DCO Rules

UNITED STATES
COMMODITY FUTURES TRADING COMMISSION

Submitter Information

Organization Name
Options Clearing Corporation

Organization Type	**Organization Acronym**
DCO	OCC
Submitted By	**Email Address**
[redacted]	[redacted]

Cover Sheet

Submission Number	**Submission Date**
2611-1615-3623-33	11/16/2026 3:36:23 PM ET

Submission Type
40.6(a) Rule Certification

Submission Description
Rule Certification by The Options Clearing Corporation Concerning Revisions to OCC Rule 213 – Cybersecurity Obligations.

☐ **Request Confidential Treatment**

Registered Entity Identifier Code

Rule Numbers
Rule 213

Date of Intended Implementation
12/1/2026

Documents

CFTC Self-Certification - Proposed Revisions to OCC Rule 213.pdf
Exhibit A_CFTC Self Certification.pdf

Request For Confidential Treatment - Detailed Written Justification

N/A

THE FOUNDATION FOR SECURE MARKETS

Options Clearing Corporation
125. S. Franklin Street, Suite 1200
Chicago, IL 60606
312 322 6200 | theocc.com

November 16, 2026

VIA CFTC PORTAL
Christopher J. Kirkpatrick
Office of the Secretariat
Commodity Futures Trading Commission
Three Lafayette Centre
1155 21st Street, N.W.
Washington, DC 20581

Re: Rule Certification by The Options Clearing Corporation Concerning Revisions to OCC Rule 213 – Cybersecurity Obligations.

Dear Secretary Kirkpatrick:

Pursuant to Section 5c(c)(1) of the Commodity Exchange Act, as amended ("Act"), and Commodity Futures Trading Commission ("CFTC") Regulation 40.6, The Options Clearing Corporation ("OCC") hereby certifies a rule change concerning revisions to OCC Rule 213 – Cybersecurity Obligations. The date of implementation of the rule is at least 10 business days following receipt of the certification by the CFTC. The proposal has also been submitted to the Securities and Exchange Commission ("SEC") under Section 19(b) of the Securities Exchange Act of 1934 ("Exchange Act") and Rule 19b-4 thereunder. The change will not be implemented until OCC has obtained all necessary regulatory approvals.

In conformity with the requirements of Regulation 40.6(a)(7), OCC states the following:

Explanation and Analysis

The purpose of this rule certification is to amend OCC Rule 213 – Cybersecurity Obligations ("Rule 213") to further enhance OCC's security protocols and promote resiliency in OCC's approach to assessing and managing cybersecurity risks. OCC's proposed changes to Rule 213 would, among other things, (i) establish the concept of a "Major Clearing Member System Event," in which OCC would be authorized to take certain action, including disconnection of a Clearing Member, or its Third-Party Service Provider, connected to OCC's Systems (as defined below); (ii) enhance the requirements of a Clearing Member to notify OCC in the event of a Security Incident (which would be redefined as a "Clearing Member System Event"); (iii) remove language that invites a Clearing Member to assess potential impact of a Clearing Member System Event on OCC's Systems and clarify OCC's authority to assess such incident and determine impact; (iv) provide OCC with the authority to inform, or require the Clearing Member to inform, the Clearing Member's Third-Party Service Provider (as defined below) of the Clearing Member System Event; (v) update

and add defined terms used throughout Rule 213; and (vi) incorporate other reporting, testing and approval requirements, process, obligations, and governance necessary for reconnection.

The proposed changes to OCC Rule 213 are contained in Exhibit A. Material proposed to be added is marked by underlining and material proposed to be deleted is marked with strikethrough text. All terms with initial capitalization that are not otherwise defined herein have the same meaning as set forth in the OCC By-Laws and Rules.[1]

Overview

OCC is a CFTC registered derivatives clearing organization ("DCO") and a clearing agency for standardized equity options listed on national securities exchanges registered with the SEC. In its role as a DCO, and as a registered clearing agency, OCC acts as a central counterparty ("CCP") that guarantees all contracts it clears. Organizations become OCC Clearing Members to facilitate the clearing and settlement of their customer transactions or proprietary transactions through OCC. More specifically, OCC guarantees the performance of its Clearing Members for all transactions cleared by OCC by becoming the buyer to every seller and the seller to every buyer (or the lender to every borrower and the borrower to every lender, in the case of stock loan transactions). In 2012, OCC was designated as a systemically important financial market utility ("SIFMU") by the Financial Stability Oversight Council pursuant to Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 ("Dodd-Frank Act").[2] Such designation highlights the critical role that OCC plays in ensuring the stability and integrity of the financial markets.

OCC is exposed to cybersecurity risks through its connections with Clearing Members and with the Third-Party Service Providers that connect to OCC's Systems on behalf of Clearing Members. Such cybersecurity risks have the potential to impact OCC, as well as market participants, as a cybersecurity attack on OCC may lead to the loss of data or system integrity, unauthorized disclosure of sensitive information, or an inability to conduct essential clearance and settlement functions. Moreover, as a SIFMU, a failure or disruption to OCC could threaten the stability of the financial system in the United States. Therefore, OCC believes it is prudent to enhance the cybersecurity notification obligations of its Clearing Members and strengthen OCC's ability to protect against and respond to such events to safeguard OCC's Systems and information against cyberattacks.

---

1 OCC's By-Laws and Rules can be found on OCC's public website: https://www.theocc.com/Company-Information/Documents-and-Archives/By-Laws-and-Rules.

2 Financial Stability Oversight Council 2012 Annual Report, Appendix A: Designation of Systemically Important Financial Market Utilities, at 145 (2012), https://home.treasury.gov/system/files/261/2012-Appendix-A-Designation-of-Systemically-Important-Market-Utilities.pdf.

In November 2023, OCC received approval[3] from the SEC to amend certain provisions in OCC's Rules relating to a Clearing Member's obligation to address a "Security Incident" (currently defined as the occurrence of a cyber-related disruption or intrusion of a Clearing Member's systems that is reasonably likely to pose an imminent risk or threat to OCC's operations). OCC also self-certified this change with the CFTC in June 2023.[4] The amended provisions became OCC's existing Rule 213, which established, among other things: (i) notification requirements of a Clearing Member in the event of a Security Incident and (ii) OCC's security requirements for the reconnection process of a Clearing Member following a Security Incident that results in a Clearing Member's disconnection.

In recent years, OCC has received Rule 213 notifications, however, none have impacted OCC. OCC monitors the threat landscape on an ongoing basis, maintaining a dedicated threat intelligence team responsible for monitoring the activities of threat actors targeting the financial services industry. Through this monitoring, OCC has observed an increase in the frequency and elevated risk of cyber events targeting the industry and the broader marketplace. Considering OCC's experience receiving Rule 213 notifications, together with the increasing frequency and elevated risk of cyber events in the financial services industry at large, OCC has identified opportunities for additional enhancements to Rule 213. Though no specific triggering event necessitated these enhancements, OCC's actions are proactive, taken in light of the elevated risk environment across the industry.

OCC's proposed amendments to Rule 213 are intended to further promote resiliency, strengthen OCC's cybersecurity protocols, and maintain consistency with industry standards, including by aligning OCC's Rules with recent rule amendments[5] of similarly situated self-regulatory organizations ("SROs") with overlapping membership with OCC. Among other things, OCC's proposed enhancements to Rule 213 would:

- Add a defined terms section to Rule 213, including defining OCC's "Systems" to include not only direct connections, but also established communication channels (e.g., access to File Transfer Protocols ("FTPs") for transmitting data or instructions that may be compromised by a systems intrusion to a Clearing Member's back-office systems);

---

3 See Securities Exchange Act Release No. 98979 (Nov. 17, 2023), 88 FR 82441 (Nov. 24, 2023) (SR–OCC–2023–003).

4 The Options Clearing Corporation, Rule Certification Concerning Clearing Member Cybersecurity Obligations, Rule Certification Pursuant to 17 C.F.R.§ 40.6(a) (June 22, 2023), https://www.cftc.gov/filings/orgrules/rules0622233107.pdf.

5 See Securities Exchange Act Release No.104183 (Nov. 17, 2025), 90 FR 52453 (Nov. 20, 2025) (SR-DTC-2025-003), (SR-FICC-2025-006), (SR-NSCC-2025-003).

- Require the Cybersecurity Confirmation to be signed by a senior executive of the Clearing Member or applicant who is authorized to attest to such matters;

- Remove language that invites a Clearing Member to assess the potential impact of a Clearing Member System Event on OCC's Systems and operations when determining whether such incident is reportable, specify the timeframe in which OCC requires a Clearing Member System Event to be reported, and identify the specific information a Clearing Member must include in such notice;

- Establish the concept of a "Major Clearing Member System Event," including a declaration requiring the approval of two or more Designated Officers and prompt notification to the Chairman of the Board of Directors;

- Reorganize and clarify OCC's authority to take action in response to a Clearing Member System Event, including specifying the actions that constitute a "disconnect," and clarify a Clearing Member's related cooperation obligations;

- Add provisions incorporating the reporting, testing, and approval requirements, process, obligations, and governance necessary for reconnection, including the ability for OCC to require an audit report from a Third-Party Cybersecurity Firm; and

- Provide OCC with the authority to inform, or require the Clearing Member to inform, the Clearing Member's Third-Party Service Provider of the Clearing Member System Event if OCC determines, in its discretion, that such action is necessary for the protection of OCC and other Clearing Members.

As described in more detail below, OCC believes its proposed changes will strengthen OCC's security protocols by enhancing Rule 213 to be more efficient, effective and clear in its cybersecurity obligations of Clearing Members so that OCC may better address cybersecurity risks to protect OCC and its Clearing Members. Furthermore, OCC believes its proposed changes will enable OCC's Clearing Members to better understand and prepare for their obligations to OCC as it relates to a cybersecurity event.

Proposed Changes

Proposed Rule 213(a)[6] – Defined Terms

First, OCC proposes to introduce new section (a) titled "Defined Terms." To strengthen the provisions of proposed Rule 213 and further clarify OCC's requirements related to the cybersecurity

[6] Existing Rule 213(a) would be renumbered to Rule 213(b).

obligations of a Clearing Member, OCC proposes to define several terms specifically for the purposes of Rule 213.[7] OCC's proposed changes would:

- Define "Best Practices" to mean policies, procedures, practices or similar standards and guidelines that are reasonably designed and consistent with then current financial-sector cybersecurity standards issued by an authoritative body that is a U.S. governmental entity or agency, an association of a U.S. governmental entity or agency, or a widely recognized industry organization. The purpose of defining "Best Practices" is to clarify the standards that OCC would require a Third-Party Cybersecurity Firm to employ when such firm is engaged, as would be required by OCC Rule 213 as discussed further below. OCC's proposed definition of "Best Practices" aligns with Section 1001(a)(4) of the SEC's Regulation Systems Compliance and Integrity ("Reg SCI").[8]

- Delete OCC's existing definition of a "Security Incident" and replace it with "Clearing Member System Event." OCC proposes to define a "Clearing Member System Event" to mean an incident resulting from the unintended or unauthorized access to, or the malfunction or corruption (whether partial or total) of one or more systems, of a Clearing Member or its Third-Party Service Provider, connected to OCC's Systems. The purpose of re-defining the concept of a "Security Incident" to a "Clearing Member System Event" is to capture only those disruptions to systems connected to OCC's Systems, whether via an established communication channel from a Clearing Member, or through the Clearing Member's Third-Party Service Provider; it is not intended to capture every disruption to every system of the Clearing Member or its Third-Party Service Provider. In addition, as described in further detail in section (d) of proposed Rule 213, OCC proposes to eliminate the existing definition of a "Security Incident" to remove language that invites Clearing Members to assess the potential impact of such incident on OCC's Systems and operations when determining whether an incident is reportable. OCC's existing definition of a "Security Incident," is defined, in part, as an incident, or an incident that is occurring, involving a cyber-related disruption or intrusion of the Clearing Member's systems that is reasonably likely to pose an imminent risk or threat to OCC's operations. OCC believes the language in the existing definition invites Clearing Members to assess whether such incident to their systems would impact OCC, and therefore OCC proposes to eliminate the definition of "Security Incident" and replace the definition with "Clearing Member System Event" in proposed Rule 213.

---

7 OCC's proposed amendments to Rule 213 align with the rule amendments of similarly situated SROs with overlapping membership with OCC, including the National Securities Clearing Corporation ("NSCC"). See supra note 5.

8 17 CFR 242.1001(a)(4).

- Define "OCC's Systems" to mean the systems, equipment and technology networks of OCC, whether owned, leased, or licensed, and including software, hardware, applications, devices, IP addresses, or other addresses or accounts used in an established communication channel with such systems, equipment and technology networks, to provide the services set forth in these Rules, or otherwise used to transact business or connect with OCC. OCC proposes to introduce the definition of "OCC's Systems" for the purposes of Rule 213 to articulate OCC's potentially impacted connections and any means of connectivity in the event of a Clearing Member System Event. OCC's proposed definition incorporates not only direct connections but also references "established communication channels," which OCC believes may include access to File Transfer Protocol ("FTPs") for transmitting data or instructions that may be compromised by a systems intrusion to a Clearing Member's back-office systems.

- Define a "Major Clearing Member System Event" to mean a Clearing Member System Event that has or is reasonably anticipated to, for example, disrupt, degrade, cause a delay in, interrupt or otherwise alter the normal operation of OCC's Systems; result in unauthorized access to OCC's Systems; result in the loss of control of, disclosure of, or loss of OCC's Confidential Information; or cause a strain on, loss of, or overall threat to the OCC's resources, functions, security or operations. The purpose of establishing the concept of a "Major Clearing Member System Event," is to tie the disruption at issue to its effect on the normal operations of OCC. This concept introduces a threshold level in which OCC would be authorized to take action, including disconnection, in the event OCC determines that a Clearing Member System Event rises to the level of a Major Clearing Member System Event. OCC's Information Security Disconnect and Reconnect Procedure would outline how OCC determines that a Clearing Member System Event rises to the level of a Major Clearing Member System Event. OCC believes the concept of a "Major Clearing Member System Event" will strengthen OCC's security protocols by establishing a baseline by which OCC can measure the disruption at issue against its impact on OCC and, as described in further detail below, take action to mitigate risks presented.

- Define "Third-Party Cybersecurity Firm" to mean a firm that, in OCC's reasonable judgement, (A) (i) is well-known and reputable; (ii) is not the subject Clearing Member, or an affiliate or a Third-Party Service Provider of the subject Clearing Member; (iii) is experienced in financial-sector cybersecurity; and (iv) employs Best Practices; or (B) is otherwise determined to be a Third-Party Cybersecurity Firm by OCC. OCC proposes to include this definition to clearly describe the type of firm that OCC would require the subject Clearing Member to engage under proposed Rule 213(g)(3).

- Define "Third-Party Service Provider" to mean an affiliate of any Clearing Member, service bureau or other similar entity, that connects to OCC's Systems on behalf of or for

the benefit of a Clearing Member. This proposed definition would help clarify that OCC Rule 213 applies to a Clearing Member's Third-Party Service Provider's connections to OCC's Systems.

Proposed Rule 213(b) – Cybersecurity Confirmation Submission

Proposed Rule 213(b) incorporates the provision from existing Rule 213(a)(ii) into proposed Rule 213(b)(1) to promote clarification and efficiency. Proposed Rule 213(b) also makes other conforming and non-substantive changes, including reorganizing provisions into a hierarchical structure, and updating language to promote clarity and efficiency.

Existing Rule 213(a) requires Clearing Members and clearing membership applicants to periodically submit a form, provided by OCC, confirming, in part, that they have a cybersecurity program in place ("Cybersecurity Confirmation"). Sections (i) and (ii) of existing Rule 213(a) require that applicants must submit it with their application, and existing Clearing Members must resubmit it at least every two years, within 180 days of the OCC's notice requiring attestation. OCC's proposed changes streamline existing Rule 213(a) into proposed Rule 213(b)(1) by combining the general description of the Cybersecurity Confirmation requirement with the specific timing obligation applicable to Clearing Members into a single paragraph. Specifically, OCC's proposed Rule 213(b)(1) would provide, in part, that each Clearing Member must complete and submit "an attestation at least every two years, and not later than 180 calendar days from the date that OCC notifies the Clearing Member that the attestation is required." In addition, proposed Rule 213(b)(1) would remove the reference to the phrase "applicant for clearing membership" as OCC believes such language is duplicative since it is included in the subsequent provision in proposed Rule 213(b)(2). OCC's proposed changes replace the term "shall" with "must" in proposed Rule 213(b)(1) and proposed Rule 213(b)(2) to promote stronger cadence and readability. OCC's proposed changes also eliminate the specific reference to the word "form" after "attestation." The concept of a "form" and an "attestation" may introduce different meanings, so this proposed change is intended to eliminate ambiguity and maintain consistency with OCC's referenced term, "Cybersecurity Confirmation." OCC also proposes to eliminate the reference that the attestation is "provided by the Corporation" because OCC believes this is unnecessary to specify. Finally, OCC proposes to remove the word "materials" in proposed Rule 213(b)(2) to promote efficiency.

Proposed Rule 213(c)[9] – Representations in the Cybersecurity Confirmation

OCC's proposed changes relocate the signature requirement set forth in existing Rule 213(c), "Execution of the Cybersecurity Confirmation," into the introductory provision of proposed Rule 213(c), "Representations in the Cybersecurity Confirmation" (redesignated from existing Rule 213(b)). As relocated, the requirement would provide that the Cybersecurity Confirmation must be

[9] Existing Rule 213(b) would be renumbered to proposed Rule 213(c).

signed by a senior executive of the Clearing Member or applicant who is authorized to attest to these matters, consistent with the substance of the existing requirement. Existing Rule 213(c) would be deleted in its entirety, as its sole requirement is preserved within proposed Rule 213(c). OCC believes this change is non-substantive and is designed to eliminate duplicative rule text and improve the clarity and organization of Rule 213. OCC's proposed changes also remove the word "designated" from the signature requirement, such that the Cybersecurity Confirmation may be signed by any senior executive of the Clearing Member or applicant who is authorized to attest to these matters, rather than requiring a designated senior executive. Specifically, proposed Rule 213(c) would provide that the Cybersecurity Confirmation "must be signed by a senior executive of the Clearing Member or applicant who is authorized to attest to these matters." OCC believes the term "designated" creates ambiguity. Additionally, OCC believes that removing this term improves operational flexibility by allowing any senior executive with the requisite authorization to sign and improves timely compliance by avoiding delays that could arise if a specifically designated individual is unavailable at the time attestation is required. OCC believes the proposed change preserves the integrity and reliability of the attestation, since the signatory must still be a senior executive with the requisite authorization to attest to these matters.

OCC's proposed changes to Rule 213(c) also make other non-substantive changes, including reorganizing the provisions into a hierarchical structure and replacing the term "shall" with "must" to promote stronger cadence and readability.

Proposed Rule 213(d) – Occurrence of a Clearing Member System Event

OCC's proposed Rule 213(d) would introduce enhanced notification requirements for a Clearing Member in the event of a Clearing Member System Event. More specifically, OCC's proposed changes would introduce a particular timeframe required for Clearing Members to report such incident and specify the information that must be included in the notification.

First, as referenced above in the proposed "Defined Terms" section, OCC proposes to re-define and broaden the definition of "Security Incident" to "Clearing Member System Event." In alignment with this proposed change, OCC would also eliminate the existing definition of a "Security Incident" in proposed Rule 213(d), which states in part, that such incident is one that is occurring involving a cyber related disruption or intrusion of the Clearing Member's systems that is reasonably likely to pose an imminent risk or threat to OCC's operations.

Second, OCC's proposed changes would require that a Clearing Member experiencing a Clearing Member System Event must notify OCC immediately "in writing, but no later than two hours" after the Clearing Member becomes aware or should be aware that there has been a Clearing Member System Event. The purpose of including a specific timeframe of two hours for which a Clearing Member System Event must be reported is to clarify OCC's existing standard of "immediate" in order to help mitigate the risk presented by a Clearing Member or its Third-Party

Service Provider that is experiencing such incident.[10] OCC believes that the term "immediately," standing alone, may be interpreted differently and therefore could create uncertainty and inconsistent compliance. By pairing "immediately" with a definite, objective two-hour limit, OCC's Clearing Members will have a clear, unambiguous benchmark for timely notification. By receiving notification of a Clearing Member System Event within two hours of its occurrence, OCC believes it will be able to address and respond to such event in a timely manner and take proactive steps to reduce any future risk presented to OCC and its Clearing Members. If a Clearing Member does not report a Clearing Member System Event within the notification timeframe set forth in section (d), OCC will evaluate the facts and circumstances of the delay in notification to determine whether a rule violation has occurred that is subject to OCC's disciplinary process under Chapter XII of OCC's Rules.

Third, OCC's proposed changes require that notification of proposed section 213(d) must, at a minimum include the following information (as described below), and any such information unconfirmed or otherwise unknown may be identified by the Clearing Member as "Unknown." OCC's existing Rule 213 does not expressly set out requirements for what to include in a notification of a Clearing Member System Event. While OCC already obtains the required information outlined out in proposed Rule 213(d) through its existing practice, the required information is not memorialized in OCC's Rules, policies, or procedures. This practice has historically included, among other things, requests regarding the legal entity name of the Clearing Member, contact information of individuals authorized to act on its behalf, and key details of the incident such as its nature, status, systems or data affected, and remediation steps taken. OCC typically obtains this information from the Clearing Member via phone or email, depending on the circumstances. This information is generally gathered over the course of OCC's engagement with the Clearing Member as the incident develops and the Clearing Member's own understanding of the incident evolves, rather than all at once at the onset of the incident. As such, the purpose of proposed section 213(d) is to codify what OCC already expects in practice, so that all Clearing Members are aware, in advance, of the information required to be included when reporting a Rule 213 incident.

OCC's proposed changes provide that the information required to be in the notice, if known, include: (i) the legal entity name of the Clearing Member or its Third-Party Service Provider affected by the Clearing Member System Event, (ii) contact information of individuals who are authorized to act on behalf of the subject Clearing Member regarding the Clearing Member System Event, and (iii) key details of the Clearing Member System Event such as event type, event effect, start date, end date, discovery date, scope, and any other notices given that would help to provide additional context of the Clearing Member System Event. As discussed above, OCC's existing Rule 213 does not expressly set out requirements for what information must be included in a notification of a Clearing Member System Event. In practice, OCC would obtain the same details identified in

---

[10] OCC's current Rule 213(d) requires a member to immediately notify OCC and to confirm such notice promptly in writing.

proposed section 213(d), but not all at once and not in the formal manner that proposed section 213(d) establishes.

OCC's proposed changes to Rule 213(d) would provide that the information required in the notice related to "Legal Entities" would include a complete list of the legal entity names of the Clearing Member and any Third-Party Service Providers experiencing or otherwise affected or potentially affected by the Clearing Member System Event. In addition, OCC's proposed changes would require that information required in the notice related to "Contact Information" would include list of persons – with their corresponding titles, primary email addresses and phone numbers, and if those primary email addresses and phone numbers are associated with the systems that are the subject of the Clearing Member System Event, alternate email addresses and phone numbers – who are authorized to act on behalf of the subject Clearing Member regarding the Clearing Member System Event. Furthermore, OCC's proposed changes would provide that information required in the notice related to "Clearing Member System Event Details" would include requirements in sections (A) through (G) of proposed Rule 213(d):

(A) Event Type – the type of Clearing Member System Event, for example an insider threat, phishing attack, Man-in-the-Middle ("MITM")[11] attack, privilege escalation, denial of service, external threat, malware, unauthorized access, ransomware, compromised user account, SQL injections, brute force attack, system compromise, supply chain attacks (as each term is commonly understood by cybersecurity professionals in the financial sector), or other with a provided explanation;

(B) Event Effect – perceived, anticipated, or known effect of the Clearing Member System Event, for example, loss of communication, data corruption, security breach, or other with a provided explanation;

(C) Start Date – date and time when the Clearing Member System Event began;

(D) End Date – date and time when the Clearing Member System Event ended, if applicable;

(E) Discovery Date – date and time when the Clearing Member System Event was first identified;

---

[11] A man-in-the-middle ("MITM") attack is an attack in which an adversary positions itself between two communicating parties in order to intercept and alter the data traveling between them. See National Institute of Standards and Technology, Computer Security Resource Center, Glossary, Man-in-the-Middle Attack (MitM), https://csrc.nist.gov/glossary/term/man_in_the_middle_attack.

(F) Scope – scope of the Clearing Member System Event, including, but not limited to, a list of each affected or likely affected system or data, including OCC's Systems and data, the degree of such affect, and any supporting evidence of such; and

(G) Notices – whether any formal or informal notices or information regarding the Clearing Member System Event was made public and, if so, provide a copy of such notices or information.

The purpose of these proposed changes is to codify OCC's expectations to increase transparency around OCC's existing process. More specifically, OCC's proposed changes codify, within Rule 213(d), the information that OCC has historically requested from Clearing Members during a Rule 213 event. Currently, OCC receives this information from Clearing Members upon request during a Rule 213 event as an incident unfolds, rather than receiving a standardized set of information upfront. By codifying OCC's expectations directly in this Rule, OCC intends to increase transparency and ensure that all Clearing Members know, in advance, precisely what information they must provide when reporting a Rule 213 incident, as well as the types of information OCC may request as its investigation proceeds. OCC believes this advance clarity will enable Clearing Members to prepare more effectively and will allow OCC to more promptly and effectively review and mitigate any risk associated with the incident.

OCC believes that the requested information in the proposed sections (A) through (G), including Legal Entities, Contact Information, and details of the Clearing Member System Event are essential pieces of information that would help OCC to efficiently and effectively review and take action to mitigate risk presented. OCC also believes the proposed changes will allow Clearing Members and their Third-Party Service Providers to better understand and prepare for their obligations to OCC in the event they experience a Clearing Member System Event.

Proposed Rule 213(e)[12] – Declaration of a Major Clearing Member System Event

OCC proposes to introduce new Rule 213(e) sections (1) through (3), which would focus on the declaration of a Major Clearing Member System Event, including the details surrounding who is authorized to declare such event and notification requirements associated with such event.

First, proposed Rule 213(e)(1) would provide that upon becoming aware of a Clearing Member System Event, OCC will consider whether such Clearing Member System Event meets the definition of a Major Clearing Member System Event. The proposed change would also provide that the existence of a Major Clearing Member System Event must be declared by two or more Designated Officers of OCC, in their reasonable judgement.

---

[12] Existing Rule 213(e) would be renumbered to Rule 213(g).

Second, proposed Rule 213(e)(2) would provide that upon declaration of a Major Clearing Member System Event, OCC may act (or refrain from acting) pursuant to this Rule to help address, correct, mitigate or alleviate any and all risks presented to OCC by or related to the Major Clearing Member System Event. The proposed change would also provide that action taken will be in consideration of the risks presented to OCC, including but not limited to, information provided pursuant to this Rule.

The purpose of OCC's Proposed Rule 213(e)(1) through (2) is to clarify that OCC will assess the potential impact of a Clearing Member System Event on OCC's Systems and operations, and OCC will determine to act, or refrain from acting, depending on the details of the Clearing Member System Event. The proposed rule removes any ambiguity that may exist in present language that invites the Clearing Member to assess potential impact of the Clearing Member System Event on OCC's Systems or operations. The purpose of the proposed change is also to clearly define who is authorized to declare a Major Clearing Member System event, specifically, that such a declaration must be made by two or more Designated Officers of OCC. OCC believes it is appropriate that such declaration be made by two or more Designated Officers of OCC to ensure that information regarding the Clearing Member System Event has been escalated to and considered at the highest management level. OCC believes the proposed rule change also provides transparency to Clearing Members and other stakeholders as to who is authorized to declare a Major Clearing Member System Event.

Lastly, OCC's proposed changes introduce a new requirement that OCC notify the Chairman of the Board of Directors following a declaration of a Major Clearing Member System Event. Specifically, proposed Rule 213(e)(3) provides that following declaration of a Major Clearing Member System Event, OCC will promptly notify the Chairman of the Board of Directors of such declaration. Because a Major Clearing Member System Event reflects OCC's determination that a Clearing Member System Event may have a significant impact on OCC's Systems or operations, OCC believes it is appropriate that this information be escalated to the Chairman of the Board of Directors without delay. OCC believes that notifying the Chairman is appropriate because it allows the Chairman to determine, based on the nature and severity of the specific Major Clearing Member System Event, the extent to which the full Board or any relevant Board Committee should be further notified or involved.

Proposed Rule 213(f) – Authority to Take Action and Required Cooperation

Proposed Rule 213(f) would expand upon OCC's existing authority to take action in the event of a Clearing Member System Event and associated Major Clearing Member System Event. More specifically, proposed Rule 213(f) introduces requirements surrounding: (i) OCC's ability to act, or refrain from acting, in the event of a Major Clearing Member System Event, (ii) OCC's responsibility to notify the Clearing Member of any disconnect or material action taken, and (iii) the Clearing Member's responsibility to cooperate fully and to the reasonable satisfaction of OCC in the

event of a Major Clearing Member System Event. Proposed Rule 213(f) also makes other conforming and non-substantive changes, including reorganizing provisions into a hierarchical structure, and updating language to promote clarity and efficiency.

OCC's proposed changes would organize Rule 213(f) into subsections (1) through (4). Proposed Rule 213(f)(1) details, in part, OCC's ability to, in the event of a Clearing Member System Event, take actions reasonably necessary to mitigate any impact to its operations, including actions described in proposed Rule 213(f)(1)(A) through Rule 213(f)(1)(C).[13] OCC's changes to proposed Rule 213(f)(1)(A) make conforming and non-substantive changes to the text, including removing the phrase "the right to." To maintain consistency and align with OCC's proposed definition of OCC's Systems, OCC proposes to eliminate the term "data" before systems in proposed Rule 213(f)(1)(A). Proposed Rule 213(f)(1)(B) is new and provides that OCC may take actions reasonably necessary to mitigate any effects to its operations, including to suspend any and all transmissions, communications, or access between OCC's Systems (together with actions taken under Rule 213(f)(1)(A), "disconnect"). The purpose of this change is to broaden OCC's authority to take action that OCC believes may be necessary to mitigate risk presented by a Clearing Member System Event and associated Major Clearing Member System Event. In addition to OCC's existing authority to disconnect access of a Clearing Member, as described in proposed Rule 213(f)(1)(A), OCC believes the proposed change to expand OCC's authority to suspend any and all transmission, communication or access of a Clearing Member will help to ensure that OCC can adequately address all potential connectivity and communication types of a Clearing Member. OCC also proposes to adopt new Rule 213(f)(1)(C) to provide OCC the authority to act in the event OCC determines that a Major Clearing Member System Event has occurred. Proposed Rule 213(f)(1)(C) provides that OCC may take, or refrain from taking, or require the subject Clearing Member to take or refrain from taking, any and all action that OCC considers appropriate to help address, correct, mitigate or alleviate the Major Clearing Member System Event and, as appropriate and practical, facilitate the continuation of services, which may include issuing instructions to the subject Clearing Member and requiring such Clearing Member to act on such instructions. Examples of actions that OCC considers appropriate may include, but are not limited to, disconnection from OCC's Systems, forced password resets, and requiring the Clearing Member to use alternative communication and file transfer methods (e.g. secure file transport instead of email). The purpose of this proposed change is to provide OCC with the authority to evaluate and address a Major Clearing Member System Event and adequately respond to such event in effort to mitigate impact to OCC and its Clearing Members. Additionally, in the event OCC determines a Major Clearing Member System Event has occurred, by adding the provision that allows OCC to issue instructions and requires the subject Clearing Member to follow those instructions, OCC believes this requirement will help to help facilitate the continuation of services for the subject Clearing Member and alleviate future impact that may otherwise result from the disruption. Specifically, the issuance of instructions allows OCC to direct a more tailored

[13] The proposed changes would not substantively alter this section of 213(f) but include only conforming changes such as changes to match defined terms.

response that is specific to the nature and severity of the Major Clearing Member System Event. This flexibility enables OCC to address the risk presented by a specific Major Clearing Member System Event while, where practicable, preserving the Clearing Member's ability to continue some or all of its services during remediation.

OCC proposes to adopt Rule 213(f)(3), which addresses OCC's notification requirements to the Clearing Member, as well as the subject Clearing Member's obligations to comply with OCC's statutory rules. More specifically, proposed Rule 213(f)(3) would provide that OCC will promptly notify the Clearing Member of any disconnect or other material action that OCC takes with respect to such Clearing Member pursuant to Rule 213. In addition, proposed Rule 213(f)(3) would provide that, notwithstanding any action taken pursuant to Rule 213, the Clearing Member must continue to meet its obligations to OCC and comply with OCC's statutory rules, as defined in its By-Laws. Under OCC's existing Rule 213, if OCC determines that disconnection of a Clearing Member from OCC's Systems is necessary, the Clearing Member must continue to meet its obligations to OCC notwithstanding that disconnection. OCC's existing Rule 213(d) focuses solely on the Clearing Member's continuing obligations following a disconnection and it does not address whether OCC will notify the Clearing Member that a disconnection (or any other action) has occurred. Proposed Rule 213(f)(3) expands the current provision in two respects: (i) it adds a notification obligation on OCC's part, and (ii) it broadens both the scope of triggering actions (from disconnection alone to any material action under the Rule) and the scope of the Clearing Member's continuing obligations to also include compliance with OCC's statutory rules, as the term is defined in OCC's By-Laws.

These proposed changes serve several purposes. First, the purpose of requiring OCC to promptly notify a Clearing Member of any disconnection or other material action taken under this Rule is to provide enhanced transparency to Clearing Members regarding actions that OCC takes that impact them. OCC believes it is prudent to notify the Clearing Member promptly in such event to allow the Clearing Member to better prepare for and understand their obligations to OCC. Second, the proposed change expands the scope of that notification obligation from disconnection alone to "any material action" taken pursuant to the Rule. This may include, for example, modifying the scope and specifications of access of the Clearing Member to OCC's Systems. The purpose of this proposed change is to ensure that Clearing Members receive notice of any material action OCC may take, not solely the most severe action of disconnection. Third, the proposed change broadens the Clearing Member's continuing obligations to apply "notwithstanding any action taken pursuant to this Rule," rather than only "notwithstanding disconnection," removing any ambiguity as to whether a Clearing Member's obligations to OCC continue in the event OCC takes a material action, outside of disconnection. Finally, the proposed change also specifies what obligations the Clearing Member must continue to meet, by adding an express requirement that the Clearing Member comply with the statutory rules of OCC, as defined in OCC's By-Laws. OCC's current Rule 213 refers only generally to the Clearing Member's "obligations to OCC" without specifying what those obligations include. OCC believes the addition of "comply with the statutory rules of OCC, as defined in its By-Laws"

clarifies what those obligations encompass. OCC's proposed changes to proposed Rule 213(f)(3) also make other conforming, non-substantive changes.

Lastly, OCC proposes to adopt new Rule 213(f)(4), which requires that the Clearing Member must cooperate fully and completely with, and to the reasonable satisfaction of, OCC in all matters relating to the Major Clearing Member System Event, including, but not limited: (i) conducting timely investigations and inquiries, as OCC believes reasonably necessary, with respect to any known or unknown information relating to the Clearing Member System Event; (ii) promptly notifying OCC of any material changes, updates, or new information learned regarding the Clearing Member System Event; and (iii) promptly providing any documentation or information requested by OCC, unless not legally permitted to do so, regarding or related to the Clearing Member System Event.[14] The purpose of this proposed change is to provide enhanced transparency to Clearing Members on their obligations to comply with the proposed requirements. OCC believes that cooperation from Clearing Members on matters relating to a Major Clearing Member System Event will help OCC to efficiently and effectively manage and respond to a Major Clearing Member System Event in effort to mitigate risk presented.

Proposed Rule 213(g)[15] Procedures for Reconnection

OCC proposes to update existing Rule 213(e) titled "Procedures for Connecting Following a Security Incident that Results in Disconnection" to Proposed Rule 213(g) titled "Procedures for Reconnection." OCC believes that such change in title is necessary to more accurately encompass the obligations of a Clearing Member pursuant to OCC's authority to act in the event of a Clearing Member System Event, as described in proposed Rule 213(f)(1). The retitled rule sets forth the information that the subject Clearing Member would be required to provide OCC in the event OCC takes action pursuant to proposed Rule 213(f)(1) and includes both substantive and non-substantive changes as described below. Proposed Rule 213(g) also reorganizes existing Rule 213(e) into proposed Rule 213(g)(1) through 213(g)(2), and incorporates new section (3) in proposed Rule 213(g)(3) titled "Report from Third-Party Cybersecurity Firm."

Proposed Rule 213(g)(1) Reconnection Attestation

OCC's proposed Rule 213(g)(1) would be titled "Reconnection Attestation." Proposed Rule 213(g)(1) would include the current requirement that a subject Clearing Member must complete and submit a Reconnection Attestation prior to OCC reestablishing connectivity to OCC's Systems.

---

14 Sections (i) through (ii) described in the narrative would be numbered to proposed Rule 213(f)(4)(A) though proposed Rule 213(f)(4)(C).

15 Existing Rule 213(e) would be renumbered to proposed Rule 213(g).

More specifically, proposed Rule 213(g)(1) would provide that if OCC takes action pursuant to Rule 213(f)(1), the Clearing Member must complete and submit a form as provided by OCC that describes the Clearing Member System Event and includes required representations ("Reconnection Attestation"). OCC proposes to add language to clarify that such requirement must be met prior to OCC reestablishing connectivity to OCC's Systems ("Reconnection"). OCC proposes to relocate the existing provision that states "The Clearing Member also will be required to complete an associated checklist provided by OCC that describes remediation efforts ("Reconnection Checklist")," because OCC believes such text is more appropriately located in proposed Rule 213(g)(2), which outlines the requirements in the Reconnection Checklist. In addition, OCC's proposed changes collapse and consolidate Rule 213(e)(1) into Rule 213(e), which becomes proposed Rule 213(g), such that the signature requirement is now reflected in proposed Rule 213(g)(1). Specifically, OCC's proposed changes reflect that the provision in current Rule 213(e)(1) on the requirement for the Reconnection Attestation to be signed by a designated senior executive becomes included in proposed Rule 213(g)(1). This change is intended to make Rule 213 easier to navigate by grouping related requirements together; it does not alter the Clearing Member's underlying obligation to obtain a signature from an individual who maintains the authorization to sign the Reconnection Attestation. OCC's proposed changes also eliminate the term "designated" when describing the senior executive of the Clearing Member that must sign the Reconnection Attestation. OCC believes the term "designated" creates ambiguity. By removing this term, OCC believes it improves operational flexibility by allowing any senior executive of the Clearing Member[16] with the requisite authorization to sign, and it improves timely compliance by avoiding delays that could arise if a specifically designated individual is unavailable at the time attestation is required. OCC believes the proposed change preserves the integrity and reliability of the attestation, since the signatory must still be a senior executive with the requisite authorization to attest to these matters.

In addition, proposed Rule 213(g)(1)(A) through 213(g)(1)(E) incorporates the requirements in current Rule 213(e)(1)(A) though Rule 213(e)(1)(E) and makes other non-substantive changes including renaming the term "Security Incident" to "Clearing Member System Event," as described in proposed Rule 213(a).

Proposed Rule 213(g)(2) Reconnection Checklist

OCC's proposed Rule 213(g)(2) would be titled "Reconnection Checklist." Proposed Rule 213(g)(2) reorganizes the provisions from existing Rule 213(e)(2) into proposed Rule 213(g)(2) and

[16] A senior executive of the Clearing Member with the requisite authorization to sign may for example include, but is not limited to, a member of the board of directors or a member of senior management with the requisite knowledge and experience to make such an attestation, as determined by the Clearing Member's own delegation of authority and procedures.

subsections (A) through (J) of proposed Rule 213(g)(2) to promote clarity and efficiency. OCC's proposed changes also make other conforming, clarifying and non-substantive changes. More specifically, OCC's proposed changes to Rule 213(g)(2) provide that if OCC takes action pursuant to Rule 213(f)(1), the Clearing Member must complete an associated checklist as provided by OCC that describes remediation efforts ("Reconnection Checklist"), which may require information including but not limited to the information in proposed subsections (A) though (J) of proposed Rule 213(g)(2).

Proposed Rule 213(g)(3) Report from Third-Party Cybersecurity Firm

OCC proposes to adopt Rule 213(g)(3), titled "Report from Third-Party Cybersecurity Firm," which provides that OCC may require that the subject Clearing Member provide a report from a Third-Party Cybersecurity Firm, either as a condition to Reconnection or following Reconnection. OCC's proposed changes describe the information required to be in such report in proposed Rule 213(g)(3)(A) through proposed Rule 213(g)(3)(G).

More specifically, proposed Rule 213(g)(3) states that if OCC takes action pursuant to Rule 213(f)(1), OCC may require, either as a condition to reconnection or following reconnection, that the Clearing Member provide a detailed, comprehensive, and auditable report from a Third-Party Cybersecurity Firm, or a summary or such report that includes: (i) a timeline of the Clearing Member System Event, including all material actions, events, and decisions taken for or relating to the Clearing Member System Event; (ii) a description of the Clearing Member System Event and an explanation of how such disruption was corrected or resolved; (iii) root cause analysis of the Clearing Member System Event; (iv) confirmation that any issues identified by the Third-Party Cybersecurity Firm as severe, critical, or moderate, or comparable categorizations, have been resolved; (v) confirmation of normal or intended operation of the subject system(s), including, but not limited to, the return or replacement of key systems and data stores to pre-Clearing Member System Event resilience, in a safe, secure and proper manner for at least 72 hours; (vi) a description of short-and long-term preventive monitoring and detection recommendations form the Third-Party Cybersecurity Firm; and (vii) any other information reasonably requested to be included by OCC.[17] In the event a Clearing Member is the subject of action pursuant to OCC's authority under proposed Rule 213(f)(1), the purpose of proposed Rule 213(g)(3) is to provide OCC with all necessary information about the subject Clearing Member's disruption and its remediation from an independent, knowledgeable and reputable Third-Party Cybersecurity Firm, so that OCC can determine whether Reconnection is appropriate. OCC's ability to require an audit report from a Third-Party Cybersecurity Firm provides OCC with essential information that will help OCC to fully

[17] The provisions described in subsections (i) through (vii) above would be organized as subsections (A) through (G), respectively, in proposed Rule 213(g)(3).

evaluate the Clearing Member System Event and take steps to mitigate risks presented by such incident.

Proposed Rule 213(h) Reconnection Testing and Approval

OCC's proposed changes would adopt Rule 213(h) titled "Reconnection Testing and Approval, " which would require, prior to any Reconnection, that the subject Clearing Member must demonstrate, as applicable, to OCC's reasonable satisfaction, that it: (i) can operate in a test environment, including, but not limited to, sending and receiving messages and transactions; (ii) can replay or resubmit previously submitted messages or transactions; (iii) can reverse or void previously submitted messages or transactions; (iv) can confirm the integrity of messages and transactions; (v) has alternative communication methods with OCC to facilitate the exchange of messages, transactions, and reports; and (vi) can complete any other such requirements as are reasonably requested by OCC. Furthermore, proposed Rule 213(h)(2) would authorize two or more Designated Officers of OCC to, in their reasonable judgment, approve the Reconnection of a Clearing Member that was the subject of action taken pursuant to proposed Rule 213, after OCC has received all required information pursuant to this Rule, in a form and a substance satisfactory OCC, and that all information necessary for a safe Reconnection and certain testing has occurred, pursuant to proposed Rule 213(h)(1).

The purpose of proposed Rule 213(h) is to ensure that the approval for a Reconnection is not made until OCC has received, to its satisfaction, all necessary information from the Clearing Member, and that OCC confirmed the subject Clearing Member can safely perform the capabilities necessary for submitting, receiving, and correcting information appropriately and in a manner unaffected by the Clearing Member System Event, so as to help mitigate the risk presented by the Reconnection. In addition, OCC believes it is appropriate that the approval of a Reconnection be made by at least two members of OCC's management committee to help ensure that information regarding the Reconnection has been escalated to the highest management level.

Proposed Rule 213(i) Certain Miscellaneous Matters

OCC proposes to adopt Rule 213(i), titled "Certain Miscellaneous Matters," which would address various provisions including, but not limited to, (i) OCC's limited liability to a Clearing Member pursuant to proposed Rule 213; (ii) OCC's authority to inform the subject Clearing Member's Third-Party Service Provider, or require the Clearing Member to inform its Third-Party Service Provider, of a Clearing Member System Event; and (iii) the failure of a Clearing Member to comply with proposed Rule 213.

First, in an effort to promote enhanced transparency to Clearing Members, proposed Rule 213(i)(1) would address, in part, OCC's limited liability to any Clearing Member as it relates to losses arising out of OCC's action or inaction pursuant to proposed Rule 213. More specifically, proposed Rule 213(i)(1) would provide that without limiting any other provisions in these Rules

concerning limitations on liability, neither OCC nor its directors, officers, employees, agents, or contractors shall be liable to any Clearing Member or any customer or client thereof for: (i) any failure, hindrance, interruption or delay in performance in whole or in part of the obligations of OCC under these Rules, if that failure, hindrance, interruption or delay arises out of or relates to a Clearing Member System Event, Major Clearing Member System Event, or any action or inaction pursuant to this Rule 213; or (ii) any loss, liability, damage, cost or expense arising from or relating in any way to any advice, request, requirement, instruction, action or inaction pursuant to this Rule 213.[18] Second, proposed Rule 213(i)(2) would provide that the power of OCC to take any action pursuant to this Rule 213, or to request or require any action, documentation, or information pursuant to this Rule 213, also includes the power to waive, repeal, rescind, revoke, amend, or vary any such action, request, or requirement in consideration of the facts and circumstances. Third, proposed Rule 213(i)(3) would provide that the powers of OCC pursuant to this Rule 213 are in addition to, and not in limitation of, any authority granted elsewhere in these Rules to act as specified therein. The purpose of proposed Rule 213(i)(2) and proposed Rule 213(i)(3) is to promote enhanced transparency to Clearing Member on OCC's authority to take action pursuant to Rule 213 so that Clearing Members can better understand and be prepared for their obligations to OCC.

Fourth, proposed Rule 213(i)(4) would provide that all information related to or regarding a Major Clearing Member System Event and all acts pursuant to this Rule 213 will be considered Confidential Information pursuant to these Rules; provided, however, that the OCC may inform, or direct the Clearing Member to inform, the Clearing Member's Third-Party Service Provider of a Clearing Member System Event if OCC determines, in its discretion, that such action is necessary for the protection of OCC and other Clearing Members. The purpose of the proposed change is to mitigate risk to OCC and its Clearing Members that may be presented by a Clearing Member System Event and associated Major Clearing Member System Event. The proposed changes also provide transparency to Clearing Members on their obligation to inform their Third-Party Service Providers in certain circumstances that OCC deems necessary.

Fifth, proposed Rule 213(i)(5) would provide that the failure of a Clearing Member to comply with the requirements of this Rule 213 may subject the Clearing Member to any and all disciplinary action permitted under these Rules, including, without limitation, suspension. Lastly, proposed Rule 213(i)(6) would provide that a Clearing Member that has authorized another party, such as a Third-Party Service Provider, to access and use OCC's systems will be responsible for such authorized party's compliance with the requirements of this Rule 213 and any compliance failure by that authorized party will be deemed to be a failure of the authorizing Clearing Member. The purpose of proposed Rules 213(i)(5) and 213(i)(6) is to highlight the importance of complying with proposed Rule 213 and the actions OCC may take if there is a failure to comply.

---

[18] The provisions described in (i) through (ii) would be organized as proposed Rule 213(i)(1)(A) through 213(i)(1)(B).

Consistency with DCO Core Principles

OCC reviewed the DCO core principles ("Core Principles") as set forth in the Act, the regulations thereunder, and the provisions applicable to a DCO that elects to be subject to the provisions of 17 CFR Subpart C ("Subpart C DCO"). During this review, OCC identified the following as potentially being impacted:

Risk Management. OCC believes that the proposed changes are consistent with Core Principle D[19] and CFTC Regulation 39.13.[20] Core Principle D requires, in relevant part, that each DCO ensure that it possesses the ability to manage the risks associated with discharging the responsibilities of the DCO through the use of appropriate tools and procedures.[21] The proposed amendments to Rule 213 support this requirement as it relates to operational risk, because they are designed to help OCC assess and take appropriate action to manage the cybersecurity risks that may be introduced to OCC's Systems and information due to a Clearing Member System Event. Because such risks could impact OCC's ability to clear and settle transactions and to discharge its responsibilities as a DCO, the proposed changes enhance OCC's processes to help mitigate risk and better protect OCC and its Clearing Members. Three of the amendments are particularly consistent with Core Principle D: (i) the expanded notification requirements; (ii) the establishment of the Major Clearing Member System Event; and (iii) the process for Reconnection.

First, proposed Rule 213(d) codifies the specific content and timeframe requirements for notification of a Clearing Member System Event. Under proposed Rule 213(d), a Clearing Member would be required to provide OCC with specified information at the onset of a Clearing Member System Event, including but not limited to the event type, effect, scope, start date, end date, discovery date, and any public notices related to the event. This will allow OCC to receive consistent, timely information, which helps minimize the risk that delayed or incomplete information impacts OCC's ability to respond promptly and effectively.

Second, proposed Rule 213(e) establishes the concept of a "Major Clearing Member System Event." Under proposed Rule 213(e), OCC would assess the potential impact of a Clearing Member System Event on OCC's Systems and operations and determine whether to act, depending on the specific details of the event. This removes the ambiguity that may exist in the current rule text, which invites the Clearing Member to assess the impact of its own Clearing Member System Event on OCC's Systems or operations. In addition, proposed Rule

---

19 7 U.S.C. 7a-1(c)(2)(D).

20 17 CFR 39.13.

21 7 U.S.C. 7a-1(c)(2)(D)(i).

213(e) requires that the existence of a Major Clearing Member System Event must be declared by two or more Designated Officers of OCC, in their reasonable judgment, and that OCC must promptly notify the Chairman of the Board. OCC believes this proposed change helps ensure that the most severe threats are escalated to the highest levels of OCC's governance and receive attention and oversight proportionate to their severity. By placing the assessment, the decision to act, and the escalation of severe events with OCC, this proposed change strengthens OCC's ability to manage the risks of a Clearing Member System Event.

Third, proposed Rule 213(h)(1) requires that, prior to Reconnection, a Clearing Member must demonstrate to OCC's reasonable satisfaction that it can, in part, operate in a test environment, send and receive messages and transactions, replay or resubmit previously submitted messages or transactions, reverse or void previously submitted messages or transactions, confirm the integrity of messages and transactions, and maintain alternative communication methods with OCC. These requirements test the Clearing Member's operational capability to interact accurately and reliably with OCC's Systems, rather than relying on the Clearing Member's representation that it is prepared to reconnect. By verifying before Reconnection that a Clearing Member's systems will not transmit corrupted or otherwise unreliable messages or transactions into OCC's Systems, this requirement helps manage the risk to OCC's clearing and settlement operations.

Accordingly, by expanding the notification requirements, establishing the Major Clearing Member System Event, and enhancing the Reconnection process, OCC believes the proposed changes strengthen its tools and procedures for managing risk, consistent with Core Principle D[22] and CFTC Regulation 39.13.[23]

Governance. OCC believes the proposed changes are consistent with Core Principle O[24] and CFTC Regulation 39.24,[25] which together require, in relevant part, that a DCO maintain governance arrangements that are clear and transparent and that specify clear and direct lines of responsibility.

Proposed Rule 213(e)(1) provides that the existence of a Major Clearing Member System Event must be declared by two or more Designated Officers of OCC, and that OCC will provide notification of such declaration to the Chairman of the Board. This establishes a defined pathway from identification of the event, through declaration by two or more Designated Officers, to notification at the Board level. OCC believes this specificity is

---

22 Id.

23 17 CFR 39.13(a).

24 7 U.S.C. 7a-1(c)(2)(O).

25 17 CFR 39.24.

consistent with the "clear and transparent" governance arrangements, required by CFTC Regulation 39.24.[26] It is likewise consistent with the "clear and direct lines of responsibility" required by CFTC Regulation 39.24,[27] because this proposed change assigns responsibility for determining a Major Clearing Member System Event to a specifically identified group of officers.

Similarly, with respect to Reconnection, proposed Rule 213(h)(2) requires that the Reconnection of a Clearing Member following OCC's action pursuant to proposed Rule 213(f)(1) be approved by two or more Designated Officers of OCC. The proposed rule conditions that approval on OCC's receipt of all information required under Rule 213, in a form and substance satisfactory to OCC, and satisfaction of the applicable testing requirements set forth in proposed Rule 213(h)(1). By specifying both who is authorized to approve Reconnection and the steps that must be satisfied before that approval may be granted, proposed Rule 213(h)(2) establishes a clear and transparent approval process, consistent with CFTC Regulation 39.24.[28] The proposed change also identifies, with the same specificity as the Major Clearing Member System Event declaration process, the officers responsible for making a determination to reconnect a Clearing Member. As such, OCC believes the proposed changes are consistent with the "clear and direct lines of responsibility" required by CFTC Regulation 39.24.[29]

System Safeguards. OCC believes that the proposed changes are consistent with the requirements of Core Principle I[30] and CFTC Regulation 39.18.[31] Core Principle I and CFTC Regulation 39.18 require, in relevant part, that each DCO establish and maintain a program of risk analysis and oversight to identify and minimize sources of operational risk through the development of appropriate controls and procedures, and automated systems, that are reliable, secure and have adequate scalable capacity.[32]

As discussed in more detail below, the proposed changes to Rule 213 support Core Principle I by helping OCC (i) identify sources of operational risk, through enhanced notification requirements and the addition of a defined terms section to Rule 213, and (ii) minimize

---

26 17 CFR 39.24(a)(ii).

27 17 CFR 39.24(b)(4).

28 17 CFR 39.24(a)(ii).

29 17 CFR 39.24(b)(4).

30 7 U.S.C. 7a-1(c)(2)(I).

31 17 CFR 39.18(b)(1).

32 7 U.S.C. 7a-1(c)(2)(I); 17 CFR 39.18(b)(1).

sources of operational risk, through new reporting, testing, approval and governance requirements for Reconnection following OCC's action under proposed Rule 213(f)(1).

(i) Identify sources of operational risk:

First, proposed Rule 213(d) outlines the requirements for a Clearing Member to notify OCC of a Clearing Member System Event. Proposed Rule 213(d) specifies the timeframe within which such an event must be reported, and identifies the information the notice must include, such as the event type, effect, scope, and the start, end and discovery dates. The proposed change also removes language that invites a Clearing Member to assess the event's potential impact on OCC's Systems and operations in determining whether the event is reportable. Because a Clearing Member System Event represents an external source of potential operational risk to OCC, OCC's ability to identify and characterize that risk depends on receiving timely, complete and accurate information from the Clearing Member. The specified timeframe and content requirements support OCC's ability to identify the nature and extent of the risk presented. Additionally, receiving that information consistently and promptly helps OCC respond effectively to minimize the risk to OCC and its Clearing Members. As such, OCC believes the enhanced notification requirements in proposed Rule 213(d) are consistent with Core Principle I[33] and CFTC Regulation 39.18.[34]

Second, the defined terms section in proposed Rule 213 helps OCC identify additional sources of operational risk. The proposed definition of OCC's Systems includes established communication channels, such as FTPs, that may be used to transmit data or instructions to a Clearing Member's back-office systems. OCC believes that expanding the definition of OCC's Systems to include these indirect channels is appropriate because a security intrusion can reach OCC through such a channel, in addition to a direct connection. In addition, the proposed definition of "Clearing Member System Event" includes an incident resulting from a Clearing Member's Third-Party Service Provider connected to OCC's Systems. Together, these definitions help OCC better identify the risks presented by a Clearing Member or its Third-party Service Provider. As such, OCC believes the defined terms in proposed Rule 213 are consistent with Core Principle I[35] and CFTC Regulation 39.18.[36]

---

33 7 U.S.C. 7a-1(c)(2)(I).

34 17 CFR 39.18(b)(1).

35 7 U.S.C. 7a-1(c)(2)(I).

36 17 CFR 39.18(b)(1).

(ii) Minimize sources of operational risk:

Proposed Rule 213(h) strengthens the requirements surrounding Reconnection of a Clearing Member, which gives OCC controls and procedures to evaluate whether Reconnection is appropriate and, if so, to ensure that it is safe. Under proposed Rule 213(h)(1), prior to Reconnection, a Clearing Member must demonstrate to OCC's reasonable satisfaction that it can operate in a test environment, replay or resubmit previously submitted messages or transactions, reverse or void previously submitted messages or transactions, confirm the integrity of messages and transactions, and maintain alternative communication methods with OCC. These requirements show whether the specific risks presented by the original Clearing Member System Event, such as data loss or communication failure, have been resolved. By requiring the Clearing Member to demonstrate these capabilities before Reconnection is granted, proposed Rule 213(h)(1) mitigates the risk that reconnecting the Clearing Member would reintroduce the same operational risk to OCC's Systems that necessitated the disconnection in the first place. The Clearing Member must also submit the Reconnection Attestation before OCC reestablishes connectivity, which, together with the testing requirements, allows OCC to identify and address vulnerabilities that may remain in the Clearing Member's environment after a Clearing Member System Event.

In addition, under proposed Rule 213(g)(3), OCC may require a detailed, comprehensive and auditable report from a Third-Party Cybersecurity Firm, either as a condition to or following Reconnection. The report must include, among other things, a timeline of the Clearing Member System Event, a description of the event and how it was corrected or resolved, a root cause analysis, confirmation that any issues identified as severe, critical or moderate have been resolved, confirmation that the affected systems have returned to normal, pre-incident operation for at least 72 hours, and short and long-term preventive monitoring and detection recommendations. This proposed change will enable OCC to evaluate information from a reputable source to help OCC determine whether to reconnect a Clearing Member. Furthermore, the requirement for a root cause analysis supports OCC's identification of the underlying cause of the operational risk, while the requirement for verified confirmation supports minimizing that risk. As such, OCC believes the enhanced Reconnection requirements are consistent with Core Principle I[37] and CFTC Regulation 39.18.[38]

For these reasons, OCC believes that the proposed changes are consistent with the requirements of the DCO Core Principles and the CFTC Regulations thereunder.

---

37 7 U.S.C. 7a-1(c)(2)(I).

38 17 CFR 39.18(b)(1).

Opposing Views

No substantive opposing views were expressed related to the rule amendments by OCC's Board members, Clearing Members or market participants. Public comments on the proposed rule change filed with the SEC, if any, and any OCC response to such comments may be viewed on the SEC's public website.[39]

Notice of Pending Rule Certification

OCC hereby certifies that notice of this rule filing has been given to Clearing Members of OCC in compliance with Regulation 40.6(a)(2) by posting a copy of this certification on OCC's website concurrently with the filing of this submission.

Certification

OCC hereby certifies that the rule set forth at Exhibit A of the enclosed filing complies with the Act and the CFTC's regulations thereunder.

Should you have any questions regarding this matter, please do not hesitate to contact me.

Sincerely,

/s/ [redacted]

[redacted]
[redacted]
The Options Clearing Corporation

Enclosure: Exhibit A

[39] See Options Clearing Corporation (OCC) Rulemaking, https://www.sec.gov/rules-regulations/self-regulatory-organization-rulemaking/occ.

EXHIBIT A



OCC Rules

Blue underlined text indicates additions

~~Red strikethrough~~ text indicates deletions

~~Green double-strikethrough~~ indicates deletions to existing Rule 213 that are being relocated within OCC's Rules, as indicated by green underlined text and in [brackets]

RULE 213 – Cybersecurity Obligations

(a) *Defined Terms*. For purposes of this Rule 213, the following terms have the following meanings:

(1) "Best Practices" means policies, procedures, practices or similar standards and guidelines that are reasonably designed and consistent with then current financial- sector cybersecurity standards issued by an authoritative body that is a U.S. governmental entity or agency, an association of a U.S. governmental entity or agency, or a widely recognized industry organization.

(2) "Clearing Member System Event" means an incident resulting from the unintended or unauthorized access to, or the malfunction or corruption (whether partial or total) of one or more systems, of a Clearing Member or its Third-Party Service Provider, connected to the Corporation's Systems.

(3) The "Corporation's Systems" means the systems, equipment and technology networks of the Corporation, whether owned, leased, or licensed, and including software, hardware, applications, devices, IP addresses, or other addresses or accounts used in an established communication channel with such systems, equipment and technology networks, to provide the services set forth in these Rules, or otherwise used to transact business or connect with the Corporation.

(4) "Major Clearing Member System Event" means a Clearing Member System Event that has or is reasonably anticipated to, for example, disrupt, degrade, cause a delay in, interrupt or otherwise alter the normal operation of the Corporation's Systems; result in unauthorized access to the Corporation's Systems; result in the loss of control of, disclosure of, or loss of the Corporation's Confidential Information; or cause a strain on, loss of, or overall threat to the Corporation's resources, functions, security or operations.

(5) "Third-Party Cybersecurity Firm" means a firm that, in the Corporation's reasonable judgement, (A) (i) is well-known and reputable; (ii) is not the subject Clearing Member, or an affiliate or a Third-Party Service Provider of the subject Clearing Member; (iii) is experienced in financial-sector cybersecurity; and (iv) employs Best Practices; or (B) is otherwise determined to be a Third-Party Cybersecurity Firm by the Corporation.

(6)"Third-Party Service Provider" means an affiliate of any Clearing Member, service bureau or other similar entity, that connects to the Corporation's Systems on behalf of or for the benefit of a Clearing Member.

(~~a~~b) *Cybersecurity Confirmation Submission*.

(1) Each Clearing Member ~~and applicant for clearing membership shall~~must complete and submit an attestation ~~form, provided by the Corporation,~~ at least every two years, and not later than 180 calendar days from the date that the Corporation notifies the Clearing Member that the attestation is required, that confirms the existence of an information system cybersecurity program and includes required representations as determined by the Corporation ("Cybersecurity Confirmation").

~~(i)~~(2) Each applicant for clearing membership ~~shall~~must 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 the Corporation notifies the Clearing Member that an attestation is required.~~

(~~b~~c) *Representations in the Cybersecurity Confirmation.* The Cybersecurity Confirmation ~~shall~~must be signed by a senior executive of the Clearing Member or applicant who is authorized to attest to these matters and 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. The Corporation may consider requests to recognize additional best practices and guidelines that are not indicated on the form of Cybersecurity Confirmation.

(3) If using a ~~t~~Third-~~p~~Party ~~s~~Service ~~p~~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~~i) evaluate the cyber risks and impact of these third parties, and (~~B~~ii) 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:

- (A) 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;
- (B) 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;
- (C) 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
- (D) 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) Execution of the Cybersecurity Confirmation. 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.~~

(d) *Occurrence of a Clearing Member System Event* ~~*Security Incident*~~. A Clearing Member experiencing a Clearing Member System Event must notify the Corporation immediately in writing, but no later than two (2) hours, ~~and shall promptly confirm such notice in writing if the~~ after the Clearing Member becomes aware or should be aware that there has been a~~n~~ Clearing Member System Event ~~incident, or a incident is occurring, involving a cyber-related disruption or intrusion of the Clearing Member's system(s) that is reasonably likely to pose an imminent risk or threat to the Corporation's operations~~. ~~Such occurrence~~ A Clearing Member System Event may include, but is not limited to, any disruption or degradation of the normal operation of the Clearing Member's system(s) or any unauthorized entry into the Clearing Member's system(s) that would result in loss of the Corporation's data or system integrity, unauthorized disclosure of sensitive information related to the Corporation, or the inability of the Corporation to conduct essential clearance and settlement functions ~~("Security Incident")~~. Notification pursuant to this section must, at a minimum include the following information, and any such information unconfirmed or otherwise unknown may be identified by the Clearing Member as "Unknown":

(1) *Legal Entities*. A complete list of the legal entity names of the Clearing Member and any Third-Party Service Providers experiencing or otherwise affected or potentially affected by the Clearing Member System Event.

(2) *Contact Information*. A list of persons – with their corresponding titles, primary email addresses and phone numbers, and, if those primary email addresses and phone numbers are associated with the systems that are the subject of the Clearing Member System Event, alternate email addresses and phone numbers – who are authorized to act on behalf of the subject Clearing Member regarding the Clearing Member System Event.

(3) C*learing Member System Event Details*:

- (A) *Event Type* – the type of Clearing Member System Event, for example, an insider threat, phishing attack, MITM attack, privilege escalation, denial of service, external threat, malware, unauthorized access, ransomware, compromised user account, SQL injections, brute force attack, system compromise, supply chain attacks (as each term is commonly understood by cybersecurity professionals in the financial sector), or other – if other, please explain.
- (B) Event Effect - perceived, anticipated, or known effect of the Clearing Member System Event, for example, loss of communication, data corruption, security breach, or other – if other, please explain.
- (C) Start Date – date and time when the Clearing Member System Event began.
- (D) End Date – date and time when the Clearing Member System Event ended, if applicable.
- (E) Discovery Date – date and time when the Clearing Member System Event was first identified.

- (F) Scope – scope of the Clearing Member System Event, including, but not limited to, a list of each affected or likely affected system or data, including the Corporation's Systems and data, the degree of such affect, and any supporting evidence of such.
- (G) Notices – whether any formal or informal notices or information regarding the Clearing Member System Event was made public and, if so, provide a copy of such notices or information.

(e) *Declaration of a Major Clearing Member System Event*.

(1) Upon becoming aware of a Clearing Member System Event, the Corporation will consider whether such Clearing Member System Event meets the definition of a Major Clearing Member System Event. The existence of a Major Clearing Member System Event must be declared by two or more Designated Officers of the Corporation, in their reasonable judgement.

(2) Upon declaration of a Major Clearing Member System Event, the Corporation may act (or refrain from acting) pursuant to this Rule to help address, correct, mitigate or alleviate any and all risks presented to the Corporation by or related to the Major Clearing Member System Event. Action taken will be in consideration of the risks presented to the Corporation, including but not limited to, information provided pursuant to this Rule.

(3) Following declaration of a Major Clearing Member System Event, the Corporation will promptly notify the Chairman of the Board of Directors of such declaration.

(f) *Authority to Take Action and Required Cooperation*.

(1) Upon ~~such~~ notice of a Clearing Member System Event, or if the Corporation has a reasonable basis to believe that a Clearing Member System Event ~~Security Incident~~ has occurred, or is occurring, the Corporation may take actions reasonably necessary to mitigate any effects to its operations, including to:

(A) ~~the right to~~ disconnect access, or to modify the scope and specifications of access, of the Clearing Member to the Corporation's information and ~~data s~~Systems;

(B) suspend any and all transmissions, communications, or access between the Corporation's Systems (together with actions taken under Rule 213(f)(1)(A), "disconnect"); or

(C) take, or refrain from taking, or require the subject Clearing Member to take or refrain from taking, any and all action that the Corporation considers appropriate to help address, correct, mitigate or alleviate the Major Clearing Member System Event and, as appropriate and practical, facilitate the continuation of services, which may include issuing instructions to the subject Clearing Member and requiring such Clearing Member to act on such instructions.

(2) In determining whether to disconnect a Clearing Member, the Corporation will evaluate the facts and circumstances related to the Clearing Member System Event ~~Security Incident~~. The Corporation may take into consideration a number of factors, including, but not limited to, the potential loss of control by a Clearing Member of its internal system(s), the potential loss of the Corporation's confidential data, the potential strain on or loss of the Corporation's resources due to the Corporation's inability to perform clearance and settlement functions, and the overall severity of the threat to the security and operations of the Corporation.

(3) The Corporation will promptly notify the Clearing Member of any disconnect or other material action the Corporation takes with respect to such Clearing Member pursuant to this Rule. Notwithstanding any action taken pursuant to this Rule, ~~If the Corporation determines that disconnection of a Clearing Member is necessary~~, the Clearing Member must continue to meet its obligations to the Corporation, and comply with the statutory rules of the Corporation, as defined in its By-Laws. ~~notwithstanding disconnection from the Corporation's systems~~.

(4) The Clearing Member must cooperate fully and completely with, and to the reasonable satisfaction of, the Corporation in all matters relating to the Major Clearing Member System Event, including, but not limited to:

(A) conducting timely investigations and inquiries, as the Corporation believes reasonably necessary, with respect to any known or unknown information relating to the Clearing Member System Event;

(B) promptly notifying the Corporation of any material changes, updates, or new information learned regarding the Clearing Member System Event; and

(C) promptly providing any documentation or information requested by the Corporation, unless not legally permitted to do so, regarding or related to the Clearing Member System Event.

(~~e~~g) *Procedures for ~~Connecting~~ Reconnection ~~Following a Security Incident that Results in Disconnection~~*.

(1) *Reconnection Attestation*. ~~In the event~~ If the Corporation ~~OCC~~ ~~disconnects~~ takes action pursuant to Rule 213(f)(1) ~~a Clearing Member that has reported a Security Incident, upon the request of the Corporation~~, the Clearing Member must complete and submit a form as provided by the Corporation that describes the Clearing Member System Event ~~Security Incident~~ and includes required representations ("Reconnection Attestation") prior to the Corporation reestablishing connectivity to the Corporation's Systems ("Reconnection"). ~~The Clearing Member also will be required to complete an associated checklist as provided by the Corporation that describes remediation efforts ("Reconnection Checklist").~~ ~~(1) *Representations in the Reconnection Attestation.*~~ The Reconnection Attestation must be signed by a ~~designated~~ senior executive of the Clearing Member who is authorized to attest to the representations required therein, including, but not limited to, the following:

(A) the Clearing Member has provided full, complete and accurate information in response to all requests made by the Corporation regarding the Clearing Member System Event ~~Security Incident~~, including all requests contained in the Reconnection Checklist, on a good faith, best efforts basis;

(B) the Clearing Member has provided full, complete and accurate information regarding any data or systems of the Corporation that were potentially compromised during the Clearing Member System Event ~~Security Incident~~, including any potential exposure of credentials used to access the Corporation's ~~s~~Systems. The Clearing Member will immediately notify the Corporation if it later becomes aware of a previously undetected or unreported compromise of data or systems of the Corporation during the Clearing Member System Event ~~Security Incident~~;

(C) the Clearing Member has determined whether the Clearing Member System Event ~~Security Incident~~ resulted, directly or indirectly, from any controls that failed or were circumvented by its employees, contractors or agents ("Failed Controls"). In a manner approved by the Corporation,

the Clearing Member has communicated Failed Controls to the Corporation and is remediating or has remediated all Failed Controls;

(D) the Clearing Member has implemented, or will implement promptly, technical and operational changes, both preventative and detective, with the intent to prevent a recurrence of the Clearing Member System Event ~~Security Incident~~. The Clearing Member has provided written summaries of such technical and operational changes to the Corporation;

(E) the Clearing Member has complied and will continue to comply with all applicable laws in connection with its response to the Clearing Member System Event ~~Security Incident~~, including any notifications required to be provided to government agencies, the Corporation, and third parties.

(2) *Reconnection Check-List*. If the Corporation takes action pursuant to Rule 213(f)(1), ~~T~~the Clearing Member ~~also will be required to~~ must complete an associated checklist as provided by the Corporation that describes remediation efforts ("Reconnection Checklist"), which may require information including but not limited to:~~.~~

[Text relocated from current Rule 213(e)]

(A) ~~Information Requirements in the Reconnection Checklist. The Reconnection Checklist may require information including, but not limited to, the following:~~ whether the disconnection was the result of a cybersecurity-related incident;

(B) the nature of the incident;

(C) the steps taken to contain the incident;

(D) the data of the Corporation, if any, that was compromised during the incident;

(E) the systems of the Corporation, if any, that were impacted during the incident;

(F) whether there was any risk of exposure of credentials used to access the systems of the Corporation, and if so, whether the credentials were reissued;

(G) the controls that were circumvented or failed that led to the incident occurring; the changes, preventative and detective, that were implemented to prevent a reoccurrence;

(H) details on how data integrity has been preserved and what data checks have been performed;

(I) whether third-parties, including government agencies, have been notified; and

(J) any additional details relevant to R~~r~~econnection.

(3) *Report from Third-Party Cybersecurity Firm*. If the Corporation takes action pursuant to Rule 213(f)(1), the Corporation may require, either as a condition to Reconnection or following Reconnection, that the Clearing Member provide a detailed, comprehensive, and auditable report from a Third-Party Cybersecurity Firm, or summary of such report, that includes:

(A) a timeline of the Clearing Member System Event, including all material actions, events, and decisions taken for or relating to the Clearing Member System Event;

(B) a description of the Clearing Member System Event and an explanation of how such disruption was corrected or resolved;

(C) root cause analysis of the Clearing Member System Event;

(D) confirmation that any issues identified by the Third-Party Cybersecurity Firm as severe, critical, or moderate, or comparable categorizations, have been resolved;

(E) confirmation of normal or intended operation of the subject system(s), including, but not limited to, the return or replacement of key systems and data stores to pre-Clearing Member System Event resilience, in a safe, secure and proper manner for at least 72 hours;

(F) a description of short- and long -term preventive monitoring and detection recommendations form the Third-Party Cybersecurity Firm; and

(G) any other information reasonably requested to be included by the Corporation.

(h) *Reconnection Testing and Approval*.

(1) Prior to any Reconnection pursuant to this Rule, the subject Clearing Member must demonstrate, as applicable, to the Corporation's reasonable satisfaction, that it:

(A) can operate in a test environment, including, but not limited to, sending and receiving messages and transactions;

(B) can replay or resubmit previously submitted messages or transactions;

(C) can reverse or void previously submitted messages or transactions;

(D) can confirm the integrity of messages and transactions;

(E) has alternative communication methods with the Corporation to facilitate the exchange of messages, transactions, and reports; and

(F) can complete any other such requirements as are reasonably requested by the Corporation.

(2) Reconnection of a Clearing Member must be approved by two or more Designated Officers of the Corporation, in their reasonable judgement, after (i) the Corporation has received all required information pursuant to this Rule, in a form and substance satisfactory to the Corporation, and (ii) the requirements of Rule 213(h)(1) have been satisfied, as applicable.

(i) *Certain Miscellaneous Matters*.

(1) Without limiting any other provisions in these Rules concerning limitations on liability, neither the Corporation nor its directors, officers, employees, agents, or contractors shall be liable to any Clearing Member or any customer or client thereof for:

(A) any failure, hindrance, interruption or delay in performance in whole or in part of the obligations of the Corporation under these Rules, if that failure, hindrance, interruption or delay arises out of or relates to a Clearing Member System Event, Major Clearing Member System Event, or any action or inaction pursuant to this Rule 213; or

(B) any loss, liability, damage, cost or expense arising from or relating in any way to any advice, request, requirement, instruction, action or inaction pursuant to this Rule 213.

(2) The power of the Corporation to take any action pursuant to this Rule 213, or to request or require any action, documentation, or information pursuant to this Rule 213, also includes the power to

waive, repeal, rescind, revoke, amend, or vary any such action, request, or requirement in consideration of the facts and circumstances.

(3) The powers of the Corporation pursuant to this Rule 213 are in addition to, and not in limitation of, any authority granted elsewhere in these Rules to act as specified therein.

(4) All information related to or regarding a Major Clearing Member System Event and all acts pursuant to this Rule 213 will be considered Confidential Information pursuant to these Rules; provided, however, that the Corporation may inform, or direct the Clearing Member to inform, the Clearing Member's Third-Party Service Provider of a Clearing Member System Event if the Corporation determines, in its discretion, that such action is necessary for the protection of the Corporation and other Clearing Members.

(5) Failure of a Clearing Member to comply with the requirements of this Rule 213 may subject the Clearing Member to any and all disciplinary action permitted under these Rules, including, without limitation, suspension.

(6) A Clearing Member that has authorized another party, such as a Third-Party Service Provider, to access and use the Corporation's Systems will be responsible for such authorized party's compliance with the requirements of this Rule 213 and any compliance failure by that authorized party will be deemed to be a failure of the authorizing Clearing Member.