EXHIBIT 5

OCC Rules

Underlined text indicates new text

CHAPTER II – MISCELLANEOUS REQUIREMENTS

* * * * *

RULE 219 – Cybersecurity Confirmation

(a) Each Clearing Member and applicant for clearing membership shall complete and submit a form, provided by the Corporation, that confirms the existence of an information system cybersecurity program and includes required representations as determined by the Corporation ("Cybersecurity Confirmation").

(i) Each applicant for clearing membership shall submit a completed Cybersecurity Confirmation as part of its application materials.

(ii) Each Clearing Member shall submit a completed Cybersecurity Confirmation at least every two years and not later than 180 calendar days from the date that OCC notifies the Clearing Member that an attestation is required.

(b) The Cybersecurity Confirmation shall consist of representations including, but not limited to, the following:

(1) The Clearing Member or applicant for clearing membership 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 Clearing Member or applicant for clearing membership 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. OCC may consider requests to recognize additional best practices and guidelines that are not 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 Clearing Member or applicant for clearing membership 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 Clearing Member's or applicant's system that connects to and/or interacts with the Corporation.

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

- The Clearing 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 Information Memorandum published 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 Information Memorandum published 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 Clearing Member or applicant, such that the findings of that review are shared with these governance bodies.

(c) The Cybersecurity Confirmation shall be signed by a designated senior executive of the Clearing Member or applicant who is authorized to attest to these matters.

* * * * *