EXHIBIT 5

FIXED INCOME CLEARING CORPORATION

GOVERNMENT SECURITIES DIVISION RULEBOOK

TEXT OF PROPOSED RULE CHANGE

Bold and underlined text indicates proposed added language.

~~**Bold and strikethrough text**~~ indicates proposed deleted language.

RULE 1 – DEFINITIONS

* * *

Cybersecurity Confirmation

The term "Cybersecurity Confirmation" means a written document provided to the Corporation by all Members, Sponsoring Members and CCIT Members (for purposes of this definition, collectively referred to as "Members") and applicants for such membership 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 Member 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 Member 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 Member 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 Member 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 Member's or applicant's system that connects to and/or interacts with the Corporation.**

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

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

* * *

RULE 2A – INITIAL MEMBERSHIP REQUIREMENTS

* * *

Section 5 – Application Documents

Each applicant to become a Member shall, as required by the Corporation from time to time, complete and deliver to the Corporation an Applicant Questionnaire in such form as may be prescribed by the Corporation. An applicant seeking membership in the Netting System shall also deliver to the Corporation the financial reports, other reports, opinions and other information as the Corporation determines appropriate.

As part of its membership application, ~~**E**~~**e**ach applicant (as determined by the Corporation with regard to membership type) shall complete and deliver to the Corporation **(1)** a FATCA Certification ~~**as part of its membership application**~~**, and (2) a Cybersecurity Confirmation**.

Each applicant to become a Member must also fulfill, within the time frames established by the Corporation, any operational testing requirements (the scope of such testing to be determined by the Corporation in its sole discretion) and related reporting requirements (such as reporting the test results to the Corporation in a manner specified by the Corporation) that may be imposed by the Corporation to ensure the operational capability of the applicant.

If the Corporation determines that a legal opinion, or update thereto, submitted by an applicant, indicates that the Corporation could be subject to Legal Risk (as defined in Section 2 of Rule 4) with respect to such applicant, the Corporation shall have the right to take, and/or require the applicant to take, appropriate action(s) to mitigate such Legal Risk, including, but not limited to, requiring the applicant to post additional Clearing Fund as set forth in Section 2 of Rule 4.

Except as otherwise provided in Rule 29, any information furnished to the Corporation pursuant to this Rule shall be held in at least the same degree of confidence as may be required by law or the rules and regulations of the appropriate regulatory body having jurisdiction over the applicant or Member.

* * *

RULE 3 – ONGOING MEMBERSHIP REQUIREMENTS

* * *

Section 2 – Reports by Netting Members

Each Netting Member shall submit to the Corporation the reports, financial or other information set forth below and such other reports, financial and other information as the Corporation from time to time may reasonably require. Unless specifically set forth below, the time periods prescribed by the Corporation are set forth in the form of notices posted at the Corporation's Website and/or distributed by the Corporation from time to time. It shall be the Member's responsibility to retrieve all notices daily from the Website.

* * *

In addition to all of the above, on a periodic basis, GCF Counterparties must submit information related to the composition of their NFE-Related Accounts. This information shall be submitted to the Corporation containing the information, in the format and within the timeframes specified by guidelines issued by the Corporation from time to time.

In addition to all of the above, each Member 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.

Notwithstanding anything to the contrary in this Rule, if a Member qualifies for more than one category of Netting System membership, the Corporation, in its sole discretion, may require that such member provide those reports and other financial or other information required to be provided to the Corporation by Members of any of those membership categories for which such Member qualifies.

* * *

RULE 3B – CENTRALLY CLEARED INSTITUTIONAL TRIPARTY SERVICE

* * *

Section 3 – Membership Application Process to Become a CCIT Member

* * *

(c) Each applicant shall complete and deliver to the Corporation**:**

(i) a FATCA Certification as part of its membership application. Without limiting the generality of the foregoing, if an applicant is a FFI Member, the Corporation shall require such applicant to certify and periodically to recertify to the Corporation that it is FATCA Compliant under such procedures as are set forth under FATCA, unless such requirements have been explicitly waived in writing by the Corporation; provided, however, that no such waiver will be issued if it shall cause the Corporation to be obligated to withhold under FATCA on gross proceeds from the sale or other disposition of any property. In addition, as part of its membership application, such applicant must agree that it shall indemnify the Corporation for any loss, liability or expense sustained by the Corporation as a result of its failing to be FATCA Compliant**; and**

(ii) a Cybersecurity Confirmation.

* * *

Section 5 – On-going Membership Requirements

(a) The eligibility qualifications and standards set forth above in this Rule shall be continuing membership requirements. In addition, each CCIT Member shall comply with the ongoing requirements set forth below in this Section.

(b) Each CCIT Member shall submit to the Corporation **the following:**

(i) disclosure on at least an annual basis regarding such CCIT Member's Net Assets, any financial statements the CCIT Member makes publicly available and such other reports, financial and other information as the Corporation from time to time may reasonably require. The time periods prescribed by the Corporation for such disclosure are set forth in the form of notices posted at the Corporation's website and/or distributed by the Corporation from time to time. It shall be the CCIT Member's responsibility to retrieve all notices daily from the Corporation's website**; and**

(ii) a completed 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.

* * *

RULE 13 – FUNDS-ONLY SETTLEMENT

* * *

Section 4 – Funds-Only Settling Bank Members

* * *

(d) Each applicant in (b)(i), (b)(ii), (b)(iii) and (b)(iv) shall sign and deliver to the Corporation:

(i) a membership agreement whereby the bank or trust company shall agree to:

(1) abide by the Rules of the Corporation applicable to Funds-Only Settling Bank Members and to be bound by all provisions thereof and that the Corporation shall have all the rights and remedies contemplated by the Rules; and

(2) be bound by any amendment to the Rules of the Corporation with respect to any transaction occurring subsequent to such time such amendment takes effect as fully as though such amendment were now a part of the Rules of the Corporation.

(ii) the "Appointment of Funds-Only Settling Bank and Funds-Only Settling Bank Agreement"; ~~**and**~~

(iii) the agreement(s) authorizing the Corporation's Settlement Agent to utilize NSS for funds-only settlement as the relevant FRB may require**; and**

(iv) a Cybersecurity Confirmation.

* * *

(k) Each Funds-Only Settling Bank shall fulfill, within the timeframe established by the Corporation, any operational testing requirements (the scope of such testing to be determined by the Corporation in its sole discretion) and related reporting requirements (such as reporting test results to the Corporation in a manner specified by the Corporation) that may be imposed by the Corporation from time to time to ensure the continuing operational capability of the Funds-Only Settling Bank.

(l) Each Funds-Only Settling Bank 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.

(~~l~~**m**) In addition to this Rule 13 and applicable provisions of Rule 1, the following Rules and any relevant schedules cited therein shall apply to Funds-Only Settling Bank Members

in the same manner as they apply to Netting Members: Rule 22D (Wind-down of the Corporation), Rule 29 (Release of Clearing Data), Rule 32 (Signatures), Rule 33 (Procedures), Rule 36 (Rule Changes), Rule 37 (Hearing Procedures), Rule 38 (Governing Law and Captions), Rule 39 (Limitations of Liability), Rule 42 (Suspension of Rules), Rule 44 (Action by the Corporation), Rule 45 (Notices), Rule 46 (Interpretation of Terms), Rule 47 (Interpretation of Rules), Rule 48 (Disciplinary Proceedings), and Rule 50 (Market Disruption and Force Majeure).

* * *

FIXED INCOME CLEARING CORPORATION

MORTGAGE-BACKED SECURITIES DIVISION

CLEARING RULES

RULE 1 - DEFINITIONS

* * *

Cybersecurity Confirmation

The term "Cybersecurity Confirmation" means a written document provided to the Corporation by all Members and applicants for membership 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 Member 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 Member 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 Member 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 Member 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 Member's or applicant's system that connects to and/or interacts with the Corporation.**

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

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

* * *

RULE 2A – INITIAL MEMBERSHIP REQUIREMENTS

* * *

Section 3 – Application Documents

Each applicant to become a Clearing Member shall, as required by the Corporation from time to time, complete and deliver to the Corporation an Applicant Questionnaire in such form as may be prescribed by the Corporation. An applicant seeking membership in the Clearing System shall also deliver to the Corporation the financial reports, other reports, opinions and other information as the Corporation requires.

As part of its membership application, ~~**E**~~**e**ach applicant (as determined by the Corporation with regard to membership type) shall complete and deliver to the Corporation **(1)** a FATCA Certification~~ **as part of its membership application**~~**, and (2) a Cybersecurity Confirmation**.

If the Corporation determines that a legal opinion, or update thereto, submitted by an applicant indicates that the Corporation could be subject to Legal Risk as defined in Rule 4 with respect to such applicant, the Corporation shall have the right to take, and/or require the applicant to take, appropriate action(s) to mitigate such Legal Risk, including, but not limited to, requiring the applicant to post additional Clearing Fund as set forth in Rule 4.

* * *

RULE 3 – ONGOING MEMBERSHIP REQUIREMENTS

* * *

Section 2 – Reports by Clearing Members

Each Clearing Member shall submit to the Corporation the reports and other information set forth below and such other reports and information as the Corporation from time to time may reasonably require. Unless specifically set forth below, the time periods prescribed by the Corporation are set forth in the form of notices posted at the Corporation's website and/or distributed by the Corporation from time to time. It shall be the Member's responsibility to retrieve all notices daily from the website.

* * *

If the Corporation determines that a legal opinion, or update thereto, submitted by a Member, indicates that the Corporation could be subject to Legal Risk (as defined in Rule 4) with respect to such Member, the Corporation shall have the right to take, and/or require the Member to take, appropriate action(s) to mitigate such Legal Risk, including, but not limited to, requiring the Member to post additional Clearing Fund as set forth in Rule 4.

In addition to all of the above, each Member 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.

Notwithstanding anything to the contrary in this Rule, if a Member qualifies for more than one category of Clearing System membership, the Corporation, in its sole discretion, may require that such Member provide those reports and other financial or other information required to be provided to the Corporation by Members of any of those membership categories for which such Member qualifies.

* * *

RULE 3A – CASH SETTLMENT BANK MEMBERS

* * *

(d) Each applicant in subsections (b)(i) through (b)(iv) shall sign and deliver to the Corporation:

(i) a membership agreement whereby the bank or trust company shall agree to:

(1) abide by the Rules of the Corporation applicable to Cash Settling Bank Members and to be bound by all provisions thereof and that the Corporation shall have all the rights and remedies contemplated by the Rules; and

(2) be bound by any amendment to the Rules of the Corporation with respect to any transaction occurring subsequent to such time such amendment takes effect as fully as though such amendment were now a part of the Rules of the Corporation.

(ii) the "Appointment of Cash Settling Bank and Cash Settling Bank Agreement"; ~~and~~

(iii) the agreement(s) authorizing the Corporation's Settlement Agent to utilize NSS for cash settlement as the relevant FRB may require**; and**

(iv) a Cybersecurity Confirmation.

* * *

(k) Each Cash Settling Bank shall fulfill, within the timeframe established by the Corporation, any operational testing requirements (the scope of such testing to be determined by the Corporation in its sole discretion) and related reporting requirements (such as reporting test results to the Corporation in a manner specified by the Corporation) that may be imposed by the Corporation from time to time to ensure the continuing operational capability of the Cash Settling Bank.

(l) Each Cash Settling Bank 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.

(~~l~~**m**) In addition to the applicable provisions of these Rules where Cash Settling Bank Members are mentioned, the following Rules and any relevant schedules cited therein shall apply to Cash Settling Bank Members in the same manner as they apply to Members: Rule 17B, "Winddown of the Corporation," Rule 22, "Release of Clearing Data," Rule 24, "Signatures," Rule 27, "Rule Changes," Rule 28, "Hearing Procedures," Rule 29, "Governing Law and Captions," Rule 30, "Limitations of Liability," Rule 33, "Suspension of Rules in Emergency Circumstances," Rule 34, "Action by the Corporation," Rule 35, "Notices," Rule 36, "Interpretation of Terms," Rule 37, "Interpretation of Rules," Rule 38 "Disciplinary Proceedings," and Rule 40 "Market Disruption and Force Majeure."

* * *

FIXED INCOME CLEARING CORPORATION

MORTGAGE-BACKED SECURITIES DIVISION

EPN RULES

ARTICLE I
DEFINITIONS AND GENERAL PROVISIONS

Rule 1. Definitions

* * *

Cybersecurity Confirmation

The term "Cybersecurity Confirmation" means a written document provided to the Corporation by all EPN Users 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 EPN User 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 EPN User 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 EPN User 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 EPN User 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 EPN User's or applicant's system that connects to and/or interacts with the Corporation.

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

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

* * *

ARTICLE III
EPN USERS

Rule 1. Requirements Applicable to EPN Users

* * *

Sec. 2. Approval of Applicants

The Corporation shall approve an EPN User Profile, submitted by an applicant, to become an EPN User if the applicant:

(a) has sufficient financial ability to meet its obligations to the Corporation; ~~**and**~~

(b) the applicant has affirmatively shown that it has the ability to satisfactorily communicate with the Corporation, fulfill anticipated commitments to and meet the operational requirements of the Corporation with necessary promptness and accuracy, and conform to any condition and requirement that the Corporation reasonably deems necessary for its protection or that of its Participants. The applicant agrees that it must fulfill, within the timeframes established by the Corporation, operational testing requirements (the scope of such testing to be determined by the Corporation in its sole discretion) and related reporting requirements (such as reporting test results to the Corporation in a manner specified by the Corporation) that may be imposed by the Corporation to ensure the continuing operational capability of the applicant**; and**

(c) has completed and delivered to the Corporation a Cybersecurity Confirmation.

* * *

Sec. 8. General Continuance Standards

A. Ongoing Obligation to Notify the Corporation

An EPN User shall promptly inform the Corporation, both orally and in writing, if the EPN User is no longer in compliance with any of the requirements for admission to membership set forth in the EPN Rules. Notification must take place within two Business Days from the date on which the EPN User first learns of its non-compliance. In addition, an EPN User shall notify the Corporation within two Business Days of learning of an investigation or proceeding to which it is or is becoming subject that would cause the EPN User to fall out of compliance with any of the relevant requirements for membership set forth in the EPN Rules. Notwithstanding the previous sentence, the EPN User shall not be required to notify the Corporation if doing so would cause the EPN User to violate an applicable law, rule or regulation. If (a) the EPN User fails to maintain the relevant requirements for admission to membership, including but not limited to operational testing and related reporting requirements imposed by the Corporation from time to time; (b) the EPN User violates any EPN Rule or other agreement with the Corporation; (c) the EPN User fails to satisfy in a timely manner any obligation to the

Corporation; (d) there is a Reportable Event relating to such EPN User; or (e) the Corporation otherwise deems it necessary or advisable, in order to protect the Corporation, its other EPN Users, or its creditors or investors, to safeguard securities and funds in the custody or control of the Corporation, or to promote the prompt and accurate processing, clearance or settlement of securities transactions, the Corporation will undertake action to determine the status of the EPN User and its continued eligibility.

Furthermore, an EPN User must submit to the Corporation written notice of any Reportable Event at least 90 calendar days prior to the effective date of such Reportable Event unless the EPN User demonstrates that it could not have reasonably done so, and provided notice, both orally and in writing, to the Corporation as soon as possible.

In addition, if the Corporation has reason to believe that an EPN User may fail to comply with any of the EPN Rules, the Corporation may require the EPN User to provide it, within such timeframe, in such detail, and pursuant to such manner as the Corporation shall determine, with assurances in writing of a credible nature that the EPN User shall not, in fact, violate any of the EPN Rules.

B. Ongoing Obligation to Provide Cybersecurity Confirmation

As a condition to continued membership, EPN Users 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.

* * *