



Joseph P. Kamnik
Senior Vice President
and General Counsel

February 22, 2016

VIA ELECTRONIC MAIL

Christopher Kirkpatrick
Secretary of the Commission
Commodity Futures Trading Commission
Three Lafayette Centre
1155 21st Street, N.W.
Washington, DC 20581

Re: RIN 3038-AE29 System Safeguards Testing Requirements for Derivative Clearing Organizations

Dear Mr. Kirkpatrick,

The Options Clearing Corporation (“OCC”) appreciates the opportunity to provide the Commodity Futures Trading Commission (“CFTC” or “Commission”) with its comments on the Commission’s proposed rules governing enhanced amended requirements for derivative clearing organizations (“DCOs”) regarding the testing of system safeguards, including new standards for the testing and assessment of potential risks in automated systems and heightened reporting requirements to the DCO’s Board of Directors (collectively, the “Proposed Rules”).

OCC supports the Commission in its efforts to strengthen cyber defenses by enhancing DCOs’ programs of risk analysis in order to ensure automated systems remain reliable and secure, and continue to have adequate scalable capacity. Generally, we agree with the approach taken by the Commission in the Proposed Rule; however, we offer suggestions regarding how the Commission might: (i) clarify compliance obligations for DCOs in the final rules, (ii) better align final rules with existing or pending obligations imposed by other regulatory bodies on DCOs, and (iii) modify final rules to reduce operational and administrative burdens on DCOs without compromising the Commission’s policy objectives. Our specific comments on the Proposed Rules are discussed in more detail below.

Detailed Comments

I. Final Rules Should Strive to Eliminate Any Conflicting or Redundant Cybersecurity Testing Requirements for DCOs

CFTC Regulation §39.18(j)(1)(i) currently requires a DCO to conduct regular, periodic, and objective testing and review of its automated systems to ensure that they are reliable and secure

and have adequate scalability. This requirement, which forms part of the DCO's risk analysis program required under CFTC Regulation §39.18(b), must be satisfied by, at a minimum, "generally accepted standards and industry best practices."¹ The Proposed Rules would alter this framework by expressly adopting, in certain instances, specific industry standards or best practices as express regulatory requirements.

As the Commission is aware, over the past two years, regulators and other international standard setting organizations have proposed or implemented a multitude of new or enhanced guidelines or standards regarding cybersecurity risk management and controls, testing and evaluation, business continuity planning and disaster recovery, and reporting and disclosure obligations. These new requirements are on top of the various national and international cybersecurity guidelines and standards or industry best practices referenced in the Preamble of the Proposed Rules, *e.g.*, (i) the Federal Financial Institutions Examination Council ("FFIEC"), (ii) National Institute of Standards and Technology ("NIST") publication 800-53, and (iii) the Payment Card Industry Data Security Standard ("PCI-DSS"). While the discussion in the Preamble seemed intended to provide context for the Proposed Rules and serve as informal guidance on how DCOs might demonstrate compliance with final rules in the future, in certain instances the Proposed Rules cherry-picked aspects from these frameworks, turning the guidance and best practices into prescriptive requirements.

We are concerned that systemically important central counterparties ("CCPs") that are subject to multiple regulatory regimes will find themselves in a compliance conundrum, particularly during regulatory exams, if regulators fail to coordinate and align on a common set of guidelines or standards in this space. This risk is highlighted by the fact that, in certain instances, the Commission provides examples from more than one guideline and standard to illustrate potential means of compliance for a specific proposal. For example, the Commission references specific sections from each of the FFIEC, NIST, and PCI-DSS in the context of discussing how DCOs might satisfy certain requirements related to vulnerability testing; specifically, which DCO employees would meet the "independent" standard and which entities are permitted to conduct required external testing.²

The Commission's Proposed Rules risk creating a set of additional controls, separate and apart from other existing regulations, and could inadvertently dilute the effectiveness of those regimes, or worse, create conflicts or inconsistencies with existing regulatory requirements. OCC believes such risks and unintended adverse consequences could be mitigated by continuing to defer to a DCO's risk analysis program for determining the cybersecurity standards or frameworks that align best with the DCO's operations and risk profile. OCC's recommended approach is similar to that which was implemented by the U.S. Securities and Exchange Commission in the adoption of Regulation Systems Compliance and Integrity ("Reg. SCI"), which became effective in November 2015. Under Reg. SCI, OCC and certain other DCOs (collectively, "SCI Entities") were afforded reasonable discretion in designing a compliance plan. Specifically, concurrent with

¹ CFTC Regulation §39.18(d).

² Proposed Rules, pages 17 – 18.

Reg. SCI, the Commission Staff issued guidance on developing policies and procedures consistent with “current SCI industry standards.” The SCI Entities could choose from the current SCI industry standards or from other industry standards so long as those standards met specified requirements that furthered the goals intended by Reg. SCI.³ Thus, SCI Entities already have developed and implemented a comprehensive and robust set of security controls that are tailored to the DCO’s business, risk profile and technology infrastructure.

OCC’s recommended approach provides flexibility to a DCO, which is critical both from the perspective of the evolving nature of cyber threats and the means of response. Moreover, this approach aligns with regulatory obligations that are already in place to further the same policy objectives, eliminating unnecessary costs for DCOs. Finally, because a DCO’s risk analysis program is a regulatory requirement for which the Commission has oversight authority and the DCO would have express compliance obligations uniquely suited for the DCO, the risk of weakness across multiple DCOs with the same requirements is already mitigated. Thus, OCC believes that a DCO’s security would not be compromised through this approach.

To the extent that the Commission believes it is necessary to adopt certain minimum standards in the final rules, OCC strongly recommends regulators and other relevant supervisory bodies strive to implement a common approach that ensures consistent requirements, maximizes budgetary resources allocated to solve these problems, and fully leverages systems capabilities – thereby avoiding fragmented solutions to meet differing regulatory requirements. For CCPs, OCC recommends regulators and other relevant supervisory bodies coalesce around the NIST Framework for Improving Critical Infrastructure Cybersecurity (“NIST Cybersecurity Framework”). Specifically, OCC recommends that the Commission require DCOs to develop an internal “framework” of the relevant collection of policies, procedures and controls addressing cybersecurity risks, based on the NIST Cybersecurity Framework and tailored to the DCOs specific risk profile and environment, taking into account existing legal and governance structure, and, importantly, its overall risk management framework.

II. Standards Respecting Use of Independent Contractors and Testing Frequency

A. Use of Independent Contractors for Testing

The Proposed Rules would require a DCO to engage independent contractors to conduct: (i) external penetration testing at least once annually, (ii) at least two of the required quarterly vulnerability tests, and (iii) testing of key controls at least once annually. The Commission believes that in these instances, an outsider’s perspective may be valuable to identify issues that a DCO employee familiar with the systems may not and to lend credibility to the DCO’s testing overall. As discussed in more detail below, OCC believes that the use of independent contractors as

³ Acceptable SCI Standards included any standard that: (A) comprised of information technology practices that are widely available for free to information technology professionals in the financial sector, and (B) issued by an authoritative body that is a U.S. government entity or agency, association of U.S. governmental entities or agencies, or widely recognized organization. (17 C.F.R. § 240, 242, and 249, 79 FR 72252, 72299).

proposed by the Commission may enhance a DCO's security in some instances, while in other instances the DCO's use of an independent employee would achieve the Commission's objectives without unnecessarily increasing costs or risks to DCOs.

OCC agrees with the Commission's Proposed Rule regarding the use of an independent contractor to perform external penetration testing. As noted in NIST 800-115, "Penetration testing can be invaluable, but it is labor-intensive and requires great expertise to minimize the risk to targeted systems."⁴ External penetration testing requires a level of specific expertise that is often beyond that which the DCO can reasonably provide. Thus, OCC believes this requirement contributes meaningfully to the robustness of a DCO's testing program, and to the extent not already performed in this manner, would enhance the security of the DCO's system without unnecessary cost.

However, OCC believes that requiring a DCO to use an independent contractor to perform vulnerability testing during the same year that such person is performing external penetration testing would unnecessarily increase costs without an added benefit. Specifically, vulnerability testing is largely subsumed within external penetration testing so it is unclear why a DCO should be required to use an independent contractor for both in the same year. Indeed, as the Commission notes in the proposal, "external security testing 'is conducted from outside the organization's security perimeter [,which] offers the ability to view the environment's security posture as it appears outside the security perimeter—usually as seen from the Internet—with the goal of revealing vulnerabilities that could be exploited by an external attacker.'"⁵

A closer look at NIST 800-115 further highlights this redundancy:

- "...penetration testing usually relies on performing both network port/service identification and vulnerability scanning to identify hosts and services that may be targets for future penetration."⁶
- "The use of scanning and penetration techniques can provide valuable information on potential vulnerabilities and predict the likelihood that an adversary or intruder will be able to exploit them."⁷
- "Most penetration tests involve looking for combinations of vulnerabilities on one or more systems that can be used to gain more access than could be achieved through a single vulnerability."⁸

⁴ Id., section 5.2, at 5-2.

⁵ Id., page 19-20, citing NIST SP 800-115, at 2-4.

⁶ NIST SP 800-115, section 2.2, at 2-3.

⁷ Id., section 2.3, at 2-4.

⁸ Id., section 5.2, at 5-2.

- “The discovery phase of penetration testing includes two parts. The first part is the start of actual testing, and covers information gathering and scanning.”... “The second part of the discovery phase is vulnerability analysis, which involves comparing the services, applications, and operating systems of scanned hosts against vulnerability databases (a process that is automatic for vulnerability scanners) and the testers’ own knowledge of vulnerabilities.”⁹

As demonstrated by the foregoing provisions from NIST 800-115, external vulnerability testing is conducted as part of the external penetration testing process. Thus, having an independent contractor conduct external penetration testing and vulnerability testing during the same year, as would be required by Proposed Rules §39.18(e)(3)(ii) and §39.18(e)(2)(i), respectively, results in an independent contractor performing a similar function for two different tests. Accordingly, OCC recommends that the Commission modify the final rules to eliminate the requirement for a DCO to use an independent contractor to perform external vulnerability testing where external penetration testing is performed in the same year, and instead permit DCOs to use independent employees to perform such testing. Adopting OCC’s recommendation would reduce the costs associated with testing without compromising system security or reliability of tests results given the overlap between vulnerability testing and penetration testing discussed above.

Finally, OCC recommends that DCOs be permitted to use independent contractors or independent employees to test and assess the effectiveness of key controls. In contrast to penetration testing, key controls testing does not require specialized expertise. Moreover, independent employees are more knowledgeable about the DCO’s business, risk profile and control environment generally, making them better positioned to perform more effective testing of key controls. At a minimum, the Commission should make clear that whenever an independent contractor is used to perform testing, the independent contractor is not required to work in isolation but rather alongside independent employees of the DCO.

B. Frequency of Testing Requirements for Controls

The Proposed Rules would require DCOs to perform testing of all “safeguards or countermeasures employed by the DCO in order to protect the reliability, security, or capacity of its automated systems or the confidentiality, integrity, or availability of its data and information, in order to enable the DCO to fulfill its statutory and regulatory responsibilities.”¹⁰ The Commission proposes to require controls testing of all controls be conducted no less frequently than every two years.¹¹ We believe the frequency of the controls testing proposed by the Commission is overly burdensome because the costs of conducting such testing far exceeds the benefits in terms of time and resources needed to conduct the testing. To be sure, the sheer number of controls that are tested likely would result in the DCO perpetually testing controls if the rule is adopted as proposed.

⁹ Id., §5.2.1, at 5-3.

¹⁰ Proposed Rules §§39.18(e)(5)(i) and 39.18(a).

¹¹ Id. at §39.18(e)(5)(i).

OCC agrees with the required testing frequency for key controls; however, we believe a better approach to the testing of other controls, and one more aligned with relevant industry best practices, is to permit a DCO to determine the frequency of controls testing based on the level of risk a control is determined to have following an appropriate controls risk analysis. This proposed approach aligns with the approach in the Proposed Rules relating to key controls, under which a DCO must first perform a risk analysis to determine if a control is a “key control” based on the control’s critical importance in safeguarding a system or if it is essential in safeguarding against more frequent threats.¹²

As the Commission knows, not all controls and systems present the same level of risk or are of the same level of importance to a DCO. In fact, a DCO’s risk analysis would find that some controls are of such a low risk, dedicating resources to testing these controls every two years would be uneconomical and provide no improvement in the risk profile of the DCO’s controls infrastructure. Instead, there is a sliding scale applicable to controls that should be accounted for in testing requirements to optimize efficiency in the context of all system safeguard testing requirements.

III. Additional Responses to Specific Provisions

A. Board of Director Reporting and Review

The Commission should amend §39.18(e)(9) to permit the option of having a designated committee of a DCO’s board of directors, as opposed to the full board, fulfill the proposed reporting and review requirements. In its current form, proposed §39.18(e)(9) states that a DCO’s board of directors must “receive and review” reports that include the testing and assessment results required elsewhere in the Proposed Rules. OCC supports the Commission’s policy objective here, which is to ensure that the board of directors is kept informed of cyber risk and plays a leadership role in overseeing a DCO’s efforts to address that risk.¹³ OCC believes, however, that this policy objective can be met by having the reporting and review requirements directed to a qualified board-level committee, so long as there are appropriate mechanisms in place for the committee to keep the full board apprised of its activities and to escalate matters, if necessary.

For example, OCC has established a board-level Technology Committee “to assist the Board in overseeing OCC’s information technology ... strategy, infrastructure, resources and risks, including ... [m]onitoring OCC’s IT risk management efforts and the security of OCC’s information systems and physical security of information systems assets; and [c]onfering with OCC’s senior IT management team and informing the Board on IT related matters.”¹⁴ OCC’s Technology Committee meetings occur at least four times per year, and provide a dedicated forum for board representatives, OCC senior management, and OCC staff to consider and discuss the

¹² Id. at §39.18(a)

¹³ 80 F.R. 80123.

¹⁴ See “The Options Clearing Corporation Technology Committee Charter”, available at:

http://www.theocc.com/components/docs/about/corporate-information/technology_committee_charter.pdf.

types of issues considered in the Proposed Rules. The Technology Committee keeps the full board of directors apprised of its activities by: (i) escalating and informing the full board of matters, as necessary; (ii) regularly disseminating minutes of its meetings; and (iii) providing an annual report. In many respects, having a board-designated committee, such as OCC's Technology Committee, that has specific and dedicated mandates for overseeing cyber risk and the DCO's activities to address those risks, and that allocates dedicated time for considering those issues is more robust than full board review. Therefore, the Commission's final rules should provide this option for DCOs.

B. Two-hour Recovery Time Objective for Cybersecurity Disruptions

Proposed §39.34(a) applies the 2-hour recovery time objective ("2-hour RTO") to "any disruption." Use of the term "any" means that the 2-hour RTO applies to disruptions caused by cybersecurity events, and not just physical security events. OCC agrees that the 2-hour RTO should apply to a physical event because the FMI can turn on backup systems at a geographically dispersed secondary site in order to address a physical event impacting the operation of primary systems.

However, the risks associated with a cybersecurity event can differ from those associated with a physical security event. Whereas a physical security event is likely localized to a particular geographic area, cybersecurity events are not. A cybersecurity event can impact a FMI's primary systems located in one location, as well as secondary systems located in a geographically dispersed location. Thus, failover to a secondary site may not be a readily available option – at least not within a predetermined 2-hour RTO.

The Commission should instead consider a reasonableness standard that permits a DCO to balance the varying risk factors and associated business impacts when remediating a cybersecurity event. Depending on the severity of an incident, or the system impacted, a DCO may be warranted in keeping a system down for more than two hours, particularly if the impacted system does not materially inhibit market facing operations. In other situations, the DCO may have to stop operating for greater than two hours because both primary and secondary systems are impacted and need to be rebuilt.

OCC recognizes the importance of setting and meeting recovery time objectives, and is committed to investing financial and other resources in order to meet reasonable objectives. However, further development and maturity of current industry standards and technological capabilities is needed before the industry can commit to a 2-hour RTO for any and all cybersecurity events. Applying such a rigid standard in the current environment will create an artificial restraint on DCOs and set false expectations for market participants. Therefore, the Commission should remove the 2-hour RTO requirement in favor of a reasonableness standard that accounts for the particular risks and other business considerations associated with cybersecurity events.

C. Definition of Security Incident

Under the Proposed Rules, “security incident” is defined as “a cybersecurity or physical security event that actually or *potentially* jeopardizes automated system operation, reliability, security, or capacity, or the availability, confidentiality or integrity of data.” (emphasis added). Inclusion of the term “potentially” renders this definition vague, and could be interpreted to include most, if not all, cybersecurity events experienced by a DCO. For the reasons that follow, OCC proposes that the Commission revise the definition of “security incident” to either (i) defer to the DCO’s definition as set forth in its risk analysis plan, or (ii) replace “potentially jeopardizes” with “has a significant likelihood of jeopardizing.”

Precedent for OCC’s recommendation exists in the SEC’s Reg. SCI rules, under which SCI Entities evaluate the likelihood of certain cybersecurity incidents impacting applicable systems. This revision would have the added benefit of aligning the CFTC’s requirements for DCOs with a DCO’s requirements under Reg. SCI. Moreover, the Commission defers to a DCO’s definition of security incident as part of the DCO’s security incident response plan.¹⁵ In the context of a DCO’s security incident response plan, a DCO’s definition of security incident is based on the requirements of the cybersecurity controls framework selected by the DCO. Thus, deferring to a DCO definition throughout would ensure the DCO’s policies, procedures, and controls are consistent as part of its compliance program under the final rules.

Alternatively, to create better alignment of the foregoing provisions in the final rules, the Commission could replace “potentially jeopardizes” with “or has a significant likelihood of jeopardizing,” which would provide some additional clarification and incorporate a risk-based approach in managing “security incidents.” Modifying the definition in this manner would better align the term with other aspects of the Proposed Rules. For example, under proposed regulation §39.18(g)(1), Notice of Exceptional Events, DCOs would be required to notify the Commission of any “security incident ... that materially impairs, or creates a *significant likelihood* of material impairment, of automated system operation.” (emphasis added.) The use of the terms “significant likelihood” here implies the DCO has performed an analysis, and has made an informed decision as to the level of risk a particular security incident may pose to an automated system. This revision also provides the added benefit of reducing costs for DCOs and the Commission related to reporting and addressing “exceptional events,” – which would encompass a much broader set of incidents as proposed – and the implementation and oversight of the DCO’s security incident response plan.

As previously mentioned, OCC is concerned that systemically important CCPs that are subject to multiple regulatory regimes will find themselves in a compliance conundrum, particularly during regulatory exams, if regulators fail to coordinate and align on a common set of guidelines or standards. OCC submits that either of the above recommended changes to the definition of “security incident” would eliminate confusion and unnecessary costs and align with the Commission intent across the board.

¹⁵ Proposed Rule §39.18(e)(6)(iii).

Christopher Kirkpatrick
Commodity Futures Trading Commission
February 22, 2016
Page 9

OCC thanks the Commission for the opportunity to provide comment on the Proposed Rules. If you have any questions, please do not hesitate to contact me at 312.322.7570, or JKamnik@theocc.com. We would be pleased to provide the Commission with any additional information or analyses that might be useful in determining the content of the final rules.

Sincerely,



Joseph P. Kamnik