OMB APPROVAL
OMB Number: 3235-0045 Estimated average burden hours per response.....38

Required fields are shown with yellow backgrounds and asterisks.

Page 1 of * 35

SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549
Form 19b-4

File No.* SR - 2019 - * 008
Amendment No. (req. for Amendments *)

Filing by The Depository Trust Company

Pursuant to Rule 19b-4 under the Securities Exchange Act of 1934

Initial * ☑ Amendment * ☐ Withdrawal ☐

Section 19(b)(2) * ☑ Section 19(b)(3)(A) * ☐ Section 19(b)(3)(B) * ☐

Pilot ☐

Extension of Time Period for Commission Action * ☐

Date Expires *

Rule

- 19b-4(f)(1) ☐
- 19b-4(f)(2) ☐
- 19b-4(f)(3) ☐
- 19b-4(f)(4) ☐
- 19b-4(f)(5) ☐
- 19b-4(f)(6) ☐

Notice of proposed change pursuant to the Payment, Clearing, and Settlement Act of 2010

Section 806(e)(1) * ☐ Section 806(e)(2) * ☐

Security-Based Swap Submission pursuant to the Securities Exchange Act of 1934

Section 3C(b)(2) * ☐

Exhibit 2 Sent As Paper Document ☐ Exhibit 3 Sent As Paper Document ☐

Description

Provide a brief description of the action (limit 250 characters, required when Initial is checked *).

Require Confirmation of Cybersecurity Program

Contact Information

Provide the name, telephone number, and e-mail address of the person on the staff of the self-regulatory organization prepared to respond to questions and comments on the action.

First Name * Allen Last Name * Brandt

Title * Executive Director and Associate General Counsel

E-mail * abrandt@dtcc.com

Telephone * (212) 855-5063 Fax

Signature

Pursuant to the requirements of the Securities Exchange Act of 1934,

has duly caused this filing to be signed on its behalf by the undersigned thereunto duly authorized.

Date 10/14/2019

By Lois J. Radisch

(Name *)

(Title *)

Managing Director and Deputy General Counsel

NOTE: Clicking the button at right will digitally sign and lock this form. A digital signature is as legally binding as a physical signature, and once signed, this form cannot be changed.

lradisch@dtcc.com

Required fields are shown with yellow backgrounds and asterisks.

SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

For complete Form 19b-4 instructions please refer to the EFFS 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 The Depository Trust Company ("DTC") is annexed hereto as Exhibit 5 and consists of modifications to the Rules, By-Laws and Organization Certificate of DTC ("Rules")[1] in order to (1) define "Cybersecurity Confirmation" as a signed, written representation that addresses the submitting firm's cybersecurity program; and (2) enhance the DTC application requirements and ongoing requirements for Participants and Pledgees to (a) require that a Cybersecurity Confirmation be provided as part of the application materials for all Participants and Pledgees, and (b) require that Participants and Pledgees deliver to DTC a complete, updated Cybersecurity Confirmation at least every two years, 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 DTC 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*

DTC is proposing to modify the Rules in order to (1) define "Cybersecurity Confirmation" as a signed, written representation that addresses the submitting firm's cybersecurity program; and (2) enhance the DTC application requirements and ongoing requirements for Participants and Pledgees to (a) require that a Cybersecurity Confirmation be provided as part of the application materials for all Participants and Pledgees, and (b) require that Participants and Pledgees deliver to DTC a complete, updated Cybersecurity Confirmation at least every two years.

The proposed change would require all Participants, Pledgees and applicants to deliver to DTC 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 as a Participant and applicant to be a Pledgee, and (2) updated and re-delivered at least every two years by all Participants and Pledgees.

---

[1] Capitalized terms not defined herein are defined in the Rules, available at http://www.dtcc.com/legal/rules-and-procedures.

As described in more detail below, the Cybersecurity Confirmation would help DTC to assess the cybersecurity risks that may be introduced to it by Participants and Pledgees that connect to DTC either through the Securely Managed and Reliable Technology ("SMART") network[2] or through other connections. The proposed Cybersecurity Confirmation would allow DTC to better understand its Participants' and Pledgees' cybersecurity programs and frameworks and identify possible cybersecurity risk exposures. Based on this information, DTC would be able to establish appropriate controls to mitigate these risks and their possible impacts to DTC's operations.

(ii) *Background of Proposal*

DTC believes it is prudent to better understand the cybersecurity risks that it may face through its interconnections to Participants and Pledgees. As a designated systemically important financial market utility, or "SIFMU," DTC occupies a unique position in the marketplace such that a failure or a disruption to DTC 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, DTC 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, DTC 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 DTC through another means, such as through a third party service provider, service bureau, network, or the Internet. Given DTC's critical role in the marketplace, DTC is proposing to address the risks that could be posed by these connections.

Participants and Pledgees 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]

---

2 The SMART network is a technology managed by DTC'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 DTC's and its Participants' and Pledgees' operating premises. DTCC operates on a shared services model with respect to DTC and DTCC's other subsidiaries pursuant to intercompany agreements under which it is generally DTCC that provides a relevant service to its subsidiaries, including DTC.

3 DTC and its affiliates, Fixed Income Clearing Corporation ("FICC") and National Securities Clearing Corporation ("NSCC"), 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).

4 For example, depending on the type of entity, Participants and Pledgees 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

In order to comply with such regulations, Participants, Pledgees 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 Participants and Pledgees 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. DTC believes that it should require confirmation of the cybersecurity standards utilized by its Participants, Pledgees and applicants that connect to its network.

The proposed Cybersecurity Confirmation would require Participants, Pledgees and applicants to represent that they have established adequate controls and security to help limit (1) cybersecurity risks to DTC and to the other Participants' and Pledgees' networks and (2) access by unauthorized third parties while the firm is connected to DTC 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*

DTC is proposing to modify its Rules to (1) define "Cybersecurity Confirmation;" and (2) require that firms deliver a completed Cybersecurity Confirmation (a) as part of their initial application with DTC, and (b) on an ongoing basis, at least every two years. Each of these proposed rule changes is described in greater detail below.

(1) *Proposed Cybersecurity Confirmation*

DTC is proposing to adopt a definition of "Cybersecurity Confirmation." Each Cybersecurity Confirmation would be required to be in writing on a form provided by DTC 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 DTC, 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.

DTC is proposing to require that the following representations be included in the form of Cybersecurity Confirmation:

---

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).

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 DTC, 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 DTC.

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.

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

---

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

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

DTC is proposing to amend the Rules to include a definition of "Cybersecurity Confirmation," as described above, in a new Section 11 of Rule 2 (Participants and Pledgees).

(2) *Initial and Ongoing Requirement*

DTC is proposing to require that a Cybersecurity Confirmation be submitted to DTC by any applicant, as part of their application materials, and at least every two years by all Participants and Pledgees. With respect to the requirement to deliver a Cybersecurity

---

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 DTC 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. DTC would identify acceptable industry cybersecurity frameworks and standards in the form of Cybersecurity Confirmation and in an Important Notice that DTC would issue from time to time. DTC would also consider accepting other industry cybersecurity frameworks and standards upon request by a Participant, Pledgee 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. DTC would identify acceptable industry standards and practices in the form of Cybersecurity Confirmation and in an Important Notice that DTC would issue from time to time. DTC would also consider accepting other industry standards and practices upon request by a Participant, Pledgee or applicant.

Confirmation at least every two years, DTC would provide all Participants and Pledgees 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, DTC would amend the Rules to include a new Section 11 of Rule 2 (Participants and Pledgees) to require that (1) applicants complete and deliver a Cybersecurity Confirmation as part of their application materials; and (2) each Participant and Pledgee complete and deliver a Cybersecurity Confirmation at least every two years, on a date that is set by DTC and following notice that is provided no later than 180 calendar days prior to such due date.

(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, DTC would provide Participants and Pledgees 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

DTC 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, DTC 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 DTC 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 Participants, Pledgees and applicants provide a Cybersecurity Confirmation regarding their cybersecurity program that includes the representations described above would provide DTC with evidence of each Participant's, Pledgee's or applicant's management of endpoint security with respect to the SMART network or other connectivity and would enhance the protection of DTC against cyberattacks. The proposed Cybersecurity Confirmation would provide DTC with information that it could use to

---

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).

make decisions about risks or threats, perform additional monitoring, target potential vulnerabilities, and protect the DTC network. The proposed Cybersecurity Confirmation would give DTC the ability to further identify its exposure and enable it to take steps to mitigate risks. These requirements would help reduce risk to DTC's network with respect to its communications with Participants and Pledgees and their submission of instructions and transactions to DTC by requiring all Participants and Pledgees connecting to DTC to have appropriate cybersecurity programs in place.

Risks, threats and potential vulnerabilities could impact DTC'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, DTC 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 appropriate systems, policies, procedures, and controls.[13] The proposed Cybersecurity Confirmation would reduce cybersecurity risks to DTC by requiring all Participants, Pledgees 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 DTC to mitigate its exposure to cybersecurity risk and, thereby, decrease the operational risks to DTC that are presented by connections to DTC through the SMART network or otherwise. The proposed Cybersecurity Confirmations would identify to DTC potential sources of external operational risks and enable it to mitigate these risks and their possible impacts to DTC's operations. As a result, DTC 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

---

12 Id.

13 17 CFR 240.17Ad-22(e)(17)(i).

14 Id.

15 17 CFR 240.17Ad-22(e)(17)(ii).

requirement, DTC would be able to prevent the connection by any applicant, and take action against any Participant and Pledgee, that may pose an increased cyber risk to DTC by not having a defined and ongoing cybersecurity program that meets appropriate standards. Participants, Pledgees or applicants that are not in alignment with a recognized framework, guideline, or standard that DTC believes is adequate to guide and assess such organization's cybersecurity program may present increased risk to DTC. By enabling DTC to identify these risks, the proposed changes would allow DTC to more effectively secure its environment against potential vulnerabilities. DTC's controls are strengthened when DTC's Participants and Pledgees have similar technology risk management controls and programs within their computing environment. Control weaknesses within a Participant's or Pledgee's environment could allow for malicious or unauthorized usage of the link between DTC and the Participant or Pledgee. As a result, DTC believes the proposal would improve DTC'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

DTC believes the proposed rule change could have an impact on competition. Specifically, DTC believes that the proposed rule change could burden competition because it would require Participants, Pledgees 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 Participants, Pledgees 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.

DTC 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, DTC 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 that applicants, Participants and Pledgees provide a Cybersecurity Confirmation, the proposed rule change would allow DTC to better understand, assess, and, therefore, mitigate the cyber risks that DTC could face through its

---

16 Id.

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

18 15 U.S.C. 78q-1(b)(3)(F).

connections to its Participants and Pledgees. As described above, these risks could impact DTC's ability to clear and settle securities transactions, or to safeguard the securities and funds which are in DTC's custody or control, or for which it is responsible. Implementing a tool as described above would help to mitigate these risks, and therefore DTC 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 DTC potential sources of external operational risks and allow it to establish appropriate controls that would mitigate these risks and their possible impacts to DTC's operations. The proposed changes would also improve DTC's ability to ensure that its systems have a high degree of security, by enabling DTC to identify the cybersecurity risks that may be presented to it by Participants and Pledgees that connect to DTC.

Second, DTC 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 Participants, Pledgees and applicants. As described above, DTC believes Participants and Pledgees 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, DTC 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, DTC would consider requests by applicants, Participants and Pledgees 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, Participant's or Pledgee's cybersecurity program. As such, DTC has endeavored to design the Cybersecurity Confirmation in a way that is reasonable and does not require one approach for meeting its requirements.

Finally, DTC is proposing to provide Participants and Pledgees with a minimum of 180 calendar days' notice before the deadline for providing a Cybersecurity Confirmation. This notice would allow Participants and Pledgees to address any impact this change may have on their business. Applicants to be Participants or Pledgees 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 Participants or Pledgees more than others. The proposal is designed to provide all impacted Participants and Pledgees with time to review their

---

19 Id.

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

cybersecurity programs with respect to the required representations, and identify, if necessary, internal or third party cybersecurity reviewers.

For the reasons described above, DTC 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

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

6. Extension of Time Period for Commission Action

DTC does not consent to an extension of the time period specified in Section 19(b)(2) of the Act[22] 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.

(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, DTC's affiliates, FICC and NSCC, 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.

---

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

22 15 U.S.C. 78s(b)(2).

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 – DTC 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-DTC-2019-008)

[DATE]

Self-Regulatory Organizations; The Depository Trust Company; 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, 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 consists of modifications to the Rules, By-Laws and Organization Certificate of DTC ("Rules")[3] in order to (1) define "Cybersecurity Confirmation" as a signed, written representation that addresses the submitting firm's cybersecurity program; and (2) enhance the DTC application requirements and ongoing requirements for Participants and Pledgees to (a) require that a Cybersecurity Confirmation be provided as part of the application materials for all Participants and Pledgees, and (b) require that Participants and Pledgees deliver to DTC a complete,

---

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.

updated Cybersecurity Confirmation at least every two years, 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*

DTC is proposing to modify the Rules in order to (1) define "Cybersecurity Confirmation" as a signed, written representation that addresses the submitting firm's cybersecurity program; and (2) enhance the DTC application requirements and ongoing requirements for Participants and Pledgees to (a) require that a Cybersecurity Confirmation be provided as part of the application materials for all Participants and Pledgees, and (b) require that Participants and Pledgees deliver to DTC a complete, updated Cybersecurity Confirmation at least every two years.

The proposed change would require all Participants, Pledgees and applicants to deliver to DTC 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 as a Participant and applicant to be a Pledgee, and (2) updated and re-delivered at least every two years by all Participants and Pledgees.

As described in more detail below, the Cybersecurity Confirmation would help DTC to assess the cybersecurity risks that may be introduced to it by Participants and Pledgees that connect to DTC either through the Securely Managed and Reliable Technology ("SMART") network[4] or through other connections. The proposed Cybersecurity Confirmation would allow DTC to better understand its Participants' and Pledgees' cybersecurity programs and frameworks and identify possible cybersecurity risk exposures. Based on this information, DTC would be able to establish appropriate controls to mitigate these risks and their possible impacts to DTC's operations.

(ii) *Background of Proposal*

DTC believes it is prudent to better understand the cybersecurity risks that it may face through its interconnections to Participants and Pledgees. As a designated systemically important financial market utility, or "SIFMU," DTC occupies a unique position in the marketplace such that a failure or a disruption to DTC could increase the risk of significant liquidity problems spreading among financial institutions or markets

---

[4] The SMART network is a technology managed by DTC'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 DTC's and its Participants' and Pledgees' operating premises. DTCC operates on a shared services model with respect to DTC and DTCC's other subsidiaries pursuant to intercompany agreements under which it is generally DTCC that provides a relevant service to its subsidiaries, including DTC.

and thereby threaten the stability of the financial system in the United States.[5] Given its designation as a SIFMU, DTC 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, DTC 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 DTC through another means, such as through a third party service provider, service bureau, network, or the Internet. Given DTC's critical role in the marketplace, DTC is proposing to address the risks that could be posed by these connections.

Participants and Pledgees 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] In order to comply with such regulations, Participants, Pledgees and applicants would be required to follow standards established by national or

---

5 DTC and its affiliates, Fixed Income Clearing Corporation and National Securities 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, Participants and Pledgees 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, document, and maintain a system for regularly reviewing the effectiveness of its management controls and supervisory procedures (17 CFR 240.15c3-5).

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 Participants and Pledgees 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. DTC believes that it should require confirmation of the cybersecurity standards utilized by its Participants, Pledgees and applicants that connect to its network.

The proposed Cybersecurity Confirmation would require Participants, Pledgees and applicants to represent that they have established adequate controls and security to help limit (1) cybersecurity risks to DTC and to the other Participants' and Pledgees' networks and (2) access by unauthorized third parties while the firm is connected to DTC 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*

DTC is proposing to modify its Rules to (1) define "Cybersecurity Confirmation;" and (2) require that firms deliver a completed Cybersecurity Confirmation (a) as part of their initial application with DTC, and (b) on an ongoing basis, at least every two years. Each of these proposed rule changes is described in greater detail below.

(1) *Proposed Cybersecurity Confirmation*

DTC is proposing to adopt a definition of "Cybersecurity Confirmation." Each Cybersecurity Confirmation would be required to be in writing on a form provided by DTC 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 DTC, 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.

DTC 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]

---

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

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 DTC, 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 DTC.

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.

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

---

[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

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 DTC 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 DTC from time to time;[10] 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 DTC with evidence of each Participant's, Pledgee's or applicant's management of cybersecurity with respect to their connectivity to DTC. By requiring these representations from Participants, Pledgees and applicants the proposed Cybersecurity Confirmation would provide DTC

---

described in the regulation, which DTC 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. DTC would identify acceptable industry cybersecurity frameworks and standards in the form of Cybersecurity Confirmation and in an Important Notice that DTC would issue from time to time. DTC would also consider accepting other industry cybersecurity frameworks and standards upon request by a Participant, Pledgee 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. DTC would identify acceptable industry standards and practices in the form of Cybersecurity Confirmation and in an Important Notice that DTC would issue from time to time. DTC would also consider accepting other industry standards and practices upon request by a Participant, Pledgee or applicant.

with information that it could use to make decisions about risks or threats, perform additional monitoring, target potential vulnerabilities, and protect the DTC network.

DTC is proposing to amend the Rules to include a definition of "Cybersecurity Confirmation," as described above, in a new Section 11 of Rule 2 (Participants and Pledgees).

(2) *Initial and Ongoing Requirement*

DTC is proposing to require that a Cybersecurity Confirmation be submitted to DTC by any applicant, as part of their application materials, and at least every two years by all Participants and Pledgees. With respect to the requirement to deliver a Cybersecurity Confirmation at least every two years, DTC would provide all Participants and Pledgees 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, DTC would amend the Rules to include a new Section 11 of Rule 2 (Participants and Pledgees) to require that (1) applicants complete and deliver a Cybersecurity Confirmation as part of their application materials; and (2) each Participant and Pledgee complete and deliver a Cybersecurity Confirmation at least every two years, on a date that is set by DTC and following notice that is provided no later than 180 calendar days prior to such due date.

(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, DTC would provide Participants and Pledgees 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

DTC 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, DTC 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 DTC 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 Participants, Pledgees and applicants provide a Cybersecurity Confirmation regarding their cybersecurity program that includes the representations described above would provide DTC with evidence of each Participant's, Pledgee's or applicant's management of endpoint security with respect to the SMART network or other connectivity and would enhance the protection of DTC against cyberattacks. The proposed Cybersecurity Confirmation would provide DTC

---

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).

with information that it could use to make decisions about risks or threats, perform additional monitoring, target potential vulnerabilities, and protect the DTC network. The proposed Cybersecurity Confirmation would give DTC the ability to further identify its exposure and enable it to take steps to mitigate risks. These requirements would help reduce risk to DTC's network with respect to its communications with Participants and Pledgees and their submission of instructions and transactions to DTC by requiring all Participants and Pledgees connecting to DTC to have appropriate cybersecurity programs in place.

Risks, threats and potential vulnerabilities could impact DTC'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, DTC 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

---

14 Id.

15 17 CFR 240.17Ad-22(e)(17)(i).

proposed Cybersecurity Confirmation would reduce cybersecurity risks to DTC by requiring all Participants, Pledgees 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 DTC to mitigate its exposure to cybersecurity risk and, thereby, decrease the operational risks to DTC that are presented by connections to DTC through the SMART network or otherwise. The proposed Cybersecurity Confirmations would identify to DTC potential sources of external operational risks and enable it to mitigate these risks and their possible impacts to DTC's operations. As a result, DTC 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, DTC would be able to prevent the connection by any applicant, and take action against any Participant and Pledgee, that may pose an increased cyber risk to DTC by not having a defined and ongoing cybersecurity program that meets appropriate standards. Participants, Pledgees

---

16 Id.

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

or applicants that are not in alignment with a recognized framework, guideline, or standard that DTC believes is adequate to guide and assess such organization's cybersecurity program may present increased risk to DTC. By enabling DTC to identify these risks, the proposed changes would allow DTC to more effectively secure its environment against potential vulnerabilities. DTC's controls are strengthened when DTC's Participants and Pledgees have similar technology risk management controls and programs within their computing environment. Control weaknesses within a Participant's or Pledgee's environment could allow for malicious or unauthorized usage of the link between DTC and the Participant or Pledgee. As a result, DTC believes the proposal would improve DTC'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

DTC believes the proposed rule change could have an impact on competition. Specifically, DTC believes that the proposed rule change could burden competition because it would require Participants, Pledgees 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 Participants, Pledgees and applicants that do not connect directly to the SMART network, but connect through a third party service provider or service bureau

---

18 Id.

would have the additional burden of evaluating the cyber risks and impact of these third parties and reviewing the third party's assurance reports.

DTC 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, DTC 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 that applicants, Participants and Pledgees provide a Cybersecurity Confirmation, the proposed rule change would allow DTC to better understand, assess, and, therefore, mitigate the cyber risks that DTC could face through its connections to its Participants and Pledgees. As described above, these risks could impact DTC's ability to clear and settle securities transactions, or to safeguard the securities and funds which are in DTC's custody or control, or for which it is responsible. Implementing a tool as described above would help to mitigate these risks, and therefore DTC believes the proposal is necessary in furtherance of the requirements of Section 17A(b)(3)(F) of the Act.[21]

---

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

20 15 U.S.C. 78q-1(b)(3)(F).

21 Id.

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

Second, DTC 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 Participants, Pledgees and applicants. As described above, DTC believes Participants and Pledgees 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, DTC 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, DTC would consider requests by applicants, Participants and Pledgees 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, Participant's or

---

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

Pledgee's cybersecurity program. As such, DTC has endeavored to design the Cybersecurity Confirmation in a way that is reasonable and does not require one approach for meeting its requirements.

Finally, DTC is proposing to provide Participants and Pledgees with a minimum of 180 calendar days' notice before the deadline for providing a Cybersecurity Confirmation. This notice would allow Participants and Pledgees to address any impact this change may have on their business. Applicants to be Participants or Pledgees 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 Participants or Pledgees more than others. The proposal is designed to provide all impacted Participants and Pledgees 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, DTC 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

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

---

[23] 15 U.S.C. 78q-1(b)(3)(I).

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-2019-008 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-2019-008. This file number should be included on the subject line if e-mail is used. To help the Commission process and review your comments more efficiently, please use only one method. The

Commission will post all comments on the Commission's Internet website (http://www.sec.gov/rules/sro.shtml). Copies of the submission, all subsequent 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-2019-008 and should be submitted on or before [insert date 21 days from publication in the Federal Register].

For the Commission, by the Division of Trading and Markets, pursuant to delegated authority.[24]

Secretary

---

[24] 17 CFR 200.30-3(a)(12).

EXHIBIT 3

CONFIRMATION OF A CLIENT CYBERSECURITY PROGRAM
DTC

The Depository Trust Company
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.

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

Are you using a third party service provider or service bureau to access The Depository Trust Company ("DTC")?

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 DTC, 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 DTC.
- 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 arisk 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: _____

EXHIBIT 5

Bold and underlined text indicates proposed added language.

RULES, BY-LAWS AND ORGANIZATION CERTIFICATE

OF THE DEPOSITORY TRUST COMPANY

***

RULE 2

PARTICIPANTS AND PLEDGEES

***

Section 11.

As part of their application materials, each applicant to become a Participant or Pledgee shall complete and deliver to the Corporation a Cybersecurity Confirmation (as defined below).

Each Participant and Pledgee 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 term "Cybersecurity Confirmation" means a written document provided to the Corporation by all Participants, Pledgees and applicants 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 Participant, Pledgee 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 Participant, Pledgee 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 Participant, Pledgee 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 Participant, Pledgee 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 Participant's, Pledgee's or applicant's system that connects to and/or interacts with the Corporation.**

5. **The Participant, Pledgee or applicant has in place an established process to remediate cyber issues identified to fulfill the Participant's, Pledgee'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 Participant's, Pledgee's or applicant's cybersecurity program and framework has been conducted by one of the following:**

   - **The Participant, Pledgee 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 Participant, Pledgee or applicant, such that the findings of that review are shared with these governance bodies.**

***