 1.1 and shall not use TLS 1.0, SSL 3.0, or SSL 2.0.⁶ The Internet Engineer Task Force (“IETF”)⁷ formally deprecated TLS versions 1.0 and 1.1 in March of 2021, stating, “These 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.”⁸ TLS 1.0 (published in 1999) does not support many modern, strong cipher (encryption) suites and TLS 1.1 (published in 2006) is a security improvement over TLS 1.0 but still does not support certain stronger cipher or encryption suites.⁹ Another communications technology, File Transfer Protocol (“FTP”) is considered an insecure protocol, because it transfers user authentication data (username and password) and file data as plain-text (not encrypted) over the network.

⁵ Transport Layer Security (“TLS”), the successor of the now-deprecated Secure Sockets Layer (“SSL”), is a cryptographic protocol designed to provide communications security over a computer network.

⁶ A government-only application is an application where the intended users are exclusively government employees or contractors working on behalf of the government. The full NIST publication is available at <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf>

⁷ The Internet Engineering Task Force (“IETF”) is an open standards organization, which develops and promotes voluntary Internet standards, in particular the technical standards that comprise the Internet protocol suite (TCP/IP).

⁸ <https://datatracker.ietf.org/doc/rfc8996/>

⁹ Id.

This makes it highly vulnerable to sniffing attacks that allow an attacker to collect usernames and passwords from the network and inject malware into downloads via FTP. Following the guidance from NIST and other standards organizations, the proposed change would require the use of TLS 1.2, Secure FTP (“SFTP”), along with other modern technology and communication standards and protocols to communication with Participants.

(ii) *Proposed Rule Changes*

To implement the proposed changes DTC would revise Rule 2, Section 11 to add the requirement that applicants for membership confirm their network technology, and communications technology and protocols to be at the levels specified by DTC, as part of their application. Rule 2, Section 11 would also be amended to add the requirement that each Participant or Pledgee maintain or upgrade their network technology, or communications technology, or protocols on the systems that connect to DTC to the version being required and within the time periods as provided through the Important Notice mechanism on the DTC website. Rule 21 would be updated to provide that a Participant or Pledgee who fails to perform the upgrade to their network technology, or communications technology, or protocols and in the required timeframe would be subject to the disciplinary sanctions as specified in the Rules.

(iii) *Implementation Timeframe and Notification Requirements*

In order to provide Participants and Pledgees adequate time to complete a required network technology, or communications technology or protocol upgrade, the time for a Participant or Pledgee to complete a required upgrade shall be set forth in the form of a notice posted on DTC’s website, with the timeline determined for the due date of any upgrade. DTC maintains a security policy and control standards that include a

review of industry, vendor and U.S. Government best practice guidelines and timelines for security reviews which are used to determine whether an upgrade may be required. Due dates for an upgrade shall be published on the website based on DTC's reasonable estimates of the complexity or potential cost of an upgrade, an estimate of potential licensing fees, an estimate of the resources that may be needed to support an upgrade, or the urgency to remediate published vulnerabilities.

Applicants to become a Participant or Pledgee shall be required to test connectivity to DTC using the current network technology or communications technology or protocols with their application for membership upon the effective date of the proposal.

2. Statutory Basis

DTC believes that the proposal is consistent with the requirements of the Act¹⁰ and the rules and regulations thereunder applicable to a registered clearing agency. In particular, DTC believes that the proposed rule changes is consistent with Section 17A(b)(3)(F) of the Act,¹¹ and Rules 17Ad-22(e)(17)(i) and (ii), (21), (23)¹², promulgated under the Act as discussed below.

Section 17A(b)(3)(F)

Section 17A(b)(3)(F) of the Act¹³ requires, in part, that the Rules be designed to promote the prompt and accurate clearance and settlement of securities transactions, to

¹⁰ 15 U.S.C. 78a et seq.

¹¹ 15 U.S.C. 78q-1(b)(3)(F).

¹² 17 CFR 240.17Ad-22(e)(17), (e)(21), (e)(23).

¹³ 15 U.S.C. 78q-1(b)(3)(F).

assure the safeguarding of securities and funds which are in the custody or control of DTC or for which it is responsible and to remove impediments to and perfect the mechanism of a national system for the prompt and accurate clearance and settlement of securities transactions.

DTC believes that the proposed rule change requiring Participants to meet DTC's standards for network technology, or communications technology or protocols is consistent with this provision of the Act. By conditioning an entity's application to DTC on its use of DTC's current network technology and communications technology or protocols, DTC should be better enabled to reduce the cyber risks of electronically connecting to entities by reducing the risks of communication interception. Accordingly, the proposed requirement would allow DTC to reduce both DTC's and its Participant's exposure to interception or the introduction of malware while communicating between the entities. Intercepting communications or the introduction of malware or altered data could potentially compromise DTC's ability to promptly and accurately settle securities transactions and safeguard securities funds. The proposal is designed to mitigate those risks and thereby promote the prompt and accurate clearance and settlement of securities transactions, to assure the safeguarding of securities and funds which are in the custody or control of DTC or for which it is responsible and to remove impediments to and perfect the mechanism of a national system for the prompt and accurate clearance and settlement of securities transactions. Providing a clear and consistent standard at the current level of network and communication security and technology would allow Participants to better understand their obligations with respect to such technology and communication requirements and providing a uniform obligation for Participants with

respect to such requirements. As such, DTC believes the proposed rule change is consistent with Section 17A(b)(3)(F) of the Act.¹⁴

17Ad 22(e)(21)(iv)

In addition, the proposed rule change is designed to be consistent with Rule 17Ad 22(e)(21)(iv) promulgated under the Act. Rule 17Ad-22(e)(21)(iv) requires DTC to, inter alia, establish, implement, maintain and enforce written policies and procedures reasonably designed to be efficient and effective in meeting the requirements of its Participants and the markets it serves with regard to the use of network technology and communication technologies or protocols. The proposed rule change would enhance DTC's security through the use of current network technology, or communication technology or protocols, and would allow DTC to reduce its and its Participants' exposure to interception or the introduction of malware while communicating between the entities. This would eliminate the current use of multiple generations of network technology and communications technology and protocols, including ones that NIST no longer permits for use on government systems due to their insecurity. The proposed rule would require, after appropriate notice to Participants, future network technology and communication or protocol upgrades as technology and threats evolve to maintain secure connectivity.

Therefore, by the reviewing and updating the efficiency and effectiveness of Participants' use of network technology and communication technology or protocols and procedures, DTC believes the proposed change is consistent with the requirements of Rule 17Ad-22(e)(21)(iv), promulgated under the Act.

¹⁴ Id.

Rule 17Ad-22(e)(17)(i)

DTC believes the proposed change is designed to reduce the following risks: (1) the risk of the communications between DTC and its Participants being intercepted or introducing malware or other unknown harmful elements into DTC's network that could cause harm to DTC; (2) the risk that a cyberattack or other unknown harmful elements could be introduced from a Participant that could cause harm to other Participants.¹⁵

In addition, the proposed rule change is designed to be consistent with Rule 17Ad-22(e)(17)(i) promulgated under the Act,¹⁶ which requires DTC to establish, implement, maintain and enforce written policies and procedures reasonably designed to manage the covered clearing agency's operational risks by identifying plausible sources of operational risk, both internal and external, and mitigating their impact through the use of appropriate systems, policies, procedures, and controls.

The use of old, obsolete, or insecure network technology or communications technologies or protocols, including communications between DTC and its Participants that are unencrypted, allowing for potential interception or making the communication highly vulnerable to sniffing attacks that allow an attacker to collect usernames and passwords from the network and inject malware, are examples of plausible sources of operational risks that DTC seeks to reduce. By requiring all Participants, after appropriate notice, to upgrade their network technology or communications technology or protocols to current standards, DTC seeks to enhance the security of its systems and the communications between it and its Participants.

¹⁵ 17 CFR 240.17Ad-22(e)(17).

¹⁶ 17 CFR 240.17Ad-22(e)(17)(i).

Because the proposed changes would help identify and manage such operational risks, DTC believes that it is consistent with the requirements of Rule 17Ad-22(e)(17)(i), promulgated under the Act.¹⁷

Rule 17Ad 22(e)(17)(ii)

In addition, the proposed rule change is designed to be consistent with Rule 17Ad-22(e)(17)(ii) promulgated under the Act, which requires DTC to establish, implement, maintain and enforce written policies and procedures reasonably designed ensure that systems have a high degree of security, resiliency, operational reliability, and adequate, scalable capacity.¹⁸

The use of unencrypted network technology and communications technology or protocols can allow a third-party to intercept messages, insert malware, or change the message content, often without the knowledge of either the sender or recipient of the messages or files. Requiring Participants to upgrade their network technology and communications technology or protocols to more modern and secure methods, may eliminate many of the earlier threats.

Therefore, by requiring Participants to upgrade their network technology or communications technology or protocols, DTC believes that the proposed change is consistent with the requirements of Rule 17Ad-22(e)(17)(ii), promulgated under the Act.¹⁹

Rule 17Ad-22(e)(22)

¹⁷ Id.

¹⁸ 17 CFR 240.17Ad-22(e)(17)(ii).

¹⁹ Id.

In addition, the proposed rule change is designed to be consistent with Rule 17Ad-22(e)(22) promulgated under the Act, which requires DTC to use, or at a minimum accommodate, relevant internationally accepted communication procedures and standards in order to facilitate efficient payment, clearing, and settlement.²⁰

The requirement to use industry approved communications technology or protocols, including those that NIST specifies as acceptable for use in government systems is a cornerstone of the changes being proposed by DTC. The use of older, obsolete, or insecure network technology or communications technology or protocols, including those specified to not be used by the IETF²¹ represents a risk to efficient payment, clearing and settlement.

Therefore, by requiring Participants to upgrade their network technology or communications technology or protocols, DTC believes that the proposed change is consistent with the requirements of Rule 17Ad-22(e)(22), promulgated under the Act.²²

Rule 17Ad-22(e)(23)

The proposed rule change is also designed to be consistent with Rule 17Ad 22(e)(23)(i), (ii) and (iv) promulgated under the Act, which requires DTC to publicly disclose all relevant rules and material procedures, provide sufficient information to enable Participants to identify and evaluate the risks, fees, potential monetary fines, and other material costs they incur by participating in the covered clearing agency, and to provide a comprehensive public disclosure that describes DTC's material rules, policies,

²⁰ 17 CFR 240.17Ad-22(e)(22).

²¹ <https://datatracker.ietf.org/doc/rfc8996/>

²² 17 CFR 240.17Ad-22(e)(22).

and procedures regarding DTC's legal, governance, risk management and operating framework.²³

Network technology, or communications technology or protocols that are being updated would be posted on the DTC website and Participants may subscribe to receive updates to such information as it occurs. This allows current or prospective Participants the ability to understand the risks and potential costs they may incur as a Participant, including the potential costs to upgrade its network technology or communications technology or protocols to the standards published by DTC.

Therefore, by providing Participants with public and readily available access to the required network technology, or communications technology or protocols, DTC believes that the proposed change is consistent with the requirements of Rule 17Ad-22(e)(23)(i)(ii) and (iv), promulgated under the Act.²⁴

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

DTC does not believe the proposed changes to require Participants to have, or to upgrade their network technology or communications technology or protocols would have any impact, or impose any burden on competition not necessary or appropriate in furtherance of the purposes of the Act.²⁵ Although the addition of the requirement to upgrade to current network technology or communications technology or protocols would be adding obligations on Participants with respect to how they communicate with DTC, such obligations would be reasonable because the requirements to protect client and

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

²⁴ Id.

²⁵ 15 U.S.C. 78q-1(b)(3)(I).

customer data would allow DTC to reduce both its and its Participants' exposure to interception or the introduction of malware while communicating between the entities.

DTC believes that the proposed change described herein is necessary in furtherance of the purposes of Section 17A(b)(3)(F) of the Act,²⁶ and Rules 17Ad-22(e)(17), (e)(21), (e)(22), and (e)(23).²⁷ The proposed changes to require Participants to upgrade their network technology, and communications technology or protocols, will (i) allow DTC to protect it and its Participants and would promote the prompt and accurate clearance and settlement of securities consistent with the requirements of Section 17A(b)(3)(F) of the Act,²⁸ (ii) identify potential operational risks from the use of obsolete and insecure network technology and communications technology or protocols consistent with Rule 17Ad 22(e)(17)(i),²⁹ (iii) through the requirement of the use of current network technology and communications technology or protocols, ensure that systems have a high degree of security, resiliency, operational reliability, and adequate, scalable capacity, consistent with Rule 17Ad 22(e)(17)(ii),³⁰ and (iv) through the use of requiring relevant internationally accepted communication procedures and standards, facilitate efficient payment, clearing, and settlement, consistent with Rules 17Ad-22(e)(22).³¹

²⁶ 15 U.S.C. 78q-1(b)(3)(F).

²⁷ 17 CFR 240.17Ad-22(e)(1), (e)(17), (e)(21), (e)(22) and (e)(23).

²⁸ Id.

²⁹ 17Ad 22(e)(17)(i).

³⁰ 17Ad 22(e)(17)(ii).

³¹ Id.

DTC believes that the proposed change described herein is appropriate in furtherance of the Act because the NIST standards and frameworks provides a common language and systematic methodology for managing cybersecurity risk. The IETF, initially supported by the U.S. Government,³² develops the internet and other technical standards used in communications between devices, and together, these are two of the leading providers of standards used by organizations to protect data and interoperability. DTC maintains policies to review current risks and standards, incorporating input from industry, vendors, and the U.S. Government to determine best practice guidelines and timelines for security reviews.

Therefore, DTC does not believe that the proposed change would impose any burden on competition that is not necessary or appropriate in furtherance of the Act.³³

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

DTC has not received or solicited any written comments relating to this proposal. If any written comments are received, they will be publicly filed as an Exhibit 2 to this filing, as required by Form 19b-4 and the General Instructions thereto.

Persons submitting comments are cautioned that, according to Section IV (Solicitation of Comments) of the Exhibit 1A in the General Instructions to Form 19b-4, the SEC does not edit personal identifying information from comment submissions. Commenters should submit only information that they wish to make available publicly, including their name, email address, and any other identifying information.

³² <https://www.internetsociety.org/internet/history-of-the-internet/ietf-internet-society/>

³³ 15 U.S.C. 78q-1(b)(3)(I).

All prospective commenters should follow the SEC's instructions on how to submit comments, available at <https://www.sec.gov/regulatory-actions/how-to-submit-comments>. General questions regarding the rule filing process or logistical questions regarding this filing should be directed to the Main Office of the SEC's Division of Trading and Markets at tradingandmarkets@sec.gov or 202-551-5777.

DTC reserves the right not to respond to any 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.

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-DTC-2022-004 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-DTC-2022-004. 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 DTC 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-DTC-2022-004 and should be submitted on or before [insert date 21 days from publication in the Federal Register].

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

J. Matthew DeLesDernier,
Assistant Secretary.

³⁴ 17 CFR 200.30-3(a)(12).