internationally accepted communication procedures and standards, facilitate efficient payment, clearing, and settlement, consistent with Rules 17Ad–22(e)(22).[32]

NSCC 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,[33] 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. NSCC 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, NSCC does not believe that the proposed changes would impose any burden on competition that is not necessary or appropriate in furtherance of the Act.[34]

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

NSCC 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.

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.

NSCC 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 email to *rule-comments@sec.gov.* Please include File Number SR–NSCC–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–NSCC–2022–004. This file number should be included on the subject line if email is used. To help the Commission process and review your comments more efficiently, please use only one method. The Commission will post all comments on the Commission's internet website (*http://www.sec.gov/rules/sro.shtml*). Copies of the submission, all subsequent amendments, all written statements with respect to the proposed rule change that are filed with the Commission, and all written communications relating to the proposed rule change between the Commission and any person, other than those that may be withheld from the public in accordance with the provisions of 5 U.S.C. 552, will be available for website viewing and printing in the Commission's Public Reference Room, 100 F Street NE, Washington, DC 20549 on official business days between the hours of 10:00 a.m. and 3:00 p.m. Copies of the filing also will be available for inspection and copying at the principal office of NSCC and on DTCC's website (*http://dtcc.com/legal/sec-rule-filings.aspx*). All comments received will be posted without change. Persons submitting comments are cautioned that we do not redact or edit personal identifying information from comment submissions. You should submit only information that you wish to make available publicly. All submissions should refer to File Number SR–NSCC–2022–004 and should be submitted on or before June 21, 2022.

For the Commission, by the Division of Trading and Markets, pursuant to delegated authority.[35]

J. Matthew DeLesDernier,

Assistant Secretary.

[FR Doc. 2022–11535 Filed 5–27–22; 8:45 am]

BILLING CODE 8011–01–P

[32] *Id.*

[33] *https://www.internetsociety.org/internet/history-of-the-internet/ietf-internet-society/.*

[34] 15 U.S.C. 78q–1(b)(3)(I).

[35] 17 CFR 200.30–3(a)(12).

SECURITIES AND EXCHANGE COMMISSION

[Release No. 34–94972; File No. SR–FICC–2022–003]

Self-Regulatory Organizations; Fixed Income Clearing Corporation; Notice of Filing of a Proposed Rule Change To Require Applicants and Members To Maintain or Upgrade Their Network or Communications Technology

May 24, 2022.

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 20, 2022, Fixed Income Clearing Corporation (''FICC'') 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 FICC consists of modifications to FICC's Government Securities Division (''GSD'') Rulebook (''GSD Rules''), FICC's Mortgage-Backed Securities Division (''MBSD'') Clearing Rules (''MBSD Rules''), and the Electronic

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

[2] 17 CFR 240.19b–4.

Pool Notification (''EPN'') Rules of MBSD (''EPN Rules,'' and, together with the GSD Rules and the MBSD Rules, the ''Rules'') [3] to revise certain provisions in the Rules relating to the requirement of applicants and Members, (collectively, ''Participants'') of FICC, to require that each Participant upgrade its network technology, and communications technology or protocols to meet standards that FICC shall publish from time to time, 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

FICC 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 FICC is currently requiring. The determination to require changes or upgrades is incorporated into FICC's procedures and includes an evaluation of the external threat landscape, threats to FICC'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, 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 FICC. The proposed changes are described in greater detail below.

(i) Background of the Requirement

Currently, FICC 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 FICC. In the current environment, FICC 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 FICC and its Participants vulnerable to interception or the introduction of unknown entries, and requires FICC 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 FICC to upgrade its internal systems, which, by doing so, risks losing connectivity with a number of Participants. Given FICC's critical role in the marketplace, this is a risk that needs to be addressed.

FICC 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 NIST [4] Special Publication 800–52 revision 2, specifies servers that support government-only applications shall be configured to use TLS [5] 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. 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

GSD Rules

FICC is proposing to modify GSD Rules Rule 2A, Section 5, Rule 3, Section 2, and Rule 3B, Section 3(c)(ii) and insert a new Rule 3A, Section 2(b)(v), which would be changed to add the requirement that applicants for Comparison-Only Members, Netting Members, Sponsoring Members, and CCIT Members respectively, must confirm their network technology, and communications technology and protocols to be at the levels specified by FICC, as part of their application. Rule 3, Section 2, Rule 3A, Section 2(e), and Rule 3B, Section 5(b)(i) would be amended to add the requirement that each Participant type maintain or upgrade their network technology, or communications technology or protocols on the systems that connect to the Corporation to the version being required and within the time periods as provided through the Important Notice mechanism on the Corporation's website. The GSD Rules Fine Schedule

[3] Capitalized terms not defined herein are defined in the Rules, *available at http://www.dtcc.com/legal/rules-and-procedures.* References to ''Members'' in this filing include the Participants of GSD and MBSD, including GSD Netting Members, GSD Comparison-Only Members, GSD Sponsoring Members, GSD CCIT Members, GSD Funds-Only Settling Bank Members, MBSD Clearing Members, MBSD Cash Settling Bank Members, and MBSD EPN Users, as such terms are defined in the respective Rules.

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

[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.*

would be updated to provide that any Participant who fails to perform the upgrade to their network technology, or communications technology or protocols and in the required timeframe would be subject to a monetary fine, as specified in the Rules.

Also, FICC is proposing to re-number Rule 3A, Section 2(e) through Section 2(h) to Section 2(f) through Section 2(i) due to the insertion of a new Section 2(e); Rule 3B, Section 3(c)(ii) to Section 3(c)(iii) due to the insertion of a new Section 3(c)(ii); and Rule 3B, Section 5(i) and Section 5(ii) to Section 5(ii) and Section 5(iii) due to the insertion of a new Section 5(i).

MBSD Rules

To implement the proposed changes described herein, FICC would revise Rule 2A, Section 2(a) which would be changed to add the requirement that applicants for Clearing Members must confirm their network technology, and communications technology and protocols to be at the levels specified by FICC, as part of their application. Rule 3, Section 2 would be amended to add the requirement that each Clearing Member to maintain or upgrade their network technology, or communications technology or protocols on the systems that connect to the Corporation to the version being required and within the time periods as provided through the Important Notice mechanism on the Corporation's website. In addition, Rule 3, Section 2 would also be updated to provide that any Participant who fails to perform the upgrade to their network technology, or communications technology or protocols and in the required timeframe would be subject to a monetary fine, as specified in the Rules. Rule 3A, Section (d)(i)(2) would be amended to add the requirement that each Cash Settling Bank Member to maintain or upgrade their network technology, or communications technology or protocols on the systems that connect to the Corporation to the version being required and within the time periods as provided through the Important Notice mechanism on the Corporation's website. The Schedule of Charges for both the Broker Account Group and the Dealer Account Group would be updated to provide that a Clearing Member or Cash Settling Bank Member who fails to perform the upgrade to their network technology, or communications technology or protocols and in the required timeframe would be subject to a monetary fine, as specified in the Rules.

Also, FICC is proposing to re-number Rule 3A, Section (d)(i)(2) to Section (d)(i)(3) due to the insertion of a new Section (d)(i)(2).

EPN Rules

FICC is proposing to revise EPN Rules Article III, Rule 1, Section 2(b) which would be changed to add the requirement that applicants for EPN Users must confirm their network technology, and communications technology and protocols to be at the levels specified by FICC, as part of their application. Article III, Rule 1, Section 3(f) would be amended to add the requirement that each EPN User to maintain or upgrade their network technology, or communications technology or protocols on the systems that connect to the Corporation to the version being required and within the time periods as provided through the Important Notice mechanism on the Corporation's website.

Also, FICC is proposing to re-number Article III Rule 1, Section 2(b) to Section 2(c) due to the insertion of a new Section 2(b) and Article III, Rule 1, Section 3(f) would be re-numbered to Section 3(g) due to the insertion of a new Section 3(f).

In addition, Article V, Rule 3, would be amended to add the requirement that a Participant who fails to perform the upgrade to their network technology, or communications technology or protocols and in the required timeframe may be subject to a monetary fine, as specified in the Rules.

(iii) Implementation Timeframe and Notification Requirements

In order to provide Participants adequate time to complete a required network technology, or communications technology or protocol upgrade, the time for a Participant to complete a required upgrade shall be set forth in the form of a notice posted on FICC's website with the timeline determined for the due date of any upgrade. FICC 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 FICC'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 for membership shall be required to test connectivity to FICC 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

FICC believes that the proposal is consistent with the requirements of the Act[10] and the rules and regulations thereunder applicable to a registered clearing agency. In particular, FICC 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), and (23),[12] promulgated under the Act as discussed below.

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

Section 17A(b)(3)(F) of the Act[13] requires, in part, that the Rules be designed to 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 FICC 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.

FICC believes that the proposed rule change requiring Participants to meet FICC'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 FICC on its use of FICC's current network technology and communications technology or protocols, FICC 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 FICC to reduce both FICC's and its Participants 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 FICC'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 FICC or for which it is responsible and to remove impediments to and perfect

[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).

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, FICC 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 FICC 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 FICC's security through the use of current network technology, or communication technology or protocols, and would allow FICC 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 reviewing and updating the efficiency and effectiveness of Participants' use of network technology and communication technology or protocols and procedures, FICC believes the proposed change is consistent with the requirements of Rule 17Ad–22(e)(21)(iv), promulgated under the Act.

Rule 17Ad–22(e)(17)(i)

FICC believes the proposed change is designed to reduce the following risks: (1) The risk of the communications between FICC and its Participants being intercepted or introducing malware or other unknown harmful elements into FICC's network that could cause harm to FICC; (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 FICC 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 FICC 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 FICC seeks to reduce. By requiring all Participants, after appropriate notice, to upgrade their network technology or communications technology or protocols to current standards, FICC seeks to enhance the security of its systems and the communications between it and its Participants.

Because the proposed change would help identify and manage such operational risks, FICC 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 FICC 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, FICC 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)

In addition, the proposed rule change is designed to be consistent with Rule 17Ad–22(e)(22) promulgated under the Act, which requires FICC 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 FICC. The use of older, obsolete, or insecure network technology or communications technology or protocols, including those specified to not be used by the IETF [21] represents a risk to efficient payment, clearing and settlement.

Therefore, by requiring Participants to upgrade their network technology or communications technology or protocols, FICC 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 FICC 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 FICC's material rules, policies, and procedures regarding FICC's legal, governance, risk management and operating framework.[23]

Network technology, or communications technology or

[14] *Id.*

[15] 17 CFR 240.17Ad–22(e)(17).

[16] 17 CFR 240.17Ad–22(e)(17)(i).

[17] *Id.*

[18] 17 CFR 240.17Ad–22(e)(17)(ii).

[19] *Id.*

[20] 17 CFR 240.17Ad–22(e)(22).

[21] *https://datatracker.ietf.org/doc/rfc8996/.*

[22] 17 CFR 240.17Ad–22(e)(22).

[23] 17 CFR 240.17Ad–23(e)(i), (ii), and (iv).

protocols that are being updated would be posted on the FICC 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 FICC.

Therefore, by providing Participants with public and readily available access to the required network technology, or communications technology or protocols, FICC 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

FICC does not believe the proposed change 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 FICC, such obligations would be reasonable because the requirements to protect client and customer data would allow FICC to reduce both its and its Participants' exposure to interception or the introduction of malware while communicating between the entities.

FICC 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 FICC 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]

FICC 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. FICC 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, FICC 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

FICC 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.

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.

FICC 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 email to *rule-comments@sec.gov.* Please include File Number SR–FICC–2022–003 on the subject line.

Paper Comments

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

All submissions should refer to File Number SR–FICC–2022–003. This file number should be included on the subject line if email is used. To help the Commission process and review your comments more efficiently, please use only one method. The Commission will post all comments on the Commission's internet website (*http://www.sec.gov/rules/sro.shtml*). Copies of the

[24] Id.

[25] 15 U.S.C. 78q–1(b)(3)(I).

[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.*

[32] *https://www.internetsociety.org/internet/history-of-the-internet/ietf-internet-society/.*

[33] 15 U.S.C. 78q–1(b)(3)(I).

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 FICC 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–FICC–2022–003 and should be submitted on or before June 21, 2022.

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

J. Matthew DeLesDernier,

Assistant Secretary.

[FR Doc. 2022–11533 Filed 5–27–22; 8:45 am]

BILLING CODE 8011–01–P

SMALL BUSINESS ADMINISTRATION

Data Collection Available for Public Comments

ACTION: 60-Day notice and request for comments.

SUMMARY: The Small Business Administration (SBA) intends to request approval, from the Office of Management and Budget (OMB) for the collection of information described below. The Paperwork Reduction Act (PRA) federal agencies to publish a notice in the **Federal Register** concerning each proposed collection of information before submission to OMB, and to allow 60 days for public comment in response to the notice. This notice complies with that requirement.

DATES: Submit comments on or before August 1, 2022.

ADDRESSES: Send all comments to, Donald Smith, Deputy Assistant Administrator, Office of Women's Business Ownership, Small Business Administration.

FOR FURTHER INFORMATION CONTACT: Donald Smith, Deputy Assistant Administrator, *Donald.smith@sba.gov* 202–205–7279, or Curtis B. Rich, Agency Clearance Officer, 202–205–7030 *curtis.rich@sba.gov.*

SUPPLEMENTARY INFORMATION: The Women's Business Center Program is funded by the SBA to provide entrepreneurial development services and current business owners. There is no data collection currently in place to systematically track program outcomes such as client satisfaction, adoption of new business practices or change in business size or scope. This data collection fills the gap by administering a service outcome survey to a random sample of WBC clients.

OMB Control Number: 3245–0402.

Title: ''Women's Business Center Program''.

Description of Respondents: Entrepreneurial development services and current business owners.

Form Number: N/A.

Annual Responses: 2,087.

Annual Burden: 700.

Curtis Rich,

Agency Clearance Officer.

[FR Doc. 2022–11583 Filed 5–27–22; 8:45 am]

BILLING CODE 8026–09–P

DEPARTMENT OF TRANSPORTATION

Federal Railroad Administration

[Docket No. FRA–2010–0034]

Port Authority Trans-Hudson's Request To Operate Its Positive Train Control System With Procedural Mitigations

AGENCY: Federal Railroad Administration (FRA), Department of Transportation (DOT).

ACTION: Notice of availability.

SUMMARY: This document provides the public with notice that, on May 23, 2022, Port Authority Trans-Hudson (PATH) submitted a request to temporarily operate its conditionally FRA-certified Communications Based Train Control (CBTC) positive train control (PTC) system with a procedural mitigation to address a recently discovered software error. As this request involves the failure of a conditionally certified PTC system to perform its intended function, FRA is publishing this notice to advise the public that: PATH has determined the cause of the failure to be a software error; PATH is in the process of repairing the error without undue delay, as FRA's regulations require; and PATH has proposed a procedural mitigation in the interim to ensure that the software error will not cause a further failure of PATH's PTC system. Based on FRA's review of all pertinent information, FRA has approved PATH to temporarily operate its conditionally certified PTC system with a procedural mitigation.

DATES: FRA may consider comments to the extent practicable and without delaying implementation of valuable or necessary modifications to a PTC system.

ADDRESSES:

Comments: Comments may be submitted by going to *https://www.regulations.gov* and following the online instructions for submitting comments.

Instructions: All submissions must include the agency name and the applicable docket number. The relevant PTC docket number for this host railroad is Docket No. FRA–2010–0034. For convenience, all active PTC dockets are hyperlinked on FRA's website at *https://railroads.dot.gov/train-control/ptc/ptc-annual-and-quarterly-reports.* All comments received will be posted without change to *https://www.regulations.gov;* this includes any personal information.

FOR FURTHER INFORMATION CONTACT: Gabe Neal, Staff Director, Signal, Train Control, and Crossings Division, telephone: 816–516–7168, email: *Gabe.Neal@dot.gov.*

SUPPLEMENTARY INFORMATION: In general, Title 49 United States Code (U.S.C.) 20157(h) requires FRA to certify that a host railroad's PTC system complies with Title 49 Code of Federal Regulations (CFR) part 236, subpart I, before the technology may be operated in revenue service. Under 49 CFR 236.1023(j) and 236.1029(a), when any safety-critical PTC system, subsystem, or component fails to perform its intended function, the cause must be determined and the faulty product adjusted, repaired, or replaced without undue delay. Until corrective action is completed, a railroad shall take appropriate action as specified in its PTC Safety Plan (PTCSP).

FRA conditionally certified PATH's CBTC PTC system on November 27, 2018. Since that time, to FRA's knowledge, PATH's PTC system has operated reliably performing its intended functions, except in May 2022. Recently, PATH experienced two safety incidents on May 12 and May 17, 2022, with its PTC system. In response to

[34] 17 CFR 200.30–3(a)(12).