ESTIMATE OF ANNUAL RESPONDENT BURDEN—Continued

Form No.	Annual responses	Time (minutes)	Burden (hours)
Total	5,450		959

3. Title and purpose of information collection: Request for Medicare Payment; OMB 3220–0131. Under Section 7(d) of the Railroad Retirement Act (45 U.S.C. 231f), the RRB administers the Medicare program for persons covered by the railroad retirement system. The collection obtains the information needed by Palmetto GBA, the Medicare carrier for railroad retirement beneficiaries, to pay claims for payments under Part B of the Medicare program. Authority for collecting the information is prescribed in 42 CFR 424.32.

The RRB currently utilizes Forms G–740S, Patient's Request for Medicare Payment, along with Centers for Medicare & Medicaid Services Form CMS–1500, to secure the information necessary to pay Part B Medicare Claims. One response is completed for each claim. Completion is required to obtain a benefit. The RRB proposes no changes to Form G–740S.

ESTIMATE OF ANNUAL RESPONDENT BURDEN

Form No.	Annual responses	Time (minutes)	Burden (hours)
G–740S	1	0	1

4. Title and purpose of information collection: Employer's Deemed Service Month Questionnaire; OMB 3220–0156. Section 3 (i) of the Railroad Retirement Act (RRA) (45 U.S.C. 231b), as amended by Public Law 98–76, provides that the Railroad Retirement Board (RRB), under certain circumstances, may deem additional months of service in cases where an employee does not actually work in every month of the year, provided the employee satisfies certain eligibility requirements, including the existence of an employment relation between the employee and his or her employer. The procedures pertaining to the deeming of additional months of service are found in the RRB's regulations at 20 CFR 210, Creditable Railroad Service.

The RRB utilizes Form GL–99, *Employer's Deemed Service Months Questionnaire,* to obtain service and compensation information from railroad employers to determine if an employee can be credited with additional deemed months of railroad service. Completion is mandatory. One response is required for each RRB inquiry. The RRB proposes no changes to Form GL–99.

ESTIMATE OF ANNUAL RESPONDENT BURDEN

Form No.	Annual responses	Time (minutes)	Burden (hours)
GL–99	2,000	2	67

Additional Information or Comments: To request more information or to obtain a copy of the information collection justification, forms, and/or supporting material, contact Kennisha Tucker at (312) 469–2591 or *Kennisha.Tucker@rrb.gov.* Comments regarding the information collection should be addressed to Brian Foster, Railroad Retirement Board, 844 North Rush Street, Chicago, Illinois 60611–1275 or emailed to *Brian.Foster@rrb.gov.* Written comments should be received within 60 days of this notice.

Brian Foster,

Clearance Officer.

[FR Doc. 2022–14985 Filed 7–13–22; 8:45 am]

BILLING CODE 7905–01–P

SECURITIES AND EXCHANGE COMMISSION

[Release No. 34–95233; File No. SR–FICC–2022–003]

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

July 8, 2022.

I. Introduction

On May 20, 2022, Fixed Income Clearing Corporation (''FICC'') filed with the Securities and Exchange Commission (''Commission'') proposed rule change SR–FICC–2022–003 (''Proposed Rule Change'') pursuant to Section 19(b)(1) of the Securities Exchange Act of 1934 (''Act'') [1] and Rule 19b–4 thereunder.[2] The Proposed Rule Change was published for comment in the **Federal Register** on May 31, 2022.[3] The Commission did not receive any comment letters on the proposed rule change. For the reasons discussed below, the Commission is approving the Proposed Rule Change.

II. Description of the Proposed Rule Change

A. Background

FICC proposes to modify its Government Securities Division Rulebook (''GSD Rules''), Mortgage-Backed Securities Division Clearing Rules (''MBSD Rules''), and Electronic Pool Notification Rules of MBSD (''EPN Rules,'' and, together with the GSD Rules and the MBSD Rules, the

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

[2] 17 CFR 240.19b–4.

[3] Securities Exchange Act Release No. 94972 (May 24, 2022), 87 FR 32489 (May 31, 2022) (SR–FICC–2022–003) (''Notice of Filing'').

''Rules'') [4] to require its Members and applicants for membership (collectively, ''members'') to upgrade and maintain their network technology, and communications technology or protocols, to meet standards that FICC would identify and publish via Important Notice on its website, as described more fully below.

FICC is made up of two divisions, the Government Securities Division (FICC/GSD) and the Mortgage Backed Securities Division (FICC/MBSD), each providing clearing services in a different portion of the fixed income market.[5] FICC/GSD provides clearing, settlement, risk management, central counterparty services, and a guarantee of trade completion for U.S. government and agency securities.[6] FICC/MBSD provides clearing, netting, settlement, risk management, and pool notification services to major market participants trading in pass-through MBS issued by the Ginnie Mae, Freddie Mac, and Fannie Mae.[7] In light of its critical role in the marketplace, FICC was designated a Systemically Important Financial Market Utility (''SIFMU'') under Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010.[8] Due to FICC's unique position in the marketplace, a failure or a disruption at FICC could, among other things, increase the risk of significant liquidity problems spreading among financial institutions or markets, and thereby threaten the stability of the financial system in the United States.[9]

FICC's Rules currently do not require, either as part of an application for membership or as an ongoing membership requirement, any level or version for network technology, such as a web browser or other technology, or any level or version of communications technology or protocols, such as email encryption, secure messaging, or file transfers, that members may use to connect to or communicate with FICC.[10] Therefore, FICC currently maintains multiple network and communications methods and protocols to interact with its members.[11] This includes some outdated communication technologies in order to support members that continue to use such older technologies.[12] FICC believes that continuing to use such outdated technologies could render communications between FICC and some of its members vulnerable to cyber risks.[13] Additionally, members' use of outdated technology delays FICC's implementation of its own internal system upgrades, which by doing so, risks losing connectivity between FICC and a number of its members.[14] Finally, FICC states that it currently expends additional resources, both in personnel and equipment, to maintain outdated communications channels.[15]

To mitigate the foregoing security concerns and resource inefficiencies, FICC proposes to require its members to upgrade and maintain network technology, communication technology, and protocol standards, in accordance with applicable technology standards that FICC would identify and publish via Important Notice on its website from time to time.[16] FICC would base these requirements on standards set forth by widely accepted organizations such as the National Institute of Standards and Technology (''NIST'') and the internet Engineer Task Force (''IETF'').[17]

To implement the proposed changes, FICC would revise its Rules to require members to maintain or upgrade their network technology, communications technology, or protocols on the systems that connect to FICC, to the version FICC requires, within the time period FICC requires.[18] Consistent with the guidance from NIST and other standards organizations, FICC would require the use of TLS 1.2, Secure FTP (''SFTP''), and other modern technology and communication standards and protocols, by its members for communication with FICC.[19] FICC would publish such requirements via Important Notice on its website.[20] FICC also proposes to amend its Rules to provide that failure to perform a necessary technology upgrade within the required timeframe would subject members to a monetary fine.[21]

III. Discussion and Commission Findings

Section 19(b)(2)(C) of the Act [22] directs the Commission to approve a proposed rule change of a self-regulatory organization if it finds that such proposed rule change is consistent with the requirements of the Act and the rules and regulations thereunder applicable to such organization. After careful consideration, the Commission finds that the Proposed Rule Change is consistent with the requirements of the Act and the rules and regulations applicable to FICC. In particular, the Commission finds that the Proposed Rule Change is consistent with Sections 17A(b)(3)(F) [23] and (b)(3)(G) [24] of the Act and Rules 17Ad–22(e)(17) [25] and (e)(21) [26] thereunder.

A. Consistency With Section 17A(b)(3)(F) of the Act

Section 17A(b)(3)(F) of the Act requires that the rules of a clearing agency be designed to, among other things, promote the prompt and accurate clearance and settlement of securities transactions and assure the safeguarding of securities and funds which are in the custody or control of the clearing agency or for which it is responsible.[27]

As described above, FICC proposes to require its members to upgrade and maintain network technology, and

[4] FICC's Rules are *available at https://www.dtcc.com/~/media/Files/Downloads/legal/rules/ficc_gov_rules.pdf; https://www.dtcc.com/~/media/Files/Downloads/legal/rules/ficc_mbsd_rules.pdf; https://www.dtcc.com/~/media/Files/Downloads/legal/rules/ficc_mbsd_epnrules.pdf.*

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

[6] *Id.*

[7] *Id.*

[8] 12 U.S.C. 5465(e)(1). *See* FSOC 2012 Report, *supra* note 5.

[9] *See* FSOC 2012 Report, Appendix A, *supra* note 5.

[10] Notice of Filing, *supra* note 3, at 32490.

[11] *Id.*

[12] *Id.*

[13] *Id.*

[14] *Id.*

[15] *Id.*

[16] *Id.*, at 32490–91.

[17] *Id.* NIST is part of the U.S. Department of Commerce. The IETF is an open standards organization that develops and promotes voluntary internet standards, in particular, the technical standards that comprise the internet protocol suite (TCP/IP). For example, NIST Special Publication 800–52 revision 2, specifies servers that support government-only applications shall be configured to use Transport Layer Security (''TLS'') 1.2 and should be configured to use TLS 1.3 as well. *See https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf.* (TLS, the successor of the now-deprecated Secure Sockets Layer (''SSL''), is a cryptographic protocol designed to provide communications security over a computer network.) These servers should not be configured to use TLS 1.1 and shall not use TLS 1.0, SSL 3.0, or SSL 2.0. Additionally, the IETF formally deprecated TLS versions 1.0 and 1.1 in March of 2021, stating that ''[t]hese versions lack support for current and recommended cryptographic algorithms and mechanisms, and various government and industry profiles of applications using TLS now mandate avoiding these old TLS versions. . . . Removing support for older versions from implementations reduces the attack surface, reduces opportunity for misconfiguration, and streamlines library and product maintenance.'' *See https://datatracker.ietf.org/doc/rfc8996/.* FICC would also require members to discontinue using File Transfer Protocol (''FTP''), which FICC believes to be an insecure protocol because it transfers user authentication data (username and password) and file data as plain-text (not encrypted) over the network. Notice of Filing, *supra* note 3, at 32490–91.

[18] Notice of Filing, *supra* note 3, at 32490–91.

[19] *Id.*

[20] *Id.*

[21] Notice of Filing, *supra* note 3, at 32490–91.

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

[23] 15 U.S.C. 78q–1(b)(3)(F).

[24] 15 U.S.C. 78q–1(b)(3)(G).

[25] 17 CFR 240.17Ad–22(e)(17)(i) and (ii).

[26] 17 CFR 240.17Ad–22(e)(21)(iv).

[27] 15 U.S.C. 78q–1(b)(3)(F).

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

If not adequately addressed, the risk of cyberattacks and other cyber vulnerabilities could affect FICC's network and, in turn, FICC's ability to clear and settle securities transactions, or to safeguard the securities and funds which are in FICC's custody or control, or for which it is responsible. FICC designed the proposed requirements for members to upgrade their communications technology to address those risks, as described above. Accordingly, the Commission finds the proposed technology requirements on FICC's members would promote the prompt and accurate clearance and settlement of securities transactions and assure the safeguarding of securities and funds which are in the custody or control of FICC or for which it is responsible, consistent with the requirements of Section 17A(b)(3)(F) of the Act.[28]

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

Section 17A(b)(3)(G) of the Act requires the rules of a clearing agency to provide that its participants shall be appropriately disciplined for violation of any provision of the rules of the clearing agency by fine or other fitting sanction.[29] As noted above, FICC proposes to require its members to upgrade and maintain network technology, communication technology, and protocol standards, in accordance with applicable technology standards that FICC would identify and publish via Important Notice on its website. The proposed requirements would enable FICC to avoid communicating with its members using outdated technologies that present security vulnerabilities to FICC. If not adequately addressed, such vulnerabilities could affect FICC's network and its ability to operate. FICC also proposes to amend its Rules to provide that failure to perform a necessary technology upgrade within the required timeframe would subject members to a monetary fine. Because the proposed monetary fine should incentivize FICC's members to upgrade and maintain secure communications technology, thereby reducing FICC's operational risks, the Commission finds the proposed rule change is consistent with the requirements of Section 17A(b)(3)(G) of the Act.[30]

C. Consistency With Rule 17Ad–22(e)(17) Under the Act

Rule 17Ad–22(e)(17)(i) under the Act requires that each covered clearing agency establish, implement, maintain and enforce written policies and procedures reasonably designed to manage the covered clearing agency's operational risks by identifying the plausible sources of operational risk, both internal and external, and mitigating their impact through the use of appropriate systems, policies, procedures, and controls.[31] FICC's operational risks include cyber risks to its electronic systems.

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

To mitigate the foregoing cyber risks, FICC proposes to require its members to upgrade and maintain network technology, and communication technology and protocol standards that meet the standards identified by FICC from time to time. The proposed technology requirements should reduce FICC's cyber risk by requiring members to upgrade and maintain communications technology based on standards set forth by widely accepted organizations such as NIST and the IETF, thereby decreasing the operational risks presented to FICC. Because the proposed technology requirements would help FICC mitigate plausible sources of external operational risk, the Commission finds the proposed changes are consistent with the requirements of Rule 17Ad–22(e)(17)(i) under the Act.[32]

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.[33] As noted above, FICC's operational risks include cyber risks.

As described above, FICC's Rules currently do not require any level or version for network technology, such as a web browser or other technology, or any level or version of communications technology or protocols, such as email encryption, secure messaging, or file transfers, that members may use to connect to or communicate with FICC. FICC designed the proposed technology requirements to reduce cyber risks by requiring its members to upgrade and maintain communications technology based on standards set forth by widely accepted organizations such as NIST and the IETF. Requiring FICC's members to use only secure communications technology would reduce FICC's cyber risks and thereby strengthen the security, resiliency, and operational reliability of FICC's network and other systems. Because the proposed technology requirements would enhance FICC's ability to ensure that its systems have a high degree of security, resiliency, and operational reliability, the Commission finds the Proposed Rule Change is consistent with the requirements of Rule 17Ad–22(e)(17)(ii) under the Act.[34]

[28] *Id.*

[29] 15 U.S.C. 78q–1(b)(3)(G).

[30] *Id.* Additionally, by including the monetary fine provision in its Rules, FICC would enable its members to better identify and evaluate the material costs they might incur by participating in FICC, consistent with Rule 17Ad–22(e)(23)(ii). under the Act, which requires a covered clearing agency to establish, implement, maintain, and enforce written policies and procedures reasonably designed to provide sufficient information to enable participants to identify and evaluate the risks, fees, and other material costs they incur by participating in the covered clearing agency. *See* 17 CFR 240.17Ad–22(e)(23)(ii).

[31] 17 CFR 240.17Ad–22(e)(17)(i).

[32] *Id.*

[33] 17 CFR 240.17Ad–22(e)(17)(ii).

[34] *Id.*

D. Consistency With Rule 17Ad–22(e)(21) Under the Act

Rule 17Ad–22(e)(21)(iv) under the Act requires that each covered clearing agency establish, implement, maintain and enforce written policies and procedures reasonably designed to have the covered clearing agency's management regularly review the efficiency and effectiveness of its use of technology and communication procedures.[35]

As mentioned above, FICC maintains multiple network and communication methods to interact with its members, including certain outdated communication technologies necessary to support members that continue to use such older technologies. FICC believes that continuing to use such outdated technologies could render communications between FICC and some of its members vulnerable to cyber risks. Additionally, members' use of outdated technology delays FICC's implementation of its own internal system upgrades, which by doing so, risks losing connectivity between FICC and a number of its members. Finally, FICC states that it currently expends unnecessary resources to maintain outdated communications channels. In other words, FICC has subjected its network communication methods to review for efficiency and effectiveness. As a result, to enhance the efficiency and effectiveness of its technology and communication procedures, FICC proposes to require its members to upgrade and maintain network technology, communication technology, and protocol standards, in accordance with applicable technology standards that FICC would identify and publish via Important Notice on its website. Because the Proposed Rule Change is an outgrowth of FICC's review of the efficiency and effectiveness of its technology and communication procedures, the Commission finds the Proposed Rule Change is consistent with the requirements of Rule 17Ad–22(e)(21)(iv) under the Act.[36]

IV. Conclusion

On the basis of the foregoing, the Commission finds that the Proposed Rule Change is consistent with the requirements of the Act and in particular with the requirements of Section 17A of the Act[37] and the rules and regulations promulgated thereunder.

It is therefore ordered, pursuant to Section 19(b)(2) of the Act[38] that Proposed Rule Change SR–FICC–2022–003, be, and hereby is, *approved*.[39]

For the Commission, by the Division of Trading and Markets, pursuant to delegated authority.[40]

J. Matthew DeLesDernier,

Assistant Secretary.

[FR Doc. 2022–15004 Filed 7–13–22; 8:45 am]

BILLING CODE 8011–01–P

SECURITIES AND EXCHANGE COMMISSION

[SEC File No. 270–780, OMB Control No. 3235–0733]

Proposed Collection; Comment Request; Extension: Rule 194

Upon Written Request, Copies Available From: Securities and Exchange Commission, Office of FOIA Services, 100 F Street NE, Washington, DC 20549–2736

Notice is hereby given that pursuant to the Paperwork Reduction Act of 1995 (''PRA'') (44 U.S.C. 3501 *et seq.*), the Securities and Exchange Commission (''Commission'') is soliciting comments on the existing collection of information provided for in Commission Rule of Practice 194, (17 CFR 240.194), under the Securities Exchange Act of 1934 (15 U.S.C. 78a *et seq.*). The Commission plans to submit this existing collection of information to the Office of Management and Budget (''OMB'') for extension and approval.

Rule of Practice 194 provides a process for security-based swap dealers and major security-based swap participants (collectively, ''SBS Entity'') to make an application to the Commission for an order permitting an associated person who is subject to a statutory disqualification to effect or be involved in effecting security-based swaps on behalf of the SBS Entity. Rule of Practice 194 specifies the process for obtaining relief from the statutory prohibition in Exchange Act Section 15F(b)(6), including by setting forth the required showing, the form of application and the items to be addressed with respect to associated persons that are natural persons. An SBS Entity is not required to file an application under Rule of Practice 194 with respect to certain associated persons that are subject to a statutory disqualification, as provided for in paragraph (h) of Rule of Practice 194. To meet those requirements, however, the SBS Entity is required to file a notice with the Commission.

It is estimated that approximately 50 entities may fit within the definition of security-based swap dealer and up to five entities may fit within the definition of major security-based swap participant—55 SBS Entities in total. The Commission anticipates that, on an average annual basis, only a small fraction of the natural persons at an SBS Entity would be subject to a statutory disqualification. Accordingly, based on available data, the Commission estimates that, on an average annual basis, the Commission would receive up to five applications in accordance with Rule of Practice 194 with respect to associated persons that are natural persons, and five notices pursuant to proposed Rule of Practice 194(h) with respect to associated persons that are natural persons. The Commission estimates that the average time necessary for an SBS Entity to research the questions, and complete and file an application under Rule of Practice 194 with respect to associated persons that are natural persons is approximately 30 hours, for a total of approximately 150 burden hours per year for all SBS Entities. The Commission estimates that approximately five SBS Entities will provide notices pursuant to Rule of Practice 194(h) for one natural person each on an average annual basis taking approximately 6 hours per notice, for a total of approximately 30 burden hours per year for all SBS Entities providing the notices for an estimated five natural persons. As such, the combined estimated annual hour burden for all SBS Entities to complete applications and notices pursuant to Rule of Practice 194 is approximately 180 hours per year (150 + 30).

Written comments are invited on: (a) whether the proposed collection of information is necessary for the proper performance of the functions of the Commission, including whether the information shall have practical utility; (b) the accuracy of the Commission's estimates of the burden of the proposed collection of information; (c) ways to enhance the quality, utility, and clarity of the information collected; and (d) ways to minimize the burden of the collection of information on respondents, including through the use of automated collection techniques or other forms of information technology. Consideration will be given to comments and suggestions submitted by September 12, 2022.

[35] 17 CFR 240.17Ad–22(e)(21)(iv).

[36] *Id.*

[37] 15 U.S.C. 78q–1.

[38] 15 U.S.C. 78s(b)(2).

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

[40] 17 CFR 200.30–3(a)(12).