6351-01-P

COMMODITY FUTURES TRADING COMMISSION

17 CFR Part 39

RIN 3038-AE29

System Safeguards Testing Requirements for Derivatives Clearing Organizations

AGENCY: Commodity Futures Trading Commission.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Commodity Futures Trading Commission ("Commission") is proposing enhanced requirements for a derivatives clearing organization's testing of its system safeguards, as well as additional amendments to reorder and renumber certain paragraphs within the regulations and make other minor changes to improve the clarity of the rule text.

DATES: Comments must be received by [**INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER**].

ADDRESSES: You may submit comments, identified by RIN 3038-AE29, by any of the following methods:

- CFTC website: http://comments.cftc.gov. Follow the instructions for submitting comments through the Comments Online process on the website.
- Mail: Send to Christopher Kirkpatrick, Secretary of the Commission, Commodity Futures Trading Commission, Three Lafayette Centre, 1155 21st Street, NW, Washington, DC 20581.
- Hand Delivery/Courier: Same as Mail, above.

- Federal eRulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.

Please submit your comments using only one method. All comments must be submitted in English, or if not, accompanied by an English translation. Comments will be posted as received to http://www.cftc.gov. You should submit only information that you wish to make available publicly. If you wish the Commission to consider information that may be exempt from disclosure under the Freedom of Information Act, a petition for confidential treatment of the exempt information may be submitted under § 145.9 of the Commission's regulations (17 CFR 145.9).

The Commission reserves the right, but shall have no obligation, to review, pre-screen, filter, redact, refuse or remove any or all of your submission from http://www.cftc.gov that it may deem to be inappropriate for publication, such as obscene language. All submissions that have been redacted or removed that contain comments on the merits of the rulemaking will be retained in the public comment file and will be considered as required under the Administrative Procedure Act and other applicable laws, and may be accessible under the Freedom of Information Act.

FOR FURTHER INFORMATION CONTACT: Eileen A. Donovan, Deputy Director, 202-418-5096, edonovan@cftc.gov; M. Laura Astrada, Associate Director, 202-418-7622, lastrada@cftc.gov; or Eileen Chotiner, Senior Compliance Analyst, (202) 418-5467, echotiner@cftc.gov, in each case, at the Division of Clearing and Risk, Commodity Futures Trading Commission, Three Lafayette Centre, 1155 21st Street, NW, Washington, DC 20581; or Julie A. Mohr, Deputy Director, (312) 596-0568, jmohr@cftc.gov; or Joseph Opron, Special Counsel, (312) 596-0653, jopron@cftc.gov, in

each case, at the Division of Clearing and Risk, Commodity Futures Trading Commission, 525 West Monroe Street, Chicago, Illinois 60661.

SUPPLEMENTARY INFORMATION:

I. Background

A. System Safeguards Requirements for DCOs

Section 5b(c)(2) of the Commodity Exchange Act ("CEA")[1] sets forth core principles with which a derivatives clearing organization ("DCO") must comply in order to be registered and to maintain registration with the Commission. In November 2011, the Commission adopted regulations[2] to establish standards for compliance with the core principles, including Core Principle I, which concerns a DCO's system safeguards.[3] In 2013, the Commission adopted additional standards for compliance with the core principles for systemically important DCOs ("SIDCOs") and DCOs that elect to opt-in to the SIDCO regulatory requirements ("Subpart C DCOs").

Regulation 39.18 implements Core Principle I and, among other things, specifies: (1) the requisite elements, standards, and resources of a DCO's program of risk analysis and oversight with respect to its operations and automated systems; (2) the requirements for a DCO's business continuity and disaster recovery plan, emergency procedures, and physical, technological, and personnel resources described therein; (3) the

[1] 7 U.S.C. 7a-1.

[2] Derivatives Clearing Organization General Provisions and Core Principles, 76 FR 69334 (Nov. 8, 2011) (codified at 17 CFR part 39).

[3] Core Principle I requires a DCO to: (1) establish and maintain a program of risk analysis and oversight to identify and minimize sources of operational risk; (2) establish and maintain emergency procedures, backup facilities, and a plan for disaster recovery that allows for the timely recovery and resumption of the DCO's operations and the fulfillment of each of its obligations and responsibilities; and (3) periodically conduct tests to verify that the DCO's backup resources are sufficient.

responsibilities, obligations, and recovery time objective of a DCO following a disruption of its operations; and (4) other system safeguards requirements related to reporting, recordkeeping, testing, and coordination with a DCO's clearing members and service providers. As discussed below, the Commission is proposing clarifications and enhanced requirements for a DCO's testing of its system safeguards, as well as additional amendments to reorder and renumber certain paragraphs and make other minor changes to improve the clarity of the rule text. The Commission is also proposing corresponding technical corrections to § 39.34.

B. Escalating and Evolving Cybersecurity Threats

Recent studies have identified a consistent, growing cybersecurity threat to the financial sector. A survey of 46 global securities exchanges conducted by the International Organization of Securities Commissions ("IOSCO") and the World Federation of Exchanges ("WFE") found that as of July 2013, over half of exchanges worldwide had experienced a cyber attack during the previous year.[4] Indeed, cybersecurity now ranks as the number one concern for nearly half of financial institutions in the United States.[5] Further, the sheer volume of cyber attacks today is remarkable. The annual Pricewaterhouse Coopers Global State of Information Security Survey ("PWC Survey") for 2015, which included 9,700 participants, found that the total number of security incidents detected in 2014 increased by 48% over 2013, for a total of 42.8 million incoming attacks, the equivalent of more than 117,000 attacks per day, every

[4] OICV-IOSCO and WFE, Cyber-crime, securities markets and systemic risk, Staff Working Paper (SWP2/2013), July 16, 2013 ("IOSCO-WFE Staff Report"), p. 3, available at: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD460.pdf.

[5] Depository Trust & Clearing Corporation, Systemic Risk Barometer Study, Q1 2015, p. 1, available at: http://dtcc.com/~/media/Files/pdfs/Systemic-Risk-Report-2015-Q1.pdf.

day.[6] As the PWC Survey pointed out, these numbers do not include undetected attacks. Verizon's 2015 Data Breach Investigations Report noted that during 2014, the financial services sector experienced an average of 350 malware attacks per week.[7]

Concerned about these developments, in March 2015, Commission staff held a Roundtable on Cybersecurity and System Safeguards Testing ("CFTC Roundtable") to, among other things, discuss the issue and identify critical areas of concern.[8] Similarly, a June 2015 Market Risk Advisory Committee ("MRAC") meeting focused on cybersecurity. Commissioner Sharon Bowen, the sponsor of MRAC, noted that cyber attacks on U.S. businesses have been "alarmingly increasing" and stated that "it's critical that the financial industry have strong protections in place."[9]

Experts have identified a number of important topics surrounding cybersecurity that financial institutions should take into consideration. First, the financial sector is facing increasing numbers of more dangerous cyber adversaries, with expanding and worsening motivations and goals.[10] Until recently, most cyber attacks on financial sector institutions were conducted by criminals whose aim was monetary theft or fraud.[11] While such attacks continue, recently there has been a rise in attacks by politically motivated

---

[6] Pricewaterhouse Coopers, Managing Cyber Risks in an Interconnected World: Key Findings from the Global State of Information Security Survey 2015, Sept. 30, 2014, p. 7, available at: www.pwc.com/gsiss2015.

[7] Verizon, 2015 Data Breach Investigations Report, p. 21, available at: http://www.verizonenterprise.com/DBIR/2015/.

[8] See generally CFTC Staff Roundtable on Cybersecurity and System Safeguards Testing, Transcript, Mar. 18, 2015 ("CFTC Roundtable"), pp. 11–91, available at: http://www.cftc.gov/ucm/groups/public/@newsroom/documents/file/transcript031815.pdf.

[9] See Market Risk Advisory Committee Meeting, Transcript, June 2, 2015, p. 6, available at: http://www.cftc.gov/ucm/groups/public/@aboutcftc/documents/file/mrac_060215_transcript.pdf.

[10] CFTC Roundtable, supra note 8, at 22–24.

[11] Id. at 18–24, 42–43.

"hacktivists" or terrorists, and by state-sponsored intruders, aimed at disruption of their targets' operations; theft of data or intellectual property; extortion, cyber espionage, corruption or destruction of data; and degradation or destruction of automated systems.[12] IOSCO and the WFE note that attacks on securities exchanges now tend to be disruptive in nature, which "suggests a shift in motive for cyber-crime in securities markets, away from financial gain and towards more destabilizing aims."[13]

Second, financial institutions face increasing cyber capabilities from both non-state actors and state-sponsored intruders. For example, there has been an increase in sophistication on the part of most actors in the cyber arena, both in terms of technical capability and the capacity to organize and carry out attacks.[14]

Third, the financial sector is experiencing an increase in the duration of cyber attacks.[15] While attacks aimed at monetary theft or fraud tend to manifest themselves quickly, today's more sophisticated attacks may involve cyber adversaries having a presence inside a target's automated systems for an extended period of time, while avoiding detection.[16]

Fourth, financial institutions face a broadening cyber threat field. They must consider cyber vulnerabilities not only with respect to desktop computers and their own

---

[12] Id. at 12, 14–15, 17–24, 42–44, 47.

[13] IOSCO-WFE Staff Report, supra note 4, at 3–4.

[14] Statement of Mr. Michael Daniel, White House Cybersecurity Coordinator, CFTC Roundtable, supra note 8, at 21–23.

[15] Id. at 77, 82–83.

[16] IOSCO and the WFE noted in 2013: "The rise of a relatively new class of cyber-attack is especially troubling. This new class is referred to as an 'Advanced Persistent Threat' (APT). . . . [APTs] are usually directed at business and political targets for political ends. APTs involve stealth to persistently infiltrate a system over a long period of time, without the system displaying any unusual symptoms." IOSCO-WFE Staff Report, supra note 4, at 3.

automated systems, but also with respect to mobile devices and data in the cloud.[17] Further, adequate risk analysis must address not just the vulnerabilities of the entity's automated systems, but also the human vulnerabilities posed by social engineering[18] or disgruntled employees.[19] Notably, today's cyber threat environment also includes automated systems that are not directly internet-facing.[20] For example, internet-facing corporate information technology and non-internet-facing operations technology can be, and often are, connected for maintenance purposes or in error.[21] Non-internet-facing systems are also vulnerable to insertion of malware-infected removable media, phishing attacks, and other social engineering techniques, and to supply-chain risk involving both hardware and software.[22]

Finally, financial institutions cannot achieve cyber resilience by addressing threats to themselves alone: they also face threats due to the increasing interconnectedness of financial services firms.[23] As such, a financial entity's risk assessments need to consider cybersecurity across the breadth of the financial sector, from exchanges and clearing

---

[17] CFTC Roundtable, supra note 8, at 22.

[18] "In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repairperson, or researcher and even offering credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility." See U.S. Computer Emergency Readiness Team, Dep't of Homeland Sec., Security Tip (ST04-014), Avoiding Social Engineering and Phishing Attacks, available at: https://www.us-cert.gov/ncas/tips/ST04-014 (last visited Sept. 14, 2015).

[19] CFTC Roundtable, supra note 8, at 14, 79–80.

[20] Id. at 60–70.

[21] Id. at 73.

[22] Id. at 62–66, 77–79.

[23] Id. at 25–26.

organizations to counterparties and customers, technology providers, other third party service providers, and the businesses and products in the entity's supply chain.[24]

C. Need for Cybersecurity Testing

In the current environment, cybersecurity testing is crucial to efforts by exchanges, clearing organizations, swap data repositories, and other entities in the financial sector to strengthen cyber defenses; mitigate operational, reputational, and financial risk; and maintain cyber resilience and the ability to recover from cyber attacks. To maintain the effectiveness of cybersecurity controls, such entities must regularly test their system safeguards in order to find and fix vulnerabilities before an attacker exploits them.

An entity's testing should be informed by how its controls and countermeasures stack up against the techniques, tactics, and procedures used by its potential attackers.[25] Adequate testing needs to include periodic risk assessments made in light of changing business conditions, the changing threat landscape, and changes to automated systems. It also needs to include recurring tests of controls and automated system components to verify their effectiveness and operability, as well as continuous monitoring and scanning of system operation and vulnerabilities. Testing should include a focus on the entity's ability to detect, contain, respond to, and recover from cyber attacks within its systems, not just on its defenses designed to prevent intrusions.[26] This should include detection, containment, and recovery from compromise of data integrity—perhaps the greatest threat with respect to financial sector data—in addition to addressing compromise of data

[24] Id. at 48–57.

[25] Id. at 45–46.

[26] Id. at 80–84.

availability or confidentiality, which tend to be the main focus of many best practices.[27] Finally, both internal testing by the entity itself and independent testing by third party service providers are essential components of an adequate testing regime.[28]

Cybersecurity testing is a well-established best practice generally and for financial sector entities. The Federal Information Security Management Act ("FISMA"), which is a source of cybersecurity best practices and also establishes legal requirements for federal government agencies, calls for "periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually . . . ."[29] The National Institute of Standards and Technology ("NIST") Framework for Improving Critical Infrastructure Cybersecurity calls for testing of cybersecurity response and recovery plans and cybersecurity detection processes and procedures.[30] The Financial Industry Regulatory Authority ("FINRA") 2015 Report on Cybersecurity Practices notes that "[r]isk assessments serve as foundational tools for firms to understand the cybersecurity risks they face across the range of the firm's activities and assets," and calls for firms to develop, implement, and test cybersecurity incident response plans.[31] FINRA notes that one common deficiency with respect to cybersecurity is "failure to conduct adequate

[27] Id. at 15–16, 65, 71–74, 82–83.

[28] Id. at 89–90, 101–108, 167–168, 172–173, 244–253.

[29] 44 U.S.C. 3544(b)(5).

[30] NIST, Framework for Improving Critical Infrastructure Cybersecurity, Feb. 2014, v.1, Subcategory PR.IP-10, p. 28, and Category DE.DP, p. 31, available at: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[31] FINRA, Report on Cybersecurity Practices, Feb. 2015 ("FINRA Report"), pp. 1–2, available at: https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf.

periodic cybersecurity assessments."[32] The Council on Cybersecurity's Critical Security Controls for Effective Cyber Defense (the "Controls") call for entities to "[c]ontinuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers."[33] The Controls further state that "[o]rganizations that do not scan for vulnerabilities and proactively address discovered flaws face a significant likelihood of having their computer systems compromised."[34] The Controls also call for entities to "[t]est the overall strength of an organization's defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker."[35] The Controls recommend conducting "regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully," from both outside and inside the boundaries of the organization's network perimeter,[36] and also call for use of vulnerability scanning and penetration testing in concert.[37]

The Federal Financial Institutions Examination Council ("FFIEC"),[38] another important source of cybersecurity best practices for financial sector entities, summarized the need for cybersecurity testing in today's cyber threat environment:

---

[32] Id. at 8.

[33] Council on Cybersecurity, The Critical Security Controls for Effective Cyber Defense, v. 5.1 ("Council on Cybersecurity"), p. 28, available at: http://www.counciloncybersecurity.org/bcms-media/Files/Download?id=a52977d7-a0e7-462e-a4c0-a3bd01512144.

[34] Id.

[35] Id. at 102.

[36] Id.

[37] Id. at 103.

[38] The FFIEC includes the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, the Consumer Financial Protection Bureau, the National Credit Union Administration, and the State Liaison Committee of the Conference of State Bank Supervision.

> Financial institutions should have a testing plan that identifies control objectives; schedules tests of the controls used to meet those objectives; ensures prompt corrective action where deficiencies are identified; and provides independent assurance for compliance with security policies. Security tests are necessary to identify control deficiencies. An effective testing plan identifies the key controls, then tests those controls at a frequency based on the risk that the control is not functioning. Security testing should include independent tests conducted by personnel without direct responsibility for security administration. Adverse test results indicate a control is not functioning and cannot be relied upon. Follow-up can include correction of the specific control, as well as a search for, and correction of, a root cause. Types of tests include audits, security assessments, vulnerability scans, and penetration tests.[39]

Some experts further note that cybersecurity testing may become a requirement for obtaining cyber insurance. Under such an approach, insurance coverage might be conditioned on cybersecurity testing and assessment, followed by implementation of appropriate prevention and detection procedures.[40]

Cybersecurity testing is also supported internationally. IOSCO has emphasized the importance of testing to ensure effective controls, in light of risks posed by the complexity of markets caused by technological advances.[41] According to IOSCO, "regulatory authorities have also recognized the need for [t]rading [v]enues to appropriately monitor critical systems and have appropriate control mechanisms in place."[42] Similarly, the European Securities and Markets Authority ("ESMA") guidelines for automated trading systems call for trading platforms to test trading systems and

---

[39] See FFIEC, E-Banking Booklet: IT Examination Handbook, Aug. 2003, p. 30, available at: http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_E-Banking.pdf.

[40] See PricewaterhouseCoopers, Insurance 2020 and Beyond: Reaping the Dividends of Cyber Resilience, 2015, available at: http://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf.

[41] IOSCO Consultation Report, Mechanisms for Trading Venues to Effectively Manage Electronic Trading Risks and Plans for Business Continuity, Apr. 2015, p. 3, available at: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD483.pdf.

[42] Id. at 9.

system updates to ensure that systems meet regulatory requirements, that risk management controls work as intended, and that the systems can function effectively in stressed market conditions.[43] Further, the Principles for Financial Market Infrastructures published by the Bank for International Settlements' Committee on Payments and Market Infrastructures ("CPMI") and IOSCO's Technical Committee (together, "CPMI-IOSCO") note that with respect to operational risks, which include cyber risk, "[a financial market infrastructure]'s arrangements with participants, operational policies, and operational procedures should be periodically, and whenever necessary, tested and reviewed, especially after significant changes occur to the system or a major incident occurs . . . ."[44] The Commission also notes that § 39.18(j)(1)(i) currently requires DCOs to conduct regular, periodic, and objective testing and review of their automated systems to ensure that these systems are reliable, secure, and have adequate scalable capacity. Finally, the Commission notes that this requirement must be satisfied by following, at a minimum, generally accepted standards and industry best practices.[45] As further explained below, the proposed rules would clarify existing system safeguards requirements by identifying relevant generally accepted standards and industry best practices. With few exceptions, such as requirements for independent contractors to conduct certain testing, the Commission is not changing the regulatory requirement for DCOs as it exists today.

---

[43] ESMA, Guidelines: Systems and controls in an automated trading environment for trading platforms, investment firms and competent authorities, Feb. 24, 2012, p. 7, available at: http://www.esma.europa.eu/system/files/esma_2012_122_en.pdf.

[44] CPMI-IOSCO, Principles for Financial Market Infrastructures, Apr. 2012, at 96, available at: http://www.iosco.org/library/pubdocs/pdf/IOSCOPD377.pdf. See also CPMI, Cyber resilience in financial market infrastructures, Nov. 2014, available at: http://www.bis.org/cpmi/publ/d122.pdf.

[45] For a more detailed discussion of current testing requirements for DCOs, please see the System Safeguards Requirements for DCOs in section I.A. above and the Consideration of Costs and Benefits in section IV.C. below.

II. Proposed Amendments

A. Enhanced Testing Requirements

As discussed above, § 39.18 requires a DCO to establish and maintain a program of risk analysis and oversight with respect to its operations and automated systems. As part of this program, a DCO is required to conduct regular, periodic, and objective testing and review of its automated systems to ensure that they are reliable, secure, and have adequate scalable capacity. DCOs are specifically required, under § 39.18(d), to follow "generally accepted standards and industry best practices with respect to the development, operation, reliability, security, and capacity of automated systems" in addressing the categories of risk analysis and oversight specified in § 39.18. As discussed in the Commission's proposing release for § 39.18, "DCO compliance with generally accepted standards and best practices with respect to the development, operation, reliability, security, and capacity of automated systems can reduce the frequency and severity of automated system security breaches or functional failures, thereby augmenting efforts to mitigate systemic risk."[46] This requirement was further designed to allow DCOs flexibility in adapting their programs to current industry best practices, which the Commission recognized would evolve over time. Similarly, the additional testing provisions that the Commission is proposing have been constructed to set forth certain minimum requirements, with the expectation that DCOs' testing may change as accepted standards and industry best practices develop over time and are reflected in the DCO's risk analysis.

[46] See Risk Management Requirements for Derivatives Clearing Organizations, 76 FR 3698, 3713 (Jan. 20, 2011).

Specifically, the Commission is proposing to strengthen the current system safeguards regulatory framework by specifying five fundamental types of systems testing and assessment that are required under § 39.18. The Commission is proposing to require that these types of testing and assessment be conducted at a frequency determined by an appropriate risk analysis, but no less frequently than a proposed minimum, which varies based on the particular type of testing or assessment. To strengthen the objectivity and reliability of the testing, assessment, and information available to the Commission in this regard, the Commission is proposing to require that independent contractors perform a significant portion of the testing and assessment. In developing these requirements, the Commission has relied on various industry standards and best practices for assessment of information security systems, which are referenced in the following discussion. The Commission has not proposed a definition of the term "independent contractor." Proposed definitions of terms related to the proposed testing requirements are discussed in the respective section setting forth each proposed testing requirement.

1. Vulnerability Testing

Identification of cyber and automated system vulnerabilities is a critical component of a DCO's ongoing assessment of risks to its systems. NIST standards call for organizations to scan for automated system vulnerabilities both on a regular and ongoing basis, and when new vulnerabilities potentially affecting their systems are identified and reported.[47] NIST adds that organizations should employ vulnerability scanning tools and techniques that automate parts of the vulnerability management

[47] NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, rev. 4 ("NIST SP 800-53"), Control RA-5, available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

process.[48] NIST also calls for the organization to remediate vulnerabilities identified by vulnerability testing, in accordance with its assessments of risk.[49] Similarly, the Controls recommend that organizations "continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers."[50]

The proposed minimum standards and frequencies for vulnerability testing are intended to strengthen a DCO's systems oversight program. Accordingly, in § 39.18(a) the Commission is proposing to define "vulnerability testing" as the testing of a DCO's automated systems to determine what information may be discoverable through a reconnaissance analysis of those systems and what vulnerabilities may be present on those systems. This definition is consistent with NIST standards for such testing.[51] For purposes of this definition, the term "reconnaissance analysis" is used to combine various aspects of vulnerability testing.[52] The proposed definition deliberately refers broadly to vulnerability testing in order to avoid prescribing use of any particular technology or

[48] Id.

[49] Id.

[50] Council on Cybersecurity, supra note 33, at 28.

[51] See NIST SP 800-53, supra note 47, at F-153.

[52] See, e.g., NIST Special Publication 800-115, Technical Guide to Information Security Testing and Assessment, Sept. 2008 ("NIST SP 800-115"), p. 24, available at: http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf (noting that "[e]xternal testing often begins with reconnaissance techniques that search public registration data, Domain Name System (DNS) server information, newsgroup postings, and other publicly available information to collect information (e.g., system names, Internet Protocol [IP] addresses, operating systems, technical points of contact) that may help the assessor to identify vulnerabilities").

tools, because vulnerability assessments may not always be automated, and technology may change.[53]

Proposed § 39.18(e)(2) would also require that vulnerability testing include automated vulnerability scanning, as well as an analysis of the test results to identify and prioritize all identified vulnerabilities that require remediation.[54] Moreover, the Commission recognizes that automated scans may be authenticated (i.e., conducted using usernames or passwords) or unauthenticated (i.e., conducted without using usernames or passwords). However, the Commission proposes requiring that, where indicated by appropriate risk analysis, a DCO conduct such scanning on an authenticated basis.[55] Where scanning is conducted on an unauthenticated basis, a DCO would be required to implement effective compensating controls.[56]

---

[53] See SANS Institute, Penetration Testing: Assessing Your Overall Security Before Attackers Do, p. 7, available at: https://www.sans.org/reading-room/whitepapers/analyst/penetration-testing-assessing-security-attackers-34635 (last visited Sept. 30, 2015) (noting, "A wide variety of tools may be used in penetration testing. These tools are of two main types; reconnaissance or vulnerability testing tools and exploitation tools. While penetration testing is more directly tied to the exploitation tools, the initial scanning and reconnaissance is often done using less intrusive tools.").

[54] See Security Standards Council, Payment Card Industry Data Security Standards, Apr. 2015, v. 3.1 ("PCI-DSS"), p. 94, available at: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf (defining a vulnerability scan as "a combination of automated or manual tools, techniques, and/or methods run against external and internal network devices and servers, designed to expose potential vulnerabilities that could be found and exploited by malicious individuals"). See also NIST SP 800-115, supra note 52, at 2-2 (noting that testing techniques that include vulnerability scanning "can identify systems, ports, services, and potential vulnerabilities, and may be performed manually but are generally performed using automated tools").

[55] See Securities Standards Council, The PCI Monitor: Weekly news, updates and insights from PCI SSC, June 25, 2014, available at: http://training.pcisecuritystandards.org/the-pci-monitor-weekly-news-updates-and-insights-from-pci-ssc2?ecid=ACsprvuuirRbrU3vDlk76s_ngGKJKEYlvaBJzvvUMldZv4KKh6V1guIKOR5VLTNfAqPQ_Gmox3zO&utm_campaign=Monitor&utm_source=hs_email&utm_medium=email&utm_content=13292865&_hsenc=p2ANqtz-_LIkkHURyUmyq1p2OxB39R5nOpRh1XHE_jW6wCC6EEUAow15E7AuExcIGwdYxyh_6YNxVvKorcurk6r90E3d7dG71fbw&_hsmi=13292865#web.

[56] See PCI-DSS, supra note 54, app. B at 112 ("Compensating controls may be considered . . . when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business

Furthermore, the Commission is proposing to require DCOs to conduct vulnerability testing at a frequency determined by an appropriate risk analysis, but no less frequently than quarterly.[57] The Commission notes that while "[t]he frequency of testing should be determined by the institution's risk assessment,"[58] best practices call for risk assessments to include consideration of a number of important factors, including, for example, the frequency and extent of changes in the organization's automated systems and operating environment; the potential impact if risks revealed by testing are not addressed appropriately; the degree to which the relevant threat environment or potential attacker profiles and techniques are changing; and the results of other testing.[59] Frequency appropriate to risk analysis can also vary depending on the type of monitoring involved; for example, with whether automated monitoring or procedural testing is being conducted.[60] Nonetheless, the Commission notes that the PCI-DSS standards provide that entities should run internal and external network vulnerability scans "at least quarterly," as well as after any significant network changes, new system component installations, firewall modifications, or product upgrades.[61] Because best practices call for vulnerability testing at a frequency determined by an appropriate risk analysis, and

---

constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other, or compensating, controls.").

[57] See FFIEC, Information Security Booklet, IT Examination Handbook, July 2006 ("FFIEC Handbook"), p. 82, available at: http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_InformationSecurity.pdf (noting that "firewall policies and other policies addressing access control between the financial institution's network and other networks should be audited and verified at least quarterly").

[58] Id.

[59] See NIST Special Publication 800-39, Managing Information Security Risk, Mar. 2011 ("NIST SP 800-39"), pp. 47–48, available at: http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf; see also FFIEC Handbook, supra note 57, at 82.

[60] Id.

[61] See Requirement 11.2, PCI-DSS, supra note 54, at 94.

call for such testing to be conducted no less than quarterly, this proposed rule does not impose new requirements on DCOs. Rather, it is designed to give additional clarity to DCOs concerning what is currently required under existing regulations. In light of these best practices and the current level of cyber threat to the financial sector discussed above, the Commission believes that this proposed rule is appropriate in today's cybersecurity environment. For the same reasons, and because the Commission understands that DCOs currently conduct vulnerability testing on at least a quarterly basis and in many cases more frequently, the Commission also believes that this minimum frequency requirement for vulnerability testing will impose only de minimis additional costs, if any, on DCOs.

In addition, the proposed rule would require DCOs to engage independent contractors to conduct two of the required quarterly vulnerability tests each year, while permitting DCOs to conduct other vulnerability testing using employees who are not responsible for development or operation of the systems or capabilities being tested. The Commission believes that important benefits are provided when a testing program includes both testing by independent contractors and testing by entity employees not responsible for building or operating the system being tested. While testing needs to be performed internally, it also needs to be conducted from the viewpoint of an outsider, particularly where testing against the possible tactics or techniques of a particular threat actor is concerned. [62] For example, entity employees can use viewpoints that the outside world would not have, based on intimate knowledge of the entity.[63] Conversely, independent contractors provide an outsider's perspective, and may search for

[62] See generally CFTC Roundtable, supra note 8, at 89–90.

[63] Id. at 178.

vulnerabilities in a system that entity employees may not have contemplated during the design or operation of the system involved.[64]

The Commission also notes that best practices support having testing conducted by both independent contractors and entity employees. Regarding the benefits provided by independent contractor testing, NIST notes that engaging third parties (e.g., auditors, contractor support staff) to conduct the assessment offers an independent view and approach that internal assessors may not be able to provide. Organizations may also use third parties to provide specific subject matter expertise that is not available internally.[65] FFIEC states that testing by independent contractors provides credibility to test results.[66] Acknowledging the use of entity employees to conduct testing, FFIEC calls for such tests to be performed "by individuals who are also independent of the design, installation, maintenance, and operation of the tested system."[67] Similarly, with respect to system safeguards testing by internal auditors, FFIEC further states that the auditors should have both independence and authority from the Board of Directors to access all records and staff necessary for their audits, and that auditors should not participate in activities that may compromise or appear to compromise their independence.[68] Further, the data security standards of the Payment Card Industry Security Standards Council call for

[64] Id. at 172–173.

[65] NIST SP 800-115, supra note 52, at 6-6. NIST also notes that giving outsiders access to an organization's systems can introduce additional risk, and recommends proper vetting and attention to contractual responsibility in this regard.

[66] FFIEC Handbook, supra note 57, at 81.

[67] Id.

[68] FFIEC, Audit Booklet: IT Examination Handbook, Apr. 2012, p.6, available at: http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_Audit.pdf.

conducting both internal and external vulnerability scans, with external scans performed by an approved vendor.[69]

Accordingly, following consideration of the recommendations set forth in the standards mentioned above, the Commission believes that requiring two of the four tests to be conducted by independent contractors is a balanced approach. Other vulnerability tests may be performed by employees of the DCO who are not responsible for development or operation of the systems or capabilities being tested. In light of the best practices and the current level of cyber threat to the financial sector discussed above, the Commission believes that the proposed rule provisions regarding vulnerability testing by independent contractors are appropriate in today's cybersecurity environment.

2. Penetration Testing

Though complementary to vulnerability testing, penetration testing differs from vulnerability testing in that its purpose is to identify ways that the vulnerabilities identified above could be exploited.[70] In other words, penetration testing attempts to exploit cyber and automated system vulnerabilities, and subjects the system to real-world attacks by testing personnel in order to identify both the extent to which an attacker could compromise the system before the organization detects and counters the attack, and the effectiveness of the organization's response mechanisms.[71]

NIST defines penetration testing as "[a] test methodology in which assessors, typically working under specific constraints, attempt to circumvent or

---

[69] See Requirement 11, PCI-DSS, supra note 54, at 94–96.

[70] See Security Standards Council, PCI-DSS Information Supplement: Penetration Testing Guidance, Mar. 2015 ("PCI-DSS Penetration Testing"), p. 3, available at: https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf.

[71] See FFIEC Handbook, supra note 57, at 81.

defeat the security features of an information system."[72] As noted in the FINRA Report, "[a]n advanced persistent attack may involve an outsider gaining a progressively greater foothold in a firm's environment, effectively becoming an insider in the process. For this reason, it is important to perform penetration testing against both external and internal interfaces and systems."[73] As further explained, 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."[74] Internal penetration testing, on the other hand, is conducted "from the internal network and [assessors] assume the identity of a trusted insider or an attacker who has penetrated the perimeter defenses."[75] Internal penetration testing can therefore reveal vulnerabilities that could be exploited, and demonstrates the potential damage this type of attacker could cause.[76]

In addition, generally accepted standards and industry best practices support annual penetration testing. For example, NIST calls for at least annual penetration testing of an organization's network and systems.[77] Moreover, the FFIEC calls for independent

---

[72] NIST SP 800-53, supra note 47, app. B at B-16.

[73] FINRA Report, supra note 31, at 22.

[74] NIST SP 800-115, supra note 52, at 2-4.

[75] Id. at 2-5. See also, e.g., SANS, Penetration Testing in the Financial Services Industry, 2010, p. 17, available at: https://www.sans.org/reading-room/whitepapers/testing/penetration-testing-financial-services-industry-33314 ("Penetration testing is essential given the context of high operational risk in the financial services industry.").

[76] See NIST SP 800-115, supra note 52, at 2-5.

[77] Id. at 5-6.

penetration testing of high risk systems at least annually, and for quarterly testing and verification of the efficacy of firewall and access control defenses.[78] Data security standards for the payment card industry provide that entities should perform both external and internal penetration testing at least annually, as well as after any significant network changes, new system component installations, firewall modifications, or product upgrades.[79]

The primary benefit of a penetration test is that it identifies the extent to which a system can be compromised before the attack is identified and assesses the effectiveness of the response mechanism.[80] Accordingly, the Commission is proposing to require both external and internal penetration testing. In § 39.18(a), the Commission proposes to define "external penetration testing" as attempts to penetrate a DCO's automated systems or networks from outside the system and network boundaries to identify and exploit vulnerabilities (including, but not limited to, methods for circumventing the security features of an application, system, or network).[81] Proposed § 39.18(e)(3) would require external penetration testing to be conducted at a frequency determined by an appropriate risk analysis, but no less frequently than annually.[82] The Commission proposes to define

---

[78] FFIEC Handbook, supra note 57, at 82.

[79] See Requirements 11.3.1 and 11.3.2, PCI-DSS, supra note 54.

[80] FFIEC Handbook, supra note 57, at 81.

[81] See NIST SP 800-53, supra note 47, app. B at B-16 (defining "penetration testing" as "[a] test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system"); see also NIST Special Publication 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations, Sept. 2011 ("NIST SP 800-137"), app. B, p. B-10, available at: http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf.

[82] See PCI-DSS Penetration Testing, supra note 70, at 8 (noting that "[p]enetration testing should be performed at least annually and after any significant change—for example, infrastructure or application upgrade or modification—or new system component installations").

"internal penetration testing" in § 39.18(a) as attempts to penetrate a DCO's automated systems or networks from inside the system and network boundaries to identify and exploit vulnerabilities (including, but not limited to, methods for circumventing the security features of an application, system, or network).[83] In § 39.18(e)(4), the Commission also proposes to require that internal penetration testing be conducted at a frequency determined by an appropriate risk analysis, but no less frequently than annually.

As discussed above, the Commission notes that generally accepted standards and industry best practices require annual penetration testing. Moreover, DCOs currently are required to follow generally accepted standards and industry best practices, which support a minimum frequency of annually for internal penetration testing, and as discussed in more detail in the Cost-Benefit Analysis in Section IV.C. below, DCOs are conducting penetration testing on at least an annual basis. However, the Commission acknowledges that Securities and Exchange Commission ("SEC") Regulation SCI, which is applicable to DCOs that are registered with the SEC as clearing agencies,[84] requires that penetration testing be conducted every three years.[85] Nonetheless, given the importance of DCOs to the U.S. financial system, the Commission believes that annual

[83] Id. at 2.

[84] Of the 15 DCOs currently registered with the Commission, four also are registered with the SEC as clearing agencies: Chicago Mercantile Exchange, Inc. ("CME"), ICE Clear Credit LLC, ICE Clear Europe Limited, and Options Clearing Corporation. However, on August 3, 2015, CME filed with the SEC a written request to withdraw from registration as a clearing agency. See Securities Exchange Act Release No. 34-75762 (Aug. 26, 2015), 80 FR 52815 (Sept. 1, 2015).

[85] 17 CFR 240.1003. The SEC noted in its adopting release that "SCI entities may, however, determine that based on its [sic] risk assessment, it is appropriate and/or necessary to conduct such penetration test reviews more frequently than once every three years." Regulation Systems Compliance and Integrity, 79 FR 72252, 72344 (Dec. 5, 2014).

internal penetration testing is appropriate in order to sufficiently address risks to a DCO's systems.

In addition, and consistent with generally accepted standards and industry best practices, proposed § 39.18(e)(3) would require DCOs to engage independent contractors to perform the required annual external penetration tests. Independent testing provides for impartiality, meaning that penetration testers are free from conflicts of interest with respect to the development, operation, or management of the system(s) that are the targets of the testing.[86] The Commission believes that the impartiality provided by independent contractors, including their lack of a stake in the outcome, is an important factor in conducting external penetration testing and enhances the credibility of the test results.[87] Proposed § 39.18(e)(4) would, however, permit internal penetration testing to be conducted by either independent contractors or employees of the DCO who are not responsible for development or operation of the systems or capabilities being tested.[88]

3. Controls Testing

Controls provide reasonable assurance that security management is effective, and adequate control testing is therefore critical to ensuring the confidentiality, integrity, and availability of information and information systems.[89] Regular, ongoing testing of all of

[86] NIST SP 800-53, supra note 47, app. F-CA at F-62.

[87] FFIEC Handbook, supra note 57, at 81 (noting that "[i]ndependence provides credibility to the test results").

[88] See, e.g., PCI-DSS, supra note 54, at 97.

[89] See generally U.S. Gov't Accountability Office, GAO-09-232G, Federal Information System Controls Audit Manual, Feb. 2009, available at: http://www.gao.gov/assets/80/77142.pdf.

an organization's system safeguards-related controls for these purposes is a crucial part of a DCO's risk analysis and oversight program.[90]

Generally accepted standards and industry best practices call for organizations to conduct regular, ongoing controls testing that over time includes testing of all their system safeguards-related controls. For example, NIST calls for organizations to assess "the security controls in the information system and its environment of operation to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements."[91] NIST notes that the results of such testing can allow organizations to, among other things, identify potential cybersecurity problems or shortfalls, identify security-related weaknesses and deficiencies, prioritize risk mitigation decisions and activities, confirm that weaknesses and deficiencies have been addressed, and inform related budgetary decisions and capital investment.[92] FFIEC calls for controls testing because "[c]ontrols should not be assumed to be completely effective," and states that a controls testing program "is sound industry practice and should be based on an assessment of the risk of non-compliance or circumvention of the institution's controls."[93]

Consistent with industry best practices, the Commission proposes to define "controls testing" in § 39.18(a) as an assessment of a DCO's controls to determine

---

[90] See generally 17 CFR 39.18 and 17 CFR 39.34.

[91] NIST SP 800-53, supra note 47, app. F-CA at F-55.

[92] NIST Special Publication 800-53A, Assessing Security and Privacy Controls in Federal Information Systems and Organizations, rev. 4 ("NIST SP 800-53A"), p. 3, available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf.

[93] FFIEC Handbook, supra note 57, at 12.

whether such controls are implemented correctly, are operating as intended, and are enabling the DCO to meet the system safeguards requirements set forth in § 39.18.[94] Furthermore, the Commission proposes to define "controls" as the safeguards or countermeasures[95] 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. Regulation 39.18(a) would also define "key controls" as those controls that an appropriate risk analysis determines are either critically important for effective system safeguards or intended to address risks that evolve or change more frequently and therefore require more frequent review to ensure their continuing effectiveness in addressing such risks. In today's cybersecurity threat environment, the Commission believes that effective testing of this subset of the system safeguards controls maintained by a DCO is particularly important.

In addition, the Commission is proposing to require controls testing in § 39.18(e)(5), which would include testing of each control included in the DCO's risk analysis and oversight program, to be conducted at a frequency indicated by an appropriate risk analysis, but no less frequently than every two years. The Commission believes that this would ensure that each such control is tested with sufficient frequency to confirm the continuing adequacy of the DCO's system safeguards. The Commission recognizes, however, that appropriate risk analysis may well determine that more

---

[94] See generally NIST SP 800-53A, supra note 92.

[95] NIST SP 800-53, supra note 47, app. B at B-5 (defining "countermeasures" as "[a]ctions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards").

frequent testing of either certain key controls or all controls is necessary. The Commission notes that industry best practices support information security continuous monitoring ("ISCM"), which is defined as "maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions."[96] Nonetheless, recognizing that it is impractical to test every security control at all times, these standards note that "[t]he frequency of assessments should be sufficient to assure adequate security commensurate with risk, as determined by system categorization and ISCM strategy requirements."[97] Thus, consistent with industry best practices, the Commission is proposing minimum frequency for the testing of each control of no less than every two years.

The Commission also proposes to permit such testing to be conducted on a rolling basis over the course of the period determined by appropriate risk analysis in recognition of the fact that an adequate system safeguards program for a DCO must necessarily include large numbers of controls, and therefore it could be impracticable and unduly burdensome to require testing of all controls in a single test. This provision is designed to give a DCO flexibility concerning how and when to test controls during the applicable minimum period, and is intended to reduce burdens associated with testing every control to the extent possible while still safeguarding and managing the DCO's security.[98]

The proposed rule would also require testing of key controls to be conducted by independent contractors. As noted above, the Commission believes that the impartiality and credibility provided by independent testing supports the proposed requirement that

[96] NIST SP 800-137, supra note 81, at vi.

[97] Id. at 11.

[98] Id. at 25–27.

testing of key controls be done by independent contractors. However, the Commission is proposing to give DCOs the discretion to test other controls using either independent contractors or employees of the DCO who are independent of the systems being tested.[99]

4. Security Incident Response Plan Testing

The Commission recognizes that adequate cyber resilience requires organizations to have sufficient capacity to detect, contain, eliminate, and recover from a cyber intrusion, and believes that security incident response plans,[100] and testing of those plans, are essential to such capabilities.

NIST urges organizations to have a security incident response plan that "establishes procedures to address cyber attacks against an organization's information systems. These procedures are designed to enable security personnel to identify, mitigate, and recover from malicious computer incidents, such as unauthorized access to a system or data, denial of service, or unauthorized changes to system hardware, software, or data (e.g., malicious logic, such as a virus, worm, or Trojan horse)."[101]

---

[99] See discussion supra section II.A.1.

[100] As discussed in more detail below, the Commission proposes to define "security incident response plan testing" as the testing of a DCO's security incident response plan to determine the plan's effectiveness, identify potential weaknesses or deficiencies, enable regular plan updating and improvement, and maintain organizational preparedness and resiliency with respect to security incidents.

[101] NIST Special Publication 800-34, Contingency Planning Guide for Federal Information Systems, rev. 1 ("NIST SP 800-34"), p. 10, available at: http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf. Specifically, NIST recommends that an organization develop, document, and distribute to the appropriate personnel "[a]n incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance," as well as "[p]rocedures to facilitate the implementation of the incident response policy and associated incident response controls." NIST SP 800-53, supra note 47, at F-103. See also NIST Special Publication 800-61, Computer Security Incident Handling Guide, rev. 2 ("NIST SP 800-61"), p. 8, available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf. Such incident response plan should:

a. Provide the organization with a roadmap for implementing its incident response capability;
b. Describe the structure and organization of the incident response capability;
c. Provide a high-level approach for how the incident response capability fits into the overall organization;
d. Meet the unique requirements of the organization, which relate to mission, size, structure, and functions;

In addition, NIST states that organizations should test their security incident response capabilities, at appropriate frequencies, to determine their effectiveness, and to document test results.[102]

FINRA's best practices also call for firms to have security incident response plans. FINRA's 2015 Report on Cybersecurity Practices states: "Firms should establish policies and procedures, as well as roles and responsibilities for escalating and responding to cybersecurity incidents. Effective practices for incident response include ... involvement in industry-wide and firm-specific simulation exercises as appropriate to the role and scale of a firm's business."[103] Similarly, the FFIEC also calls for security incident response plan testing, stating that "[f]inancial institutions should assess the adequacy of their preparation by testing incident response guidelines to ensure that the procedures correspond with business continuity strategies."[104] Moreover, the Controls argue that organizations should protect their information, as well as their reputations, by developing and implementing a security incident response plan,[105] and "conduct[ing] periodic incident scenario sessions for personnel associated with the incident handling

---

e. Define reportable incidents;
f. Provide metrics for measuring the incident response capability within the organization;
g. Define the resources and management support needed to effectively maintain and mature an incident response capability; and
h. Be reviewed and approved by [appropriate organization-defined personnel or roles].
Id. at F-109. Finally, copies of the plan should be distributed to appropriate personnel; reviewed at an appropriate frequency; updated to address system or organizational changes, or problems encountered during plan implementation, execution, or testing, with plan changes communicated to appropriate personnel; and protected from unauthorized disclosure and modification. Id.

[102] NIST SP 800-53, supra note 47, app. F-IR at F-104.

[103] FINRA Report, supra note 31, at 23.

[104] FFIEC, Business Continuity Planning Booklet: IT Examination Handbook, Feb. 2015 ("FFIEC BCP Booklet"), p. 26, available at: http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_BusinessContinuityPlanning.pdf.

[105] Council on Cybersecurity, supra note 33, at 96.

team, to ensure that they understand current threats and risks, as well as their responsibilities in supporting the incident handling teams."[106]

The Commission believes that industry best practices require the development, implementation, and testing of a security incident response plan.[107] Proposed § 39.18(e)(6) would require that DCOs have a security incident response plan that is tested at a frequency determined by an appropriate risk analysis, but no less frequently than annually. Because § 39.18 already calls for a DCO's risk analysis and oversight program to follow best practices, this requirement should not impose any additional burdens or costs on DCOs. In addition, the Commission notes that having such plans regularly tested will help DCOs address security incidents more quickly and effectively when they actually happen. Moreover, the Commission notes that annual testing is consistent with industry best practices and an important part of a DCO's business continuity and disaster recovery plan.

The proposed rule would define a "security incident" 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.[108] The Commission further proposes defining a "security incident response

---

[106] Id. at 97.

[107] See, e.g., FINRA Report, supra note 31, at 23; and FFIEC BCP Booklet, supra note 104, at 25 (noting that "[e]very financial institution should develop an incident response policy that is properly integrated into the business continuity planning process").

[108] NIST defines an "incident" as "[a]n occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies." NIST SP 800-53, supra note 47, at B-9. NIST further defines a "computer security incident" as "a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices." NIST SP 800-61, supra note 101, at 6. The FFIEC notes that a security incident represents "the attempted or successful unauthorized access, use, modification, or destruction of information systems or customer data. If unauthorized access occurs, the

plan" as a written plan documenting the DCO's policies, controls, procedures, and resources for identifying, responding to, mitigating, and recovering from security incidents, and the roles and responsibilities of its management, staff, and independent contractors in responding to security incidents. Under the proposed definition, a security incident response plan may be a separate document or a business continuity-disaster recovery plan section or appendix dedicated to security incident response. However, the Commission proposes requiring the DCO's security incident response plan to include the DCO's definition and classification of security incidents; its policies and procedures for reporting security incidents and for internal and external communication and information sharing regarding security incidents; and the hand-off and escalation points in its security incident response process.

The Commission proposes to define "security incident response plan testing" in § 39.18(a) as the testing of a DCO's security incident response plan to determine the plan's effectiveness, identify potential weaknesses or deficiencies, enable regular plan updating and improvement, and maintain organizational preparedness and resiliency with respect to security incidents. Methods of conducting security incident response plan testing may include, but would not be limited to, checklist completion, walk-through or table-top exercises, simulations, and comprehensive exercises.[109] Pursuant to proposed § 39.18(e)(6), a DCO would also be permitted to coordinate its security incident response

---

financial institution's computer systems could potentially fail and confidential information could be compromised." FFIEC BCP Booklet, supra note 104, at 25.

[109] See NIST SP 800-53, supra note 47, app. F-IR at F-104 (stating that "[i]ncident response testing includes, for example, the use of checklists, walk-through or tabletop exercises, simulations (parallel/full interrupt), and comprehensive exercises. Incident response testing can also include a determination of the effects on organizational operations (e.g., reduction in mission capabilities), organizational assets, and individuals due to incident response").

plan testing with other testing required by proposed § 39.18(e),[110] or with the testing of its other business continuity-disaster recovery and crisis management plans. In addition, a DCO would be permitted to conduct security incident response plan testing by engaging independent contractors or by using employees of the DCO who are not responsible for development or operation of the systems or capabilities being tested. The Commission notes that discussion at the CFTC Roundtable included concerns about performing tests in a production environment, as the tests could have the unintended consequence of disrupting business as usual and potentially cause an event.[111] Accordingly, the Commission proposes to give DCOs discretion to decide whether the testing is completed in a production or non-production environment.

5. Enterprise Technology Risk Assessment ("ETRA")

ETRA is an important part of a DCO's risk assessment program because it helps the DCO produce a broad determination of its system safeguards-related risks.[112] In a sense, ETRA can be seen as a strategic approach through which a DCO identifies risks and aligns its systems goals accordingly. A well-conducted ETRA, and the knowledge and prioritization of risks that it provides, can also inform and guide the ongoing testing process and result in more effective cybersecurity risk management.

The Commission notes that with respect to ETRA, best practices provide a number of sources for such risk assessment frameworks,[113] and a DCO would generally be free to choose the assessment framework it believes most appropriate to its particular

[110] In addition to the changes proposed herein, the Commission is proposing to renumber § 39.18(j) as § 39.18(e).

[111] CFTC Roundtable, supra note 8, at 87–88, 118, 321–326, 345–346.

[112] NIST SP 800-39, supra note 59, at 1.

[113] See, e.g., FFIEC Handbook, supra note 57; NIST SP 800-39, supra note 59.

circumstances, provided that its choice is congruent with best practices and is consistent with the DCO's risk profile. For example, FINRA notes that approaches to integrating threats and vulnerabilities in an overall risk assessment report often differ, with some organizations following proprietary risk assessment methodologies and other using vendor products tailored to their particular needs, and with firms using a variety of cyber incident and threat intelligence inputs for their risk assessments.[114]

The Commission proposes to define "ETRA" in § 39.18(a) as a written assessment that includes, but is not limited to, an analysis of threats and vulnerabilities in the context of mitigating controls. An ETRA identifies, estimates, and prioritizes risks to a DCO's operations or assets (which include, for example, mission, functions, image, and reputation risks), or to market participants, individuals, and other entities, resulting from impairment of the confidentiality, integrity, or availability of data and information or the reliability, security, or capacity of automated systems.[115] Proposed § 39.18(e)(7) would provide DCOs flexibility by permitting the ETRA to be completed by independent contractors or employees of the DCO not responsible for development or operation of the systems or capabilities being assessed. The proposal would, however, require an ETRA to be completed at a frequency determined by an appropriate risk analysis by the DCO, but no less frequently than annually.[116] As noted in the PCI-DSS standards, "[p]erforming risk assessments at least annually and upon significant changes allows the organization to keep up to date with organizational changes and evolving threats, trends,

[114] FINRA Report, supra note 31, at 14.

[115] NIST SP 800-53, supra note 47, app. B at B-19.

[116] See, e.g., FINRA Report, supra note 31, at 14 (stating that firms conducting defined risk assessment processes do so either annually or on an ongoing basis throughout the year, in either case culminating in an annual risk assessment report).

and technologies."[117] However, the Commission emphasizes that the proposed requirement to prepare a written assessment on at least an annual basis is not intended to substitute for the DCO's obligation to conduct risk assessment and monitoring on an ongoing basis; rather, its purpose is to formalize the risk assessment process and ensure that it is documented at a minimum frequency. As noted in the FFIEC Handbook: "Monitoring and updating the security program is an important part of the ongoing cyclical security process. Financial institutions should treat security as dynamic with active monitoring; prompt, ongoing risk assessment; and appropriate updates to controls."[118]

B. Scope of Testing and Assessment

The Commission believes that the scope of a DCO's testing should be based on a proper risk analysis that takes into account the DCO's particular automated systems and networks and vulnerabilities, including any recent changes to them, as well as the nature of the DCO's possible adversaries and their capabilities as revealed by current cybersecurity threat analysis.[119] The Commission recognizes that, however, the scope set for particular instances of the various types of cybersecurity testing can vary appropriately.[120] Thus, proposed § 39.18(e)(8) would give a DCO flexibility in setting the scope of particular cybersecurity tests, so long as its overall testing program is sufficient to provide adequate assurance of the overall effectiveness of its cybersecurity controls with respect to its system safeguards-related risks. The Commission believes

[117] See, e.g., PCI-DSS, supra note 54, at 100.

[118] FFIEC Handbook, supra note 57, at 86.

[119] CFTC Roundtable, supra note 8, at 98, 101–103, 108–113, 128–130, 140–142, 173–180.

[120] Id.

that such flexibility should reduce costs and burdens associated with the proposed scope while still effectively measuring the resilience of the DCO system safeguards.

Accordingly, the Commission is proposing that the scope of all testing and assessment required by its system safeguards regulations for DCOs should be broad enough to include all testing of automated systems and controls necessary to identify any vulnerability which, if exploited or accidentally triggered, could enable an intruder or unauthorized user or insider to: interfere with the DCO's operations or with fulfillment of its statutory and regulatory responsibilities; impair or degrade the reliability, security, or capacity of the DCO's automated systems; add to, delete, modify, exfiltrate, or compromise the integrity of any data related to the DCO's regulated activities; or undertake any other unauthorized action affecting the DCO's regulated activities or the hardware or software used in connection with those activities. The Commission believes that this proposed scope is broad enough to address all significant threats to the DCO, while still providing sufficient guidance regarding the elements of the DCO's program.

C. Internal Reporting, Review, and Remediation

Under current § 39.18(j)(3)[121] reports on testing protocols and results must be communicated to, and reviewed by, senior management of the DCO. However, consistent with industry best practices, in § 39.18(e)(9) the Commission is proposing to expand this reporting requirement to include communication to, and review by, the DCO's board of directors. The Commission notes that active management with board level involvement "is an essential effective practice to address cybersecurity threats[, because] [w]ithout that involvement and commitment, a firm is unlikely to achieve its

[121] The Commission is further proposing to renumber § 39.18(j)(3) as § 39.18(e)(9).

cybersecurity goals."[122] Further, the Commission notes that FINRA observes that "[b]oards should play a leadership role in overseeing firms' cybersecurity efforts," and states that the board of directors should understand and approach cybersecurity as an enterprise-wide risk management issue rather than merely an information technology issue.[123] The Commission also notes that FFIEC states that regular reports to the board of directors should address the results of the organization's risk assessment process and of its security monitoring and testing, including both internal and external audits and reviews.[124] In addition, FFIEC calls for boards to review recommendations for changes to the information security program resulting from testing and assessment, and to review the overall effectiveness of the program.[125]

Accordingly, proposed § 39.18(e)(10) would also require DCOs to establish and follow appropriate procedures for the remediation of issues identified through such review, and for evaluation of the effectiveness of testing and assessment protocols. The proposed rule would also add a provision requiring a DCO to analyze the results of the testing and assessment required by the applicable system safeguards rules, in order to identify all vulnerabilities and deficiencies in its systems, and to remediate those vulnerabilities and deficiencies to the extent necessary to enable the DCO to fulfill the requirements of part 39 and meet its statutory and regulatory obligations. The proposed rule would require such remediation to be timely in light of appropriate risk analysis with respect to the risks presented.

---

[122] FINRA Report, supra note 31, at 7.

[123] Id.

[124] FFIEC Handbook, supra note 57, at 5.

[125] Id.

D. Additional Amendments

In addition to the changes discussed above, the Commission is proposing to reorder and renumber certain paragraphs in § 39.18 to make certain technical corrections to improve the clarity of the rule text.

1. Definitions

The Commission is proposing to amend the introductory text of § 39.18(a) to make clear that the definitions therein are also applicable to § 39.34, which sets forth additional system safeguards requirements for SIDCOs and Subpart C DCOs.

The Commission also is proposing to revise the definitions of "relevant area" and "recovery time objective" to make the language consistent with that used elsewhere in § 39.18.

Finally, the Commission is proposing to change references to "the clearing and settlement of existing and new products" to "the processing, clearing, and settlement of transactions" and a single reference to "an entity" to "a [DCO]."

2. Program of Risk Analysis and Oversight

Regulation 39.18(b) requires a DCO to have a program of risk analysis and oversight with respect to its operation and systems that addresses the following elements, set forth in § 39.18(c): (1) information security; (2) business continuity and disaster recovery planning and resources; (3) capacity and performance planning; (4) systems operations; (5) systems development and quality assurance; and (6) physical security and environmental controls. Specific requirements concerning business continuity and disaster recovery are addressed in § 39.18(e), but the regulation does not provide any further guidance on the other five elements. Therefore, the Commission is proposing to

amend § 39.18(c) (renumbered as § 39.18(b)(2))[126] to provide more detail for each of those other five elements.[127]

3. Business Continuity and Disaster Recovery Plan

Regulation 39.18(e)(1) requires that a DCO maintain a business continuity and disaster recovery plan, emergency procedures, and physical, technological, and personnel resources sufficient to enable the timely recovery and resumption of operations and the fulfillment of each obligation and responsibility of the DCO following any disruption of its operations. Regulation 39.18(e)(2) explains that the "responsibilities and obligations" described in § 39.18(e)(1) include the daily processing, clearing, and settlement of transactions. Because these provisions are so closely linked, the Commission is proposing to combine them into a new § 39.18(c)(1).[128]

4. Location of Resources; Outsourcing

Regulation 39.18(f) allows a DCO to satisfy the resource requirement in § 39.18(e)(1) (renumbered as § 39.18(c)(1)) using its own employees and property or through written contractual arrangements with another DCO or other service provider (i.e., outsourcing). The Commission is proposing to amend this provision (and renumber

[126] The Commission is further proposing to renumber § 39.18(d) as § 39.18(b)(3); renumber § 39.18(e)(2) as § 39.18(b)(4); and delete § 39.18(e)(3) and fold its requirements into § 39.18(c)(2). The Commission is also proposing conforming changes to the text of the renumbered provisions.

[127] Although the Commission is proposing, in a concurrent notice of proposed rulemaking, to require that the program of risk analysis and oversight for designated contract markets ("DCMs") include enterprise risk management and governance applicable specifically to security and technology, at this time the Commission is not proposing such a requirement for DCOs. The Commission believes that DCOs face a wider array of risks than DCMs, and therefore any enterprise risk management requirements for DCOs would not be limited to the system safeguards context but rather would need to be addressed in a more comprehensive fashion. The Commission is considering this issue and may address it in a future rulemaking.

[128] The Commission is further proposing to renumber § 39.18(e)(3) as § 39.18(c)(2), and § 39.18(k) as § 39.18(c)(3). The Commission is also proposing conforming changes to the text of the renumbered provisions.

it as § 39.18(d)) to clarify that a DCO is also permitted to use outsourcing to satisfy § 39.18(b)(2) (renumbered as § 39.18(b)(4)), which requires a DCO to establish and maintain resources that allow for the fulfillment of each obligation and responsibility of the DCO in light of the risks identified by the DCO's program of risk analysis and oversight.

In addition, the Commission is proposing to amend § 39.18(f)(2)(i) (renumbered as § 39.18(d)(2)), which states that, if a DCO chooses to use outsourced resources, the DCO retains liability for any failure to meet the responsibilities specified in § 39.18(e)(1) (renumbered as § 39.18(c)(1)), "although it is free to seek indemnification from the service provider." Regulation 39.18 contains no restrictions that would prevent a DCO from seeking indemnification from its service provider; therefore, the Commission is proposing to delete this unnecessary language.

5. Recordkeeping

Under current § 39.18(i), a DCO is required to maintain, and provide to Commission staff upon request, current copies of its business continuity plan and other emergency procedures, its assessments of its operational risks, and records of testing protocols and results. The Commission is proposing to renumber § 39.18(i) as § 39.18(f), and to amend the language to conform with the testing requirements proposed herein.

6. Notice of Exceptional Events

Under current § 39.18(g)(1), a DCO is required to promptly notify Commission staff of any cybersecurity incident that materially impairs, or creates a significant likelihood of material impairment of, automated system operation, reliability, security, or capacity. The Commission is proposing a conforming amendment to § 39.18(g)(1), to

replace the term "cybersecurity incident" with "security incident," as the proposed definition of "security incident" would include a cybersecurity incident.

7. System Safeguards for SIDCOs and Subpart C DCOs

The Commission is proposing to amend § 39.34 to update several cross-references to various provisions of § 39.18.

III. Request for Comment

The Commission requests comment on all aspects of the proposed amendments to §§ 39.18 and 39.34. With respect to testing, the Commission is particularly interested in the following:

Are the testing requirements being proposed in § 39.18 consistent with the DCO core principles set forth in the CEA, particularly the goals of Core Principle I? If so, in what ways? If not, why not?

Are the proposed testing frequencies sufficient to safeguard DCOs against cyber attacks? In particular, should the proposed control testing be done more frequently, or less frequently? In each case, please provide any data you may have that supports an alternate frequency for such testing.

Should the Commission define the term "independent contractor"? If so, how should such term be defined? If not, why not?

What alternatives, if any, would be more effective in reducing systemic risk, mitigating the growing cybersecurity threats faced by DCOs, and achieving compliance with the DCO core principles set forth in the CEA?

The Commission requests that commenters include a detailed description of any such alternatives and estimates of the costs and benefits of such alternatives. Can the

proposed changes to § 39.18 be effectively implemented and complied with? If not, what changes could be made to increase the likelihood of effective implementation and compliance?

IV. Related Matters

A. Regulatory Flexibility Act

The Regulatory Flexibility Act ("RFA") requires that agencies consider whether the regulations they propose will have a significant economic impact on a substantial number of small entities and, if so, provide a regulatory flexibility analysis respecting the impact.[129] The rules proposed by the Commission will impact DCOs. The Commission has previously established certain definitions of "small entities" to be used by the Commission in evaluating the impact of its regulations on small entities in accordance with the RFA.[130] The Commission has previously determined that DCOs are not small entities for the purpose of the RFA.[131] Accordingly, the Chairman, on behalf of the Commission, hereby certifies pursuant to 5 U.S.C. 605(b) that the proposed rules will not have a significant economic impact on a substantial number of small entities.

B. Paperwork Reduction Act

The Paperwork Reduction Act of 1995 ("PRA")[132] imposes certain requirements on Federal agencies, including the Commission, in connection with their conducting or sponsoring any collection of information, as defined by the PRA. An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information

---

[129] 5 U.S.C. 601 et seq.

[130] See 47 FR 18618, 18618–21 (Apr. 30, 1982).

[131] See New Regulatory Framework for Clearing Organizations, 66 FR 45604, 45609 (Aug. 29, 2001).

[132] 44 U.S.C. 3501 et seq.

unless it displays a currently valid control number. This proposed rulemaking contains recordkeeping and reporting requirements that are collections of information within the meaning of the PRA.

The proposed rulemaking contains provisions that would qualify as collections of information, for which the Commission has already sought and obtained a control number from the Office of Management and Budget ("OMB"). The title for this collection of information is "Risk Management Requirements for Derivatives Clearing Organizations" (OMB Control Number 3038-0076). If adopted, responses to this collection of information would be mandatory. As discussed below, the Commission believes the proposal will not impose any new recordkeeping or reporting requirements that are not already accounted for in collection 3038-0076.[133] Accordingly, the Commission invites public comment on the accuracy of its estimate that no additional recordkeeping or information collection requirements or changes to existing collection requirements would result from the proposal.

The Commission will protect proprietary information according to the Freedom of Information Act ("FOIA") and 17 CFR part 145, "Commission Records and Information." In addition, section 8(a)(1) of the CEA strictly prohibits the Commission, unless specifically authorized by the Act, from making public "data and information that would separately disclose the business transactions or market positions of any person and trade secrets or names of customers." The Commission is also required to protect certain

[133] See Risk Management Requirements for Derivatives Clearing Organizations, OMB Control No. 3038-0076, available at: http://www.reginfo.gov/public/do/PRAOMBHistory?ombControlNumber=3038-0076.

information contained in a government system of records according to the Privacy Act of 1974.

1. Clarification of Collection 3038-0076

The Commission notes that DCOs are already subject to system safeguard-related recordkeeping and reporting requirements. As discussed above in section II, the Commission is proposing to amend and renumber current § 39.18(i) as § 39.18(f), to clarify the system safeguard recordkeeping and reporting requirements for DCOs. The proposed regulation would require DCOs, in accordance with § 1.31,[134] to provide the Commission with the following documents promptly upon request of Commission staff: (1) current copies of the DCO's business continuity and disaster recovery plan and other emergency procedures; (2) all assessments of the DCO's operational risks or system safeguard-related controls; (3) all required reports concerning system safeguards testing and assessment, whether conducted by independent contractors or employees of the DCO; and (4) all other documents requested by staff of the Division of Clearing and Risk, or any successor division, in connection with Commission oversight of system safeguards pursuant to the CEA or Commission regulations, or in connection with Commission maintenance of a current profile of the DCO's automated systems. The pertinent recordkeeping and reporting requirements of proposed § 39.18(f) are contained in the provisions of current § 39.18(i), which was adopted on November 8, 2011.[135]

[134] Regulation 1.31(a)(1) specifically provides that "all books and records required to be kept by the CEA or by these regulations shall be kept for a period of five years from the date thereof and shall be readily accessible during the first 2 years of the 5-year period. The rule further provides that "all such books and records shall be open to inspection by any representative of the Commission or the United States Department of Justice.'' See 17 CFR 1.31(a)(1).

[135] 76 FR 69334.

Accordingly, the Commission believes that proposed § 39.18(f) would not impact the burden estimates currently provided for in collection 3038-0076.

2. Information Collection Comments

The Commission invites comment on any aspect of the proposed information collection requirements discussed above. Pursuant to 44 U.S.C. 3506(c)(2)(B), the Commission will consider public comments on such proposed requirements in: (1) evaluating whether the proposed collection of information is necessary for the proper performance of the functions of the Commission, including whether the information will have a practical use; (2) evaluating the accuracy of the Commission's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used; (3) enhancing the quality, utility, and clarity of the information proposed to be collected; and (4) minimizing the burden of collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological information collection techniques.

Copies of the submission from the Commission to OMB are available from the CFTC Clearance Officer, 1155 21st Street, NW, Washington, DC 20581, (202) 418–5160 or from http://RegInfo.gov. Persons desiring to submit comments on the proposed information collection requirements should send those comments to: The Office of Information and Regulatory Affairs, Office of Management and Budget, Room 10235, New Executive Office Building, Washington, DC 20503, Attention: Desk Officer of the Commodity Futures Trading Commission; (202) 395–6566 (fax); or OIRAsubmissions@omb.eop.gov (email). Please provide the Commission with a copy

of submitted comments so that all comments can be summarized and addressed in the final rulemaking, and please refer to the **ADDRESSES** section of this rulemaking for instructions on submitting comments to the Commission. OMB is required to make a decision concerning the proposed information collection requirements between thirty (30) and sixty (60) days after publication of the proposal in the **Federal Register**. Therefore, a comment to OMB is best assured of receiving full consideration if OMB (as well as the Commission) receives it within thirty (30) days of publication of the proposal.

C. Consideration of Costs and Benefits

1. Introduction

Section 15(a) of the CEA requires the Commission to consider the costs and benefits of its actions before promulgating a regulation under the CEA or issuing certain orders.[136] Section 15(a) further specifies that the costs and benefits shall be evaluated in light of five broad areas of market and public concern: (1) protection of market participants and the public; (2) efficiency, competitiveness and financial integrity of futures markets; (3) price discovery; (4) sound risk management practices; and (5) other public interest considerations. The Commission's cost and benefit considerations in accordance with section 15(a) are discussed below.

As an initial matter, the Commission considers the incremental costs and benefits of these regulations, that is the costs and benefits that are above the current system safeguard practices and requirements under the CEA and the Commission's regulations for DCOs. Where reasonably feasible, the Commission has endeavored to estimate

[136] 7 U.S.C. 19(a).

quantifiable costs and benefits. Where quantification is not feasible, the Commission identifies and describes costs and benefits qualitatively.[137]

The Commission requests comment on the costs and benefits associated with the proposed regulations. As discussed below, the Commission has identified certain costs and benefits associated with the proposed regulations and requests comment on all aspects of its proposed consideration of costs and benefits, including identification and assessment of any costs and benefits not discussed herein. In addition, the Commission requests that commenters provide data and any other information or statistics that the commenters relied on to reach any conclusions regarding the Commission's proposed consideration of costs and benefits, including the series of questions in section 3(f).

2. Background and Baseline for the Proposal

As discussed above, the Commission believes that the current cyber threats to the financial sector have expanded dramatically over recent years.[138] Accordingly, the current cyber threat environment highlights the need to consider an updated regulatory framework with respect to cybersecurity testing for DCOs. Although the Commission acknowledges that the proposed amendments would likely result in some additional costs for DCOs, the proposal would also bring several overarching benefits to the futures and swaps industry. As discussed more fully below, a comprehensive cybersecurity testing program is crucial to efforts by DCOs to strengthen cyber defenses, to mitigate operational, reputational, and financial risk, and to maintain cyber resilience and ability

[137] For example, to quantify benefits such as enhanced protections for market participants and the public and financial integrity of the futures and swaps markets would require information, data and/or metrics that either do not exist, or to which the Commission generally does not have access.

[138] See supra section I.B.

to recover from cyber attack.[139] Significantly, to ensure the effectiveness of cybersecurity controls, a DCO must test in order to find and fix its vulnerabilities before an attacker exploits them.[140]

The Commission recognizes that any economic effects, including costs and benefits, should be compared to a baseline that accounts for current regulatory requirements. The baseline for this cost and benefit consideration is the set of requirements under the CEA and the Commission's regulations for DCOs. Currently, § 39.18(j)(1)(i) requires a DCO to conduct regular, periodic, and objective testing and review of its automated systems to ensure that they are reliable, secure, and have adequate scalable capacity.[141] This requirement, which forms part of the DCO risk analysis program required under § 39.18(b), must be satisfied by following, at a minimum, "generally accepted standards and industry best practices."[142] In addition to the generally accepted standards and industry best practices discussed in section II above, this cost and benefit discussion uses information provided by DCOs in connection with a recent survey of DCO system safeguard costs and practices conducted by Commission staff ("February 2015 DCR Survey").[143]

---

[139] See also supra section I.C.

[140] See supra section II.A.

[141] 17 CFR 39.18(j).

[142] See 17 CFR 39.18(d).

[143] On February 19, 2015, the Division of Clearing and Risk requested, pursuant to § 39.19(c)(5)(i), information from each registered DCO regarding the scope and costs of its current system safeguard testing. Of the 14 DCOs contacted, 13 responded. ICE Clear Credit, ICE Clear Europe, Ice Clear US, and the Clearing Corporation, each subsidiaries of Intercontinental Exchange, Inc., provided a single response, indicating that their testing costs are shared. LCH.Clearnet Ltd, LCH.Clearnet LLC, and LCH.Clearnet SA, each subsidiaries of LCH.Clearnet Group Ltd., also provided a single response, indicating that their testing costs are shared.

The Commission notes, however, that in certain instances the cost estimates provided by the DCOs included estimates at the parent company level of the DCO. Where parent level estimates were provided, the DCOs explained that they generally share the same automated systems and system safeguard programs with other entities within the corporate structure and were therefore unable to apportion the actual costs to particular entities. The Commission further notes that some of the DCOs that supplied cost information are also registered with the Commission in other capacities (as DCMs and/or swap data repositories). These DCOs provided cost estimates that cover all of their Commission-regulated functions because they generally share the same automated systems and system safeguard programs. Therefore, the Commission has attempted to account for these distinctions, where appropriate.

The Commission believes that certain entities that would be subject to the proposal already comply with most of the testing requirements while others may need some modest enhancements to their system safeguard program to achieve compliance. In this same regard, the Commission notes that some DCOs are larger or more complex than others, and the proposed requirements may impact DCOs differently depending on their size and the complexity of their systems. Thus, the Commission expects that the costs and benefits may vary somewhat among DCOs. The Commission also believes that to the extent the new requirements impose additional costs, the primary costs will be in the form of more frequent testing, including some testing that would have to be carried out by independent contractors on behalf of the DCO. As a result, the proposed rules may increase operational costs for DCOs by requiring additional resources. The Commission is sensitive to the economic effects of the proposed regulations, including costs and

benefits. Accordingly, the Commission seeks comment on the costs and benefits of the proposed regulations, including where possible, quantitative data.

While certain costs are amenable to quantification, other costs are not easily estimated, such as the costs to the public or market participants in the event of a cybersecurity incident at a DCO. The Commission's proposed regulations are intended to further mitigate the frequency and severity of system security breaches or functional failures, and therefore, serve an important, if unquantifiable, public benefit. Although the benefits of effective regulation are difficult to value in dollar terms, the Commission believes that they are no less important to consider given the Commission's mission to protect market participants and the public and to promote market integrity.

The discussion of costs and benefits that follows begins with a summary of the current testing requirements and sources for industry best practices as well as a summary of each proposed regulation and a consideration of the corresponding costs and benefits. At the conclusion of this discussion, the Commission considers the costs and benefits of the proposed regulations collectively in light of the five factors set forth in section 15(a) of the CEA.

3. Consideration of Costs and Benefits Related to Related to the Proposed Rules

a. Regulation 39.18(a)—Definitions

(i) Summary of Proposed Regulations

As discussed above in section II, proposed § 39.18(a) would add to the existing list of definitions, definitions for the following terms: (1) controls; (2) controls testing; (3) enterprise technology risk assessment; (4) external penetration testing; (5) internal

penetration testing; (6) key controls; (7) security incident; (8) security incident response plan; (9) security incident response plan testing; and (10) vulnerability testing.

(ii) Costs and Benefits

The proposed definitions simply provide context to the specific system safeguard tests and assessments that a DCO would be required to conduct on an ongoing basis. Accordingly, the costs and benefits of these terms are attributable to the substantive testing requirements and, therefore, are discussed in the cost and benefit considerations related to the rules describing the requirements for each test.

b. Regulation 39.18(e)(2)—Vulnerability testing

(i) Summary of Proposed Regulations

As discussed above in section II(A)(1), proposed § 39.18(a) defines "vulnerability testing" as testing of a DCO's automated systems to determine what information may be discoverable through a reconnaissance analysis of those systems and what vulnerabilities may be present on those systems. Regulation 39.18(e)(2) requires such testing to be of a scope sufficient to satisfy the testing scope requirements of proposed § 39.18(e)(8). Regulation 39.18(e)(2)(i) requires a DCO to conduct vulnerability testing at a frequency determined by an appropriate risk analysis, but at a minimum no less frequently than quarterly. Among the four vulnerability tests conducted annually, the proposed regulations would require a DCO to engage independent contractors to perform two of the required quarterly tests each year for the DCO, although other vulnerability testing may be conducted by employees of the DCO who are not responsible for development or operation of the systems or capabilities being tested. The vulnerability test would also

require automated vulnerability scanning, which may be authenticated or unauthenticated.

(ii) Costs

The Commission believes that the scope requirement of proposed § 39.18(e)(2) will not impose new costs on DCOs. Comprehensive vulnerability testing is an industry best practice,[144] and therefore required to be conducted under current Commission regulations. Moreover, the Commission believes, based on the representations made by DCOs to Commission staff in administering the Commission's examination program and DCO responses to the February 2015 DCR Survey, that most DCOs are currently conducting vulnerability testing sufficient to meet the scope requirements of proposed § 39.18(e)(2). The Commission also believes that the frequency requirement of proposed § 39.18(e)(2)(i) will not impose new costs on DCOs. The Commission notes that industry best practices state that vulnerability testing should be conducted "at least quarterly."[145] Accordingly, current § 39.18 requires DCOs to conduct vulnerability testing on a quarterly basis. In addition, the Commission notes that all 13 DCOs responding to the February 2015 DCR Survey conduct vulnerability testing on a quarterly basis at a minimum.[146]

Proposed § 39.18(e)(2)(ii) would require a DCO to conduct vulnerability tests that include automated vulnerability scanning on an authenticated basis, or, where not

[144] See, e.g., NIST SP-800-53, supra note 47, at F-153; FFIEC Handbook, supra note 57, at 10 ("Financial institutions should assess potential threats and vulnerabilities of their information systems."); PCI-DSS, supra note 54, at 94.

[145] See supra section II.A.1.; see also supra note 57 and accompanying text.

[146] The frequency of vulnerability testing ranged from 5 to 200 tests per year.

conducted on an authenticated basis, to implement compensating controls.[147] The Commission notes that industry best practices specifically recommend authenticated scanning.[148] Likewise, current § 39.18 requires DCOs to conduct authenticated scanning and Commission staff has examined DCOs for compliance with such requirement. Accordingly, the Commission does not believe that DCOs will incur additional costs as a result of the adoption of proposed § 39.18(e)(2)(ii).

Under proposed § 39.18(e)(2)(iii), for at least two of the required quarterly vulnerability tests each year, vulnerability testing must be conducted by an independent contractor. However, the remaining two vulnerability tests may be conducted by a DCO's employees so long as those employees are not responsible for development or operation of the systems or capabilities being tested.[149] The Commission notes that at least 9 of the 13 DCOs responding to the February 2015 DCR Survey currently conduct at least some of their vulnerability testing using independent contractors. The Commission does not, however, have quantification or estimation of the costs associated with proposed § 39.18(e)(2)(iii). Nonetheless, in qualitative terms, the Commission recognizes that, compared to the status quo, this proposed requirement may impose some costs on DCOs equal to the difference between conducting vulnerability testing in-house and hiring an independent contractor. In particular, these proposed regulations may require DCOs to establish and implement internal policies and procedures that are reasonably designed to address the workflow associated with the test, which may include

[147] See supra notes 55 and 56 and accompanying text.

[148] See, e.g., NIST SP 800-53, supra note 47, at F-154 ("Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and also protects the sensitive nature of such scanning.").

[149] See supra section II.A.1.

the communication and cooperation between the entity and independent contractor, communication and cooperation between the entity's legal, business, technology, and compliance departments, appropriate authorization to remediate vulnerabilities identified by the independent contractor, implementation of the measures to address such vulnerabilities, and verification that these measures are effective and appropriate. The Commission requests comment on the potential costs of proposed § 39.18(e)(2)(iii) on DCOs, including, where possible, quantitative data.

(iii) Benefits

Vulnerability testing identifies, ranks, and reports vulnerabilities that, if exploited, may result in an intentional or unintentional compromise of a system.[150] The complex analysis and plan preparation that a DCO undertakes to complete vulnerability testing, including designing and implementing changes to existing plans, are likely to contribute to a better ex ante understanding by the DCO's management of the challenges the DCO would face in a cyber threat scenario, and thus better preparation to meet those challenges. This improved preparation helps reduce the possibility of market disruptions and financial losses to clearing members and their customers. Regularly conducting vulnerability tests enables a DCO to mitigate the impact that a cyber threat to, or a disruption of, a DCO's operations would have on customers, clearing members, and, more broadly, the stability of the U.S. financial markets. Accordingly, the Commission believes that such testing strengthens DCOs' systems, thereby protecting clearing members and their customers from a disruption in clearing services.

[150] PCI-DSS Penetration Testing, supra note 70, at 3.

The Commission acknowledges, as described above, that some DCOs may incur additional costs as a result of the new requirement in proposed § 39.18(e)(2)(iii) that independent contractors complete the vulnerability testing. Nevertheless, the Commission believes that the use of independent contractions for vulnerability testing – a practice that many DCOs report already doing – will strengthen this important system safeguard, significantly benefitting the DCO, financial markets, and the public by mitigating systemic risk.

The Commission requests comments on the potential benefits to a DCO in complying with all aspects of proposed § 39.18(e)(2), and any benefits that would be realized by members of DCOs and their customers, as well as other market participants or the financial system more broadly. The Commission specifically requests comment on alternative means to address these issues, and the benefits associated with such alternatives.

c. Regulation 39.18(e)(3)—External penetration testing

(i) Summary of Proposed Regulations

As discussed above in section II(A)(2), proposed § 39.18(a) defines "external penetration testing" as "attempts to penetrate a [DCO's] automated systems from outside the systems' boundaries to identify and exploit vulnerabilities," and proposed § 39.18(e)(3) requires such testing to be of a scope sufficient to satisfy the testing scope requirements of proposed § 39.18(e)(8). Proposed § 39.18(e)(3)(i) would require a DCO to conduct external penetration testing at a frequency determined by an appropriate risk analysis, but at a minimum no less frequently than annually. The proposed rule also provides that independent contractors must perform the required annual external

penetration test on behalf of the DCO. However, other external penetration testing may be performed by appropriately qualified DCO employees not responsible for development or operation of the systems or capabilities being tested.

(ii) Costs

The Commission believes that the scope requirement of proposed § 39.18(e)(3) will not impose new costs on DCOs. Comprehensive external penetration testing is an industry best practice[151] and, based on the representations made by DCOs to Commission staff in administering the Commission's examination program and DCO responses to the February 2015 DCR Survey, the Commission believes that most DCOs are currently conducting external penetration testing sufficient to meet the scope requirements of proposed § 39.18(e)(3).

In addition, the Commission believes that the frequency requirement of proposed § 39.18(e)(3)(i) will not impose new costs on DCOs. The Commission notes that industry best practices specifically state that external penetration testing should be conducted "at least annually."[152] Therefore current Commission regulations require annual penetration testing. Moreover, the Commission notes that at least 11 of the 13 DCOs responding to the February 2015 DCR Survey conduct, at a minimum, annual external penetration testing, with two DCOs responding that they conduct periodic external penetration testing.

The Commission believes that the requirement of proposed § 39.18(e)(3)(ii) to use an independent contractor will not impose new costs on DCOs. Current § 39.18(j)(2)

[151] See, e.g., NIST SP 800-53, supra note 47, app. F-CA at F-62; FFIEC Handbook, supra note 57, at 81; PCI-DSS, supra note 54, at 96–97; see also section II.A.2.

[152] See, e.g., PCI-DSS, supra note 54, at 96–97; see also section II.A.2.

requires external penetration testing to be conducted by a qualified, independent professional, who can be employed by the DCO so long as he or she is not responsible for development or operation of the systems or capabilities being tested. However, as discussed above, [153] the Commission notes that it is industry best practice for DCOs to employ independent contractors to conduct their external penetration testing, and therefore it is currently required under § 39.18. The Commission notes that at least 11 of the 13 DCOs responding to the February 2015 DCR Survey already employ independent contractors to conduct their external penetration testing. The Commission is proposing § 39.18(e)(3)(ii) to make clear that independent contractors must conduct the required annual external penetration test.

The Commission requests comment on the potential costs of proposed § 39.18(e)(3) on DCOs, including, where possible, quantitative data.

(iii) Benefits

External penetration testing benefits DCOs by identifying the extent to which its systems can be compromised before an attack is identified.[154] Such testing is conducted outside a DCO's security perimeter to help reveal vulnerabilities that could be exploited by an external attacker. Accordingly, the Commission believes that the external penetration testing strengthens DCOs' systems, thereby protecting clearing members and their customers from a disruption in clearing services, which could potentially disrupt the functioning of the broader financial markets.

[153] See supra section II.A.2.

[154] FFIEC Handbook, supra note 57, at 81; see also supra section II.A.2.

As stated above, industry best practices require DCOs to engage independent contractors to conduct annual external penetration testing. Further, to the extent there is a lack of clarity regarding the applicability of certain industry best practices in light of the language in current § 39.18(j)(2), proposed § 39.18(e)(3)(ii) would provide additional clarity. Moreover, the Commission believes that testing by an independent contractor has particular value with respect to external penetration testing because the test comes from the viewpoint of an outsider, which may differ from the views of current tactics, techniques, and threat vectors of current threat actors held by DCO employees. The Commission believes that external penetration testing helps DCOs, which constitute critical infrastructures important to the national economy, to be adequately protected against the level of cybersecurity threat now affecting the financial sector.

The Commission requests comments on the potential benefits to a DCO in complying with all aspects of proposed § 39.18(e)(3), and any benefits that would be realized by members of DCOs and their customers, as well as other market participants or the financial system more broadly. The Commission specifically requests comment on alternative means to address these issues, and the benefits associated with such alternatives.

d. Regulation 39.18(e)(4)—Internal penetration testing

(i) Summary of Proposed Regulations

As discussed above in section II(A)(2), proposed § 39.18(a) defines "internal penetration testing" as "attempts to penetrate a [DCO's] automated systems from inside the systems' boundaries to identify and exploit vulnerabilities." Proposed § 39.18(e)(4) requires such testing to be of a scope sufficient to satisfy the testing scope requirements

of proposed § 39.18(e)(8). Proposed § 39.18(e)(4)(i) requires a DCO to conduct internal penetration testing at a frequency determined by an appropriate risk analysis, but no less frequently than annually. The test may be conducted by independent contractors, or by appropriately qualified DCO employees not responsible for development or operation of the systems or capabilities being tested.

(ii) Costs

The Commission believes that the scope requirement of proposed § 39.18(e)(4) will not impose new costs on DCOs. Comprehensive internal penetration testing is an industry best practice,[155] and is therefore required under current regulations. In addition, based on the representations made by DCOs to Commission staff in administering the Commission's examination program and responses to the February 2015 DCR Survey, the Commission believes that most DCOs are currently conducting internal penetration testing sufficient to meet the scope requirements of proposed § 39.18(e)(4).

Proposed § 39.18(e)(4)(i) would require a DCO to conduct internal penetration testing at a frequency determined by an appropriate risk analysis, but no less frequently than annually. As discussed above, industry best practices require annual internal penetration testing, as well as after any significant infrastructure or application upgrade or modification."[156] Moreover, the Commission notes that the February 2015 DCR Survey indicated that most DCOs conduct internal penetration testing at least annually.

The Commission also believes that proposed § 39.18(e)(4)(ii) will not impose new costs on DCOs. Proposed § 39.18(e)(4)(ii) requires DCOs to conduct internal

[155] See, e.g., NIST SP 800-53, supra note 47, at F-62; FFIEC Handbook, supra note 57, at 81; PCI-DSS, supra note 54, at 96–97; see also supra section II.A.2.

[156] See, e.g., PCI-DSS, supra note 54, at 96–97; see also supra section II.A.2.

penetration testing by engaging independent contractors, or by using employees of the DCO who are not responsible for development or operation of the systems or capabilities being tested. Regulation 39.18(j)(2) currently requires testing to be conducted by a qualified, independent professional, who can be employed by the DCO so long as he or she is not responsible for development or operation of the systems or capabilities being tested. Accordingly, proposed § 39.18(e)(4)(ii) would not change current regulatory requirements.

The Commission requests comment on the potential costs of proposed § 39.18(e)(4) on DCOs, including, where possible, quantitative data.

(iii) Benefits

By attempting to penetrate a DCO's automated systems from inside the systems' boundaries, internal penetration tests allow DCOs to assess system vulnerabilities from attackers that penetrate the DCO's perimeter defenses and from trusted insiders, such as former employees and contractors. In addition to being an industry best practice, the Commission believes that an annual internal penetration testing is important because such potential attacks by trusted insiders generally pose a unique and substantial threat due to their more sophisticated understanding of a DCO's systems. Moreover, "[a]n advanced persistent attack may involve an outsider gaining a progressively greater foothold in a firm's environment, effectively becoming an insider in the process. For this reason, it is important to perform penetration testing against both external and internal interfaces and systems."[157] The Commission also believes that internal penetration testing strengthens DCOs' systems, thereby protecting clearing members and their customers from a

[157] FINRA Report, supra note 31, at 22.

disruption in clearing services, which could potentially disrupt the functioning of the broader financial markets.

The Commission requests comments on the potential benefits to a DCO in complying with all aspects of proposed § 39.18(e)(4), and any benefits that would be realized by members of DCOs and their customers, as well as other market participants or the financial system more broadly. The Commission specifically requests comment on alternative means to address these issues, and the benefits associated with such alternatives.

e. Regulation 39.18(e)(5)—Controls testing

(i) Summary of Proposed Regulations

As discussed above in section II(A)(3), proposed § 39.18(a) defines "controls testing" as an assessment of the DCO's controls to determine whether such controls are implemented correctly, are operating as intended, and are enabling the DCO to meet the requirements of proposed § 39.18, and proposed § 39.18(e)(5) requires such testing to be of a scope sufficient to satisfy the testing scope requirements of proposed § 39.18(e)(8). Proposed § 39.18(e)(5)(i) would require a DCO to conduct controls testing, which includes testing of each control included in its program of risk analysis and oversight, at a frequency determined by an appropriate risk analysis, but no less frequently than every two years.

Pursuant to proposed § 39.18(e)(5)(ii), a DCO would be required to engage independent contractors to test and assess its "key controls," which are defined in proposed § 39.18(a) as "controls that an appropriate risk analysis determines are either critically important for effective system safeguards or intended to address risks that

evolve or change more frequently and therefore require more frequent review to ensure their continuing effectiveness in addressing such risks." DCOs may conduct any other non-key controls testing by using independent contractors or employees of the DCO who are not responsible for development or operation of the systems or capabilities being tested.

(ii) Costs

The Commission does not believe that the scope requirement of proposed § 39.18(e)(5) will impose new costs on DCOs. Comprehensive controls testing is an industry best practice.[158] Accordingly, current § 39.18 requires DCOs to conduct comprehensive controls testing. In addition, based on the representations made by DCOs to Commission staff in administering the Commission's examination program and responses to the February 2015 DCR Survey, the Commission believes that most DCOs are currently conducting controls testing sufficient to meet the scope requirements of proposed § 39.18(e)(5).

Proposed § 39.18(e)(5)(i) would require control testing to be conducted at a frequency determined by an appropriate risk analysis, but no less frequently than every two years. The Commission recognizes, however, that appropriate risk analysis may well determine that more frequent testing of either certain key controls or all controls is necessary. For example, the Commission notes that the February 2015 DCR Survey indicated that most DCOs conduct controls testing at least annually.[159]

---

[158] See, e.g., NIST SP 800-137, supra note 81, at vi; PCI-DSS, supra note 54, at 13; see also supra section II.A.3.

[159] Seven of the responding DCOs conduct controls testing annually, three DCOs conduct controls testing biannually, two DCOs conduct controls testing triennially, and one DCO does not conduct controls testing.

Proposed § 39.18(e)(5)(ii) would require DCOs to engage independent contractors to test and assess its key controls. Regulation 39.18(j)(2) currently requires testing to be conducted by a qualified, independent professional, who can be employed by the DCO so long as he or she is not responsible for development or operation of the systems or capabilities being tested. The Commission notes that at least 11 of the 13 DCOs responding to the February 2015 DCR Survey already employ independent contractors to conduct key controls testing.

The Commission does not have quantification or estimation of the costs associated with proposed § 39.18(e)(5)(i) or proposed § 39.18(e)(5)(ii). Nonetheless, in qualitative terms, the Commission recognizes that, compared to the status quo, this proposed requirement may impose some costs on DCOs equal to the difference between conducting controls testing every two years in-house and hiring an independent contractor to do so. In addition, with respect to the frequency requirement in the proposed rule, a DCO would be required to test each control included in its program of system safeguards-related risk analysis oversight, at a frequency determined by appropriate risk analysis, but no less frequently than every two years. The Commission further recognizes that actual costs may vary as a result of numerous factors, including the size of the DCO and the complexity of the automated systems. Moreover, these proposed regulations may require DCOs to establish and implement internal policies and procedures that are reasonably designed to address the workflow associated with the controls test, which may include the communication and cooperation between the DCO and independent contractor, communication and cooperation between the DCO's legal, business, technology, and compliance departments, appropriate authorization to

remediate vulnerabilities identified by the independent contractor, implementation of the measures to address such vulnerabilities, and verification that these measures are effective and appropriate.

The Commission requests comment on the potential costs of proposed § 39.18(e)(5) on DCOs, including, where possible, quantitative data.

(iii) Benefits

Controls testing is essential in determining risk to an organization's operations and assets, to individuals, and to other organizations, and to the Nation resulting from the use of the organization's systems.[160] In other words, controls testing is vital because it allows firms to be nimble in preventing, detecting, or recovering from an attack.[161] The Commission believes that the complex analysis and plan preparation that a DCO undertakes with respect to controls testing, including designing and implementing changes to existing plans, likely contributes to a better ex ante understanding by the DCO's management of the challenges the DCO would face in a cyber threat scenario, and thus better preparation to meet those challenges. This improved preparation would help reduce the possibility of market disruptions and financial losses to clearing members and their customers. Moreover, regularly conducting controls testing enables a DCO to mitigate the impact that a cyber threat to, or a disruption of, a DCO's operations would have on customers, clearing members, and, more broadly, the stability of the U.S. financial markets. Accordingly, the Commission believes that such testing strengthens a

[160] See NIST SP 800-53A, supra note 92, at 1; see also supra section II.A.3.

[161] Statement of Mr. Mark Clancy, Chief Executive Officer, Soltra, CFTC Roundtable, supra note 8.

DCO's systems, thereby protecting clearing members and their customers from a disruption in clearing services

In addition, the Commission acknowledges that, as described above, some DCOs may incur some additional costs as a result of the need to conduct testing by an independent contractor. However, the Commission believes that testing by an independent contractor has particular value because the test comes from the viewpoint of an outsider, which may differ from the views of current tactics, techniques, and threat vectors of current threat actors held by DCO employees. The Commission also acknowledges that, as described above, some DCOs may incur some additional costs as a result of the need to accelerate the testing of some controls in order to comply with the two-year cycle requirement. Nevertheless, the Commission believes that it is essential for each control to be tested within the two-year cycle requirement in order to confirm the continuing adequacy of the DCO's system safeguards and maintain market stability. Additionally, the Commission notes that the proposed rule would permit such testing to be conducted on a rolling basis over the course of a two year period or period determined by appropriate risk analysis. The rolling basis provision in the proposed rule is designed to give a DCO flexibility concerning when controls are tested during the required minimum frequency period. This flexibility is intended to reduce burdens associated with testing every control while still ensuring the needed minimum testing frequency. The Commission also notes that testing on a rolling basis is consistent with best practices.

The Commission requests comments on the potential benefits to a DCO in complying with all aspects of proposed § 39.18(e)(5), and any benefits that would be realized by members of DCOs and their customers, as well as other market participants or

the financial system more broadly. The Commission specifically requests comment on alternative means to address these issues, and the benefits associated with such alternatives.

f. Regulation 39.18(e)(6)—Security incident response plan testing

(i) Summary of Proposed Regulations

As discussed above in section II(A)(4), proposed § 39.18(a) defines security incident response plan testing as testing of a DCO's security incident response plan to determine the plan's effectiveness, identifying its potential weaknesses or deficiencies, enabling regular plan updating and improvement, and maintaining organizational preparedness and resiliency with respect to security incidents. Methods of conducting security incident response plan testing would include, but not be limited to, checklist completion, walk-through or table-top exercises, simulations, and comprehensive exercises.

Proposed § 39.18(e)(6)(i) would require DCOs to conduct such testing at a frequency determined by an appropriate risk analysis, but at a minimum no less frequently than annually. Proposed § 39.18(e)(6)(ii) would require the DCO's security incident response plan to include, without limitation, the entity's definition and classification of security incidents, its policies and procedures for reporting security incidents and for internal and external communication and information sharing regarding security incidents, and the hand-off and escalation points in its security incident response process. Under proposed § 39.18(e)(6)(iii), the DCO may coordinate its security incident response plan testing with other testing required by this section or with testing of its other business continuity-disaster recovery and crisis management plans. Moreover, proposed

§ 39.18(e)(6)(iv) would permit the DCO to conduct security incident response plan testing by engaging independent contractors or by using its own employees.

(ii) Costs

The Commission believes that proposed § 39.18(e)(6)(i) will not impose new costs on DCOs. Security incident response plan testing is an industry best practice and therefore is required to be conducted under current Commission regulations.[162] Moreover, the Commission notes that industry best practices state that security incident response plan testing should be conducted annually.[163] Accordingly, proposed § 39.18(e)(6)(ii) will not impose new costs on DCOs because current § 39.18 requires DCOs to conduct security incident response plan testing on an annual basis. Finally, as stated above, § 39.18(e)(6)(iii) and (iv) do not contain explicit requirements, but rather provide a DCO with flexibility to: (1) coordinate its security incident response plan testing with other testing required by § 39.18 or with testing of its other business continuity-disaster recovery and crisis management plans; and (2) consistent with current § 39.18(j)(2), engage independent contractors or use employees of the DCO who are not responsible for development or operation of the systems or capabilities being tested. Accordingly, these provisions will not impose new costs on DCOs.

---

[162] See e.g., NIST SP 800-34, supra note 101, at 11; FINRA Report, supra note 31, at 23; FFIEC BCP Booklet, supra note 104, at 25; and Council on Cybersecurity, supra note 33, at CSC 18; see also supra section II.A.4. Similarly, the Commission proposes to expressly require DCOs to update their business continuity and disaster recovery plans and other emergency plans at least annually. The Commission notes that updating such plans and procedures at least annually is an industry best practice. See NIST SP 800-61, supra note 101, at 8. Thus, annual updates are required under current Commission regulations. Therefore, the Commission does not believe that this proposal would impose new costs on DCOs. The Commission acknowledges that this proposal could impose additional burdens or costs on DCOs. The Commission believes, however, that DCOs must be adequately protected in today's environment.

[163] See, e.g., NIST Special Publication 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, Sept. 2006, p. ES-2, available at: http://csrc.nist.gov/publications/nistpubs/800-84/SP800-84.pdf; PCI-DSS, supra note 54, at 108; see also supra section II.A.4.

The Commission requests comment on the potential costs of proposed § 39.18(e)(6) on DCOs, including, where possible, quantitative data.

(iii) Benefits

Security incident response plans, and adequate testing of such plans, reduce the damage caused by breaches of a DCO's network security. Network security breaches are highly likely to have a substantial negative impact on a DCO's operations. They can increase costs through lost productivity, lost current and future market participation or swap data reporting, compliance penalties, and damage to the DCO's reputation and brand. Moreover, the longer a cyber intrusion continues, the more its impact may be compounded.

As noted above, and consistent with industry best practices, the Commission believes that annual security incident response testing increases the ability of a DCO to mitigate the duration and impact in the event of a security incident.[164] Thus, a DCO may be better positioned to minimize any potential impacts to automated system operations, reliability, security, or capacity, or the availability, confidentiality, or integrity of its derivatives data.

The Commission requests comments on the potential benefits to a DCO in complying with all aspects of proposed § 39.18(e)(6), and any benefits that would be realized by members of DCOs and their customers, as well as other market participants or the financial system more broadly. The Commission specifically requests comment on

[164] As noted above, the proposed provision that would require DCOs to update their business continuity and disaster recovery plans and other emergency plans at least annually reflects what is already considered an industry best practice. Further, annual updates are important because once an organization has developed a business continuity and disaster recovery plan, "the organization should implement the plan and review it at least annually to ensure the organization is following the roadmap for maturing the capability and fulfilling their [sic] goals for incident response." NIST SP 800-61, supra note 101, at 8.

alternative means to address these issues, and the benefits associated with such alternatives.

g. Regulation 39.18(e)(7)—Enterprise technology risk assessment

(i) Summary of Proposed Regulations

Proposed § 39.18(a) defines an "enterprise technology risk assessment" as a written assessment that includes, but is not limited to, an analysis of threats and vulnerabilities in the context of mitigating controls. Proposed § 39.18(a) also provides that an enterprise technology risk assessment identifies, estimates, and prioritizes risks to a DCO's operations or assets, or to market participants, individuals, or other entities, resulting from impairment of the confidentiality, integrity, or availability of data and information or the reliability, security, or capacity of automated systems. Proposed § 39.18(e)(7) requires such assessment to be of a scope sufficient to satisfy the requirements of proposed § 39.18(e)(8). Proposed § 39.18(e)(7)(i) requires DCOs to conduct an enterprise technology risk assessment at a frequency determined by an appropriate risk analysis, but no less frequently than annually. Proposed § 39.18(e)(7)(ii) provides that DCOs may use independent contractors or employees of the DCO not responsible for development or operation of the systems or capabilities being assessed to conduct an enterprise technology risk assessment.

(ii) Costs

The Commission does not believe that the scope requirement of proposed § 39.18(e)(7) will impose new costs on DCOs. Comprehensive enterprise technology

risk assessments are an industry best practice.[165] Accordingly, current § 39.18 requires DCOs to conduct enterprise technology risk assessments. In addition, based on the representations made by DCOs to Commission staff in administering the Commission's examination program and responses to the February 2015 DCR Survey, the Commission believes that most DCOs are currently conducting enterprise technology risk assessments sufficient to meet the scope requirements of proposed § 39.18(e)(7).

Proposed § 39.18(e)(7)(i) would require a DCO to conduct an enterprise technology risk assessment at a frequency determined by an appropriate risk analysis, but no less frequently than annually. As discussed above,[166] industry best practices require enterprise technology risk assessments at least annually and upon significant changes to the environment.[167] Thus, current regulations require DCOs to conduct enterprise technology risk assessments on an annual basis. Accordingly, the Commission does not believe that proposed § 39.18(e)(7)(i) will impose new costs on DCOs. Moreover, the Commission notes that responses to the February 2015 DCR Survey indicated that most DCOs conduct an enterprise technology risk assessment at least annually.

Proposed § 39.18(e)(7)(ii) requires DCOs to conduct enterprise technology risk assessments by using independent contractors or employees of the DCO not responsible for development or operation of the systems or capabilities being assessed. Regulation 39.18(j)(2) currently requires testing to be conducted by a qualified, independent professional, who can be employed by the DCO so long as he or she is not responsible for

---

[165] See, e.g., NIST SP 800-39, supra note 59; FFIEC Handbook, supra note 57, at 86; PCI-DSS, supra note 54, at 100; see also supra section II.A.5.

[166] See supra section II.A.5.

[167] PCI-DSS, supra note 54, at 100.

development or operation of the systems or capabilities being tested. Accordingly, the Commission does not believe that DCOs will incur additional costs as a result of the adoption of proposed § 39.18(e)(7)(ii).

(iii) Benefits

The Commission believes that enterprise technology risk assessments are essential components of a comprehensive system safeguard program. Enterprise technology risk assessments can be viewed as a strategic approach through which a DCO identifies risks and aligns its systems goals accordingly. The Commission believes that these requirements are necessary to support a strong risk management framework for DCOs, thereby helping to protect DCOs, their members, and other market participants, and helping to mitigate the risk of market disruptions.

The Commission requests comments on the potential benefits to a DCO in complying with all aspects of proposed § 39.18(e)(7), and any benefits that would be realized by members of DCOs and their customers, as well as other market participants or the financial system more broadly. The Commission specifically requests comment on alternative means to address these issues, and the benefits associated with such alternatives.

h. Regulation 39.18(e)(8)—Scope of testing and assessment

(i) Summary of Proposed Regulations

As discussed above in section II(B), proposed § 39.18(e)(8) provides that the scope for all system safeguards testing and assessment required by proposed § 39.18 must be broad enough to include all testing of automated systems, networks, and controls necessary to identify any vulnerability which, if exploited or accidentally triggered, could

enable an intruder or unauthorized user or insider to: (1) interfere with the entity's operations or with fulfillment of the entity's statutory and regulatory responsibilities; (2) impair or degrade the reliability, security, or adequate scalable capacity of the entity's automated systems; (3) add to, delete, modify, exfiltrate, or compromise the integrity of any data related to the entity's regulated activities; and (4) undertake any other unauthorized action affecting the entity's regulated activities or the hardware or software used in connection with those activities.

(ii) Costs and Benefits

The Commission believes that the costs and benefits associated with the scope for testing and assessment are generally attributable to the substantive testing requirements, and therefore, are discussed above in the cost and benefit considerations related to the rules describing the requirements for each test or assessment.

i. Regulation 39.18(e)(9)—Internal reporting and review

(i) Summary of Proposed Regulations

As discussed above in section II(C), proposed § 39.18(e)(9) provides that both the senior management and the board of directors of the DCO must receive and review reports setting forth the results of the testing and assessment required by proposed § 39.18. Moreover the DCO would be required to establish and follow appropriate procedures for the remediation of issues identified through such review, as provided in proposed § 39.18(e)(10), and for evaluation of the effectiveness of testing and assessment protocols.

(ii) Costs

As discussed above, review of system safeguard testing and assessments by senior management and the DCO's board of directors is an industry best practice and is therefore required to be conducted under current Commission regulations.[168] Accordingly, the Commission does not believe that DCOs will incur additional costs as a result of the adoption of the proposed rules.

Nevertheless, the Commission requests comment on any potential costs of proposed § 39.18(e)(9) on DCOs, including, where possible, quantitative data.

(iii) Benefits

The Commission believes that internal reporting and review are an essential component of a comprehensive and effective system safeguard program. While senior management and the DCO's board of directors may have to devote resources to reviewing testing and assessment reports, active supervision by these individuals promotes responsibility and accountability by ensuring they receive and review the results of all system safeguard testing and assessments, thereby affording them the opportunity to evaluate the effectiveness of the testing and assessment protocols. Moreover, the attention by the board of directors and senior management should help to promote a focus on such reviews and issues, and enhance communication and coordination regarding such reviews and issues among the business, technology, legal, and compliance personnel of the DCO. Such focus could cause a DCO to internalize and/or more appropriately allocate certain costs that would otherwise be borne by clearing members, customers of clearing members, and other relevant stakeholders.

[168] See supra section II.C.

Active supervision by senior management and the board of directors also promotes a more efficient, effective, and reliable DCO risk management and operating structure. Consequently, the DCO should be better positioned to strengthen the integrity, resiliency, and availability of its automated systems.

The Commission requests comments on the potential benefits to a DCO in complying with all aspects of proposed § 39.18(e)(9), and any benefits that would be realized by members of DCOs and their customers, as well as other market participants or the financial system more broadly. The Commission specifically requests comment on alternative means to address these issues, and the benefits associated with such alternatives.

j. Regulation 39.18(e)(10)—Remediation

(i) Summary of Proposed Regulations

As discussed above in section II(C), proposed § 39.18(e)(10) requires a DCO to analyze the results of the testing and assessment required by proposed § 39.18 to identify all vulnerabilities and deficiencies in its systems. The DCO would also be required to remediate those vulnerabilities and deficiencies to the extent necessary to enable the DCO to fulfill its statutory and regulatory obligations. The remediation would have to be timely in light of appropriate risk analysis with respect to the risks presented by such vulnerabilities and deficiencies.

(ii) Costs

The Commission believes that, based on a DCO's risk analysis, the DCO generally remediates the vulnerabilities and deficiencies revealed by testing and assessment in the ordinary course of business to mitigate harm to the DCO and to satisfy

current statutory and regulatory requirements. As discussed above, remediation of vulnerabilities and deficiencies revealed by cybersecurity testing is an industry best practice,[169] and DCOs are already required to comply with this requirement. Accordingly, the Commission does not believe that DCOs will incur additional costs as a result of the adoption of the proposed rules.

The Commission requests comment on any potential costs of proposed § 39.18(e)(10) on DCOs, including, where possible, quantitative data.

(iii) Benefits

The Commission believes that effective remediation is a critical component of a comprehensive and effective system safeguard program. As discussed above, the Commission believes that the remediation of vulnerabilities and deficiencies revealed by cybersecurity testing is a current industry best practice and therefore already required under current regulations. Moreover, remediation may reduce the frequency and severity of systems disruptions and breaches for DCOs. In addition, remediation helps ensure that DCOs dedicate appropriate resources to timely address system safeguard-related deficiencies and would place an emphasis on mitigating harm to market participants while promoting market integrity. Without a timely remediation requirement, the impact of the vulnerabilities or deficiencies identified by the testing or assessment could persist and have a detrimental effect on the derivatives markets generally, as well as market participants. The Commission also believes that remediation could potentially result in DCOs reviewing and revising their existing policies and procedures to ensure that they are sufficiently thorough in the context of the new regulatory requirements, which would

[169] See, e.g., FFIEC Handbook, supra note 57, at 5; see also supra section II.C.

also assist their staffs in responding appropriately to vulnerabilities or deficiencies identified by the testing and assessments.

The Commission requests comments on the potential benefits to a DCO in complying with all aspects of proposed § 39.18(e)(10), and any benefits that would be realized by members of DCOs and their customers, as well as other market participants or the financial system more broadly. The Commission specifically requests comment on alternative means to address these issues, and the benefits associated with such alternatives.

4. Section 15(a) Factors

a. Protection of Market Participants and the Public

Automated systems are critical to a DCO's operations, which provide essential counterparty credit risk protection to market participants and the investing public. Proposed § 39.18 is designed to further enhance DCOs' risk analysis programs in order to ensure that such automated systems are reliable, secure, and have an adequate scalable capacity. Accordingly, the Commission believes that the proposed rules will further help protect the derivatives markets by promoting more robust automated systems and therefore fewer disruptions and market-wide closures, systems compliance issues, and systems intrusions.

Additionally, providing the Commission with reports concerning the system safeguards testing and assessments required by the proposed regulations will further facilitate the Commission's oversight of derivatives markets, augment the Commission's efforts to monitor systemic risk, and will further the protection of market participants and

the public by helping to ensure that a DCO's automated systems are available, reliable, secure, have adequate scalable capacity, and are effectively overseen.

The costs of this proposed rulemaking would be mitigated by the countervailing benefits of improved design, more efficient and effective processes, and enhanced planning that would lead to increased safety and soundness of DCOs and the reduction of systemic risk, which protect market participants and the public from the adverse consequences that would result from a DCO's failure or a disruption in its functioning.

b. Efficiency, Competitiveness and Financial Integrity

The proposed amendments to § 39.18 would help preserve the efficiency and financial integrity of the derivatives markets by promoting comprehensive oversight and testing of a DCO's operations and automated systems. Specifically, the proposed amendments will further reduce the probability of a cyber attack that could lead to a disruption in clearing services which could, in turn, cause disruptions to the efficient functioning and financial integrity of the derivatives markets. Preventing cyber attacks could prevent monetary losses to DCOs, and thereby help protect their financial integrity.

The Commission does not anticipate the proposed amendments to have a significant impact on the competitiveness of the derivatives markets.

c. Price Discovery

The Commission does not anticipate the proposed amendments to § 39.18 to have a direct effect on the price discovery process. However, ensuring that DCOs' automated systems function properly to clear trades protects the price discovery process to the extent that a prolonged disruption or suspension in clearing at a DCO may cause potential market participants to refrain from trading.

d. Sound Risk Management Practices

The proposed amendments to § 39.18 would strengthen and promote sound risk management practices across DCOs. Specifically, the proposed amendments would build upon the current system safeguards requirements by ensuring that tests of DCOs' key system safeguards are conducted at minimum intervals and, where appropriate, by independent professionals. The applicable tests are each recognized by industry best practices as essential components of a sound risk management program. Moreover, the benefits of the proposed rules will be shared by market participants and the investing public as DCOs, by their nature, serve to provide such parties with counterparty credit risk protection.

In addition, reliably functioning computer systems and networks are crucial to comprehensive risk management, and being able to request reports of the system safeguards testing required by the proposed regulations will assist the Commission in its oversight of DCOs and will bolster the Commission's ability to assess systemic risk levels.

e. Other public interest considerations

The Commission notes the public interest in promoting and protecting public confidence in the safety and security of the financial markets. DCOs are essential to risk management in the financial markets, both systemically and on an individual firm level. Proposed § 39.18, by explicating current requirements and identifying several additional key tests and assessments, promotes the ability of DCOs to perform these functions free from disruption due to both internal and external threats to its systems.

5. Request for Comment

In addition to the requests for comment specified above, the Commission requests comment on the following:

What are the potential costs and benefits resulting from, or arising out of, requiring DCOs to comply with the proposed changes to § 39.18? In considering costs and benefits, commenters are requested to address the effect of the proposed regulation not only on a DCO, but also on the DCO's clearing members, the customers of clearing members, and the financial system more broadly. The Commission requests that, where possible, commenters provide quantitative data in their comments, particularly with respect to estimates of costs and benefits.

The Commission has identified the baseline as current regulatory requirements. Is this baseline correct? If not, what should the baseline be, and how would the alternative baseline change the costs and benefits associated with the proposed changes to § 39.18?

Do rules impose costs above those required by current system safeguards rule and identified by the Commission? Specify and provide data to support.

Do rules provide benefits above those required by current system safeguards rule and identified by the Commission? Specify and provide data to support.

Do the costs or impacts of the proposed rules differ depending on the size of a DCO? Do they differ depending on the complexity of a DCO's systems?

List of Subjects in 17 CFR Part 39

Commodity futures, Reporting and recordkeeping requirements, System safeguards.

For the reasons stated in the preamble, the Commodity Futures Trading Commission proposes to amend 17 CFR part 39 as follows:

PART 39 – DERIVATIVES CLEARING ORGANIZATIONS

1. The authority citation for part 39 continues to read as follows:

Authority: 7 U.S.C. 2, 7a-1, and 12a; 12 U.S.C. 5464; 15 U.S.C. 8325.

2. Revise § 39.18 to read as follows:

§ 39.18 System safeguards.

(a) Definitions. For purposes of this section and § 39.34:

Controls mean the safeguards or countermeasures employed by the derivatives clearing organization 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 derivatives clearing organization to fulfill its statutory and regulatory responsibilities.

Controls testing means assessment of the derivatives clearing organization's controls to determine whether such controls are implemented correctly, are operating as intended, and are enabling the derivatives clearing organization to meet the requirements established by this section.

Enterprise technology risk assessment means a written assessment that includes, but is not limited to, an analysis of threats and vulnerabilities in the context of mitigating controls. An enterprise technology risk assessment identifies, estimates, and prioritizes risks to a derivatives clearing organization's operations or assets, or to market participants, individuals, or other entities, resulting from impairment of the

confidentiality, integrity, or availability of data and information or the reliability, security, or capacity of automated systems.

External penetration testing means attempts to penetrate a derivatives clearing organization's automated systems from outside the systems' boundaries to identify and exploit vulnerabilities. Methods of conducting external penetration testing include, but are not limited to, methods for circumventing the security features of an automated system.

Internal penetration testing means attempts to penetrate a derivatives clearing organization's automated systems from inside the systems' boundaries to identify and exploit vulnerabilities. Methods of conducting internal penetration testing include, but are not limited to, methods for circumventing the security features of an automated system.

Key controls means those controls that an appropriate risk analysis determines are either critically important for effective system safeguards or intended to address risks that evolve or change more frequently and therefore require more frequent review to ensure their continuing effectiveness in addressing such risks.

Recovery time objective means the time period within which a derivatives clearing organization should be able to achieve recovery and resumption of processing, clearing, and settlement of transactions, after those capabilities become temporarily inoperable for any reason up to or including a wide-scale disruption.

Relevant area means the metropolitan or other geographic area within which a derivatives clearing organization has physical infrastructure or personnel necessary for it to conduct activities necessary to the processing, clearing, and settlement of transactions.

The term "relevant area" also includes communities economically integrated with, adjacent to, or within normal commuting distance of that metropolitan or other geographic area.

Security incident means 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.

Security incident response plan means a written plan documenting the derivatives clearing organization's policies, controls, procedures, and resources for identifying, responding to, mitigating, and recovering from security incidents, and the roles and responsibilities of its management, staff, and independent contractors in responding to security incidents. A security incident response plan may be a separate document or a business continuity-disaster recovery plan section or appendix dedicated to security incident response.

Security incident response plan testing means testing of a derivatives clearing organization's security incident response plan to determine the plan's effectiveness, identify its potential weaknesses or deficiencies, enable regular plan updating and improvement, and maintain organizational preparedness and resiliency with respect to security incidents. Methods of conducting security incident response plan testing may include, but are not limited to, checklist completion, walk-through or table-top exercises, simulations, and comprehensive exercises.

Vulnerability testing means testing of a derivatives clearing organization's automated systems to determine what information may be discoverable through a

reconnaissance analysis of those systems and what vulnerabilities may be present on those systems.

Wide-scale disruption means an event that causes a severe disruption or destruction of transportation, telecommunications, power, water, or other critical infrastructure components in a relevant area, or an event that results in an evacuation or unavailability of the population in a relevant area.

(b) Program of risk analysis and oversight—(1) General. A derivatives clearing organization shall establish and maintain a program of risk analysis and oversight with respect to its operations and automated systems to identify and minimize sources of operational risk through:

(i) The development of appropriate controls and procedures; and

(ii) The development of automated systems that are reliable, secure, and have adequate scalable capacity.

(2) Elements of program. A derivatives clearing organization's program of risk analysis and oversight with respect to its operations and automated systems, as described in paragraph (b)(1) of this section, shall address each of the following elements:

(i) Information security, including, but not limited to, controls relating to: access to systems and data (e.g., least privilege, separation of duties, account monitoring and control); user and device identification and authentication; security awareness training; audit log maintenance, monitoring, and analysis; media protection; personnel security and screening; automated system and communications protection (e.g., network port control, boundary defenses, encryption); system and information integrity (e.g., malware defenses, software integrity monitoring); vulnerability management; penetration testing;

security incident response and management; and any other elements of information security included in generally accepted best practices;

(ii) Business continuity and disaster recovery planning and resources, including, but not limited to, the controls and capabilities described in paragraph (c) of this section; and any other elements of business continuity and disaster recovery planning and resources included in generally accepted best practices;

(iii) Capacity and performance planning, including, but not limited to, controls for monitoring the derivatives clearing organization's systems to ensure adequate scalable capacity (e.g., testing, monitoring, and analysis of current and projected future capacity and performance, and of possible capacity degradation due to planned automated system changes); and any other elements of capacity and performance planning included in generally accepted best practices;

(iv) Systems operations, including, but not limited to, system maintenance; configuration management (e.g., baseline configuration, configuration change and patch management, least functionality, inventory of authorized and unauthorized devices and software); event and problem response and management; and any other elements of system operations included in generally accepted best practices;

(v) Systems development and quality assurance, including, but not limited to, requirements development; pre-production and regression testing; change management procedures and approvals; outsourcing and vendor management; training in secure coding practices; and any other elements of systems development and quality assurance included in generally accepted best practices; and

(vi) Physical security and environmental controls, including, but not limited to, physical access and monitoring; power, telecommunication, and environmental controls; fire protection; and any other elements of physical security and environmental controls included in generally accepted best practices.

(3) Standards for program. In addressing the elements listed under paragraph (b)(2) of this section, a derivatives clearing organization shall follow generally accepted standards and industry best practices with respect to the development, operation, reliability, security, and capacity of automated systems.

(4) Resources. A derivatives clearing organization shall establish and maintain resources that allow for the fulfillment of each obligation and responsibility of the derivatives clearing organization, including the daily processing, clearing, and settlement of transactions, in light of any risk to its operations and automated systems. The derivatives clearing organization shall periodically verify the adequacy of such resources.

(c) Business continuity and disaster recovery—(1) General. A derivatives clearing organization shall establish and maintain a business continuity and disaster recovery plan, emergency procedures, and physical, technological, and personnel resources sufficient to enable the timely recovery and resumption of operations and the fulfillment of each obligation and responsibility of the derivatives clearing organization, including, but not limited to, the daily processing, clearing, and settlement of transactions, following any disruption of its operations.

(2) Recovery time objective. A derivatives clearing organization's business continuity and disaster recovery plan, as described in paragraph (c)(1) of this section, shall have, and the derivatives clearing organization shall maintain physical,

technological, and personnel resources sufficient to meet, a recovery time objective of no later than the next business day following a disruption.

(3) Coordination of plans. A derivatives clearing organization shall, to the extent practicable:

(i) Coordinate its business continuity and disaster recovery plan with those of its clearing members, in a manner adequate to enable effective resumption of daily processing, clearing, and settlement of transactions following a disruption;

(ii) Initiate and coordinate periodic, synchronized testing of its business continuity and disaster recovery plan with those of its clearing members; and

(iii) Ensure that its business continuity and disaster recovery plan takes into account the plans of its providers of essential services, including telecommunications, power, and water.

(d) Outsourcing. (1) A derivatives clearing organization shall maintain the resources required under paragraphs (b)(4) and (c)(1) of this section either:

(i) Using its own employees as personnel, and property that it owns, licenses, or leases; or

(ii) Through written contractual arrangements with another derivatives clearing organization or other service provider.

(2) Retention of responsibility. A derivatives clearing organization that enters into a contractual outsourcing arrangement shall retain complete responsibility for any failure to meet the requirements specified in paragraphs (b) and (c) of this section. The derivatives clearing organization must employ personnel with the expertise necessary to enable it to supervise the service provider's delivery of the services.

(3) Testing of resources. The testing referred to in paragraph (e) of this section shall apply to all of the derivatives clearing organization's own and outsourced resources, and shall verify that all such resources will work together effectively. Where testing is required to be conducted by an independent contractor, the derivatives clearing organization shall engage a contractor that is independent from both the derivatives clearing organization and any outside service provider used to design, develop, or maintain the resources being tested.

(e) Testing—(1) General. A derivatives clearing organization shall conduct regular, periodic, and objective testing and review of:

(i) Its automated systems to ensure that they are reliable, secure, and have adequate scalable capacity; and

(ii) Its business continuity and disaster recovery capabilities, using testing protocols adequate to ensure that the derivatives clearing organization's backup resources are sufficient to meet the requirements of paragraph (c) of this section.

(2) Vulnerability testing. A derivatives clearing organization shall conduct vulnerability testing of a scope sufficient to satisfy the requirements set forth in paragraph (e)(8) of this section.

(i) A derivatives clearing organization shall conduct such vulnerability testing at a frequency determined by an appropriate risk analysis, but no less frequently than quarterly.

(ii) Such vulnerability testing shall include automated vulnerability scanning. Where indicated by appropriate risk analysis, such scanning shall be conducted on an authenticated basis, e.g., using log-in credentials. Where scanning is conducted on an

unauthenticated basis, the derivatives clearing organization shall implement effective compensating controls.

(iii) A derivatives clearing organization shall engage independent contractors to conduct two of the required quarterly vulnerability tests each year. A derivatives clearing organization may conduct other vulnerability testing by using employees of the derivatives clearing organization who are not responsible for development or operation of the systems or capabilities being tested.

(3) External penetration testing. A derivatives clearing organization shall conduct external penetration testing of a scope sufficient to satisfy the requirements set forth in paragraph (e)(8) of this section.

(i) A derivatives clearing organization shall conduct such external penetration testing at a frequency determined by an appropriate risk analysis, but no less frequently than annually.

(ii) A derivatives clearing organization shall engage independent contractors to conduct the required annual external penetration test. A derivatives clearing organization may conduct other external penetration testing by using employees of the derivatives clearing organization who are not responsible for development or operation of the systems or capabilities being tested.

(4) Internal penetration testing. A derivatives clearing organization shall conduct internal penetration testing of a scope sufficient to satisfy the requirements set forth in paragraph (e)(8) of this section.

(i) A derivatives clearing organization shall conduct such internal penetration testing at a frequency determined by an appropriate risk analysis, but no less frequently than annually.

(ii) A derivatives clearing organization shall conduct internal penetration testing by engaging independent contractors, or by using employees of the derivatives clearing organization who are not responsible for development or operation of the systems or capabilities being tested.

(5) Controls testing. A derivatives clearing organization shall conduct controls testing of a scope sufficient to satisfy the requirements set forth in paragraph (e)(8) of this section.

(i) A derivatives clearing organization shall conduct controls testing, which includes testing of each control included in its program of risk analysis and oversight, at a frequency determined by an appropriate risk analysis, but no less frequently than every two years. A derivatives clearing organization may conduct such testing on a rolling basis over the course of the period determined by such risk analysis.

(ii) A derivatives clearing organization shall engage independent contractors to test and assess the key controls, as determined by appropriate risk analysis, included in the derivatives clearing organization's program of risk analysis and oversight no less frequently than every two years. A derivatives clearing organization may conduct any other controls testing required by this section by using independent contractors or employees of the derivatives clearing organization who are not responsible for development or operation of the systems or capabilities being tested.

(6) Security incident response plan testing. A derivatives clearing organization shall conduct security incident response plan testing sufficient to satisfy the requirements set forth in paragraph (e)(8) of this section.

(i) The derivatives clearing organization shall conduct such security incident response plan testing at a frequency determined by an appropriate risk analysis, but no less frequently than annually.

(ii) The derivatives clearing organization's security incident response plan shall include, without limitation, the derivatives clearing organization's definition and classification of security incidents, its policies and procedures for reporting security incidents and for internal and external communication and information sharing regarding security incidents, and the hand-off and escalation points in its security incident response process.

(iii) The derivatives clearing organization may coordinate its security incident response plan testing with other testing required by this section or with testing of its other business continuity-disaster recovery and crisis management plans.

(iv) The derivatives clearing organization may conduct security incident response plan testing by engaging independent contractors or by using employees of the derivatives clearing organization who are not responsible for development or operation of the systems or capabilities being tested.

(7) Enterprise technology risk assessment. A derivatives clearing organization shall conduct enterprise technology risk assessments of a scope sufficient to satisfy the requirements set forth in paragraph (e)(8) of this section.

(i) A derivatives clearing organization shall conduct an enterprise technology risk assessment at a frequency determined by an appropriate risk analysis, but no less frequently than annually.

(ii) A derivatives clearing organization may conduct enterprise technology risk assessments by using independent contractors or employees of the derivatives clearing organization not responsible for development or operation of the systems or capabilities being assessed.

(8) Scope of testing and assessment. The scope of all testing and assessment required by this section shall be broad enough to include testing of all automated systems and controls necessary to identify any vulnerability which, if exploited or accidentally triggered, could enable an intruder or unauthorized user or insider to:

(i) Interfere with the derivatives clearing organization's operations or with fulfillment of its statutory and regulatory responsibilities;

(ii) Impair or degrade the reliability, security, or capacity of the derivatives clearing organization's automated systems;

(iii) Add to, delete, modify, exfiltrate, or compromise the integrity of any data related to the derivatives clearing organization's regulated activities; or

(iv) Undertake any other unauthorized action affecting the derivatives clearing organization's regulated activities or the hardware or software used in connection with those activities.

(9) Internal reporting and review. Both the senior management and the board of directors of the derivatives clearing organization shall receive and review reports setting forth the results of the testing and assessment required by this section. The derivatives

clearing organization shall establish and follow appropriate procedures for the remediation of issues identified through such review, as provided in paragraph (e)(10) of this section, and for evaluation of the effectiveness of testing and assessment protocols.

(10) Remediation. A derivatives clearing organization shall analyze the results of the testing and assessment required by this section to identify all vulnerabilities and deficiencies in its systems. The derivatives clearing organization shall remediate those vulnerabilities and deficiencies to the extent necessary to enable the derivatives clearing organization to fulfill the requirements of this chapter and meet its statutory and regulatory obligations. Such remediation must be timely in light of appropriate risk analysis with respect to the risks presented by such vulnerabilities and deficiencies.

(f) Recordkeeping. A derivatives clearing organization shall maintain, and provide to staff of the Division of Clearing and Risk, or any successor division, promptly upon request, pursuant to § 1.31 of this chapter:

(1) Current copies of the derivatives clearing organization's business continuity and disaster recovery plan and other emergency procedures. Such plan and procedures shall be updated at a frequency determined by an appropriate risk analysis, but no less frequently than annually;

(2) All assessments of the derivatives clearing organization's operational risks or system safeguards-related controls;

(3) All reports concerning testing and assessment required by this section, whether conducted by independent contractors or by employees of the derivatives clearing organization; and

(4) All other documents requested by staff of the Division of Clearing and Risk, or any successor division, in connection with Commission oversight of system safeguards pursuant to the Act or Commission regulations, or in connection with Commission maintenance of a current profile of the derivatives clearing organization's automated systems.

(5) Nothing in this paragraph (f) of this section shall be interpreted as reducing or limiting in any way a derivatives clearing organization's obligation to comply with § 1.31 of this chapter.

(g) Notice of exceptional events. A derivatives clearing organization shall notify staff of the Division of Clearing and Risk, or any successor division, promptly of:

(1) Any hardware or software malfunction, security incident, or targeted threat that materially impairs, or creates a significant likelihood of material impairment, of automated system operation, reliability, security, or capacity; or

(2) Any activation of the derivatives clearing organization's business continuity and disaster recovery plan.

(h) Notice of planned changes. A derivatives clearing organization shall provide staff of the Division of Clearing and Risk, or any successor division, timely advance notice of all material:

(1) Planned changes to the derivatives clearing organization's automated systems that may impact the reliability, security, or capacity of such systems; and

(2) Planned changes to the derivatives clearing organization's program of risk analysis and oversight.

3. Revise paragraphs (a), (b)(3), and (c) of § 39.34 to read as follows:

§ 39.34 System safeguards for systemically important derivatives clearing organizations and subpart C derivatives clearing organizations.

(a) Notwithstanding § 39.18(c)(2), the business continuity and disaster recovery plan described in § 39.18(c)(1) for each systemically important derivatives clearing organization and subpart C derivatives clearing organization shall have the objective of enabling, and the physical, technological, and personnel resources described in § 39.18(c)(1) shall be sufficient to enable, the systemically important derivatives clearing organization or subpart C derivatives clearing organization to recover its operations and resume daily processing, clearing, and settlement no later than two hours following the disruption, for any disruption including a wide-scale disruption.

(b) * * *

(3) The provisions of § 39.18(d) shall apply to these resource requirements.

(c) Each systemically important derivatives clearing organization and subpart C derivatives clearing organization must conduct regular, periodic tests of its business continuity and disaster recovery plans and resources and its capacity to achieve the required recovery time objective in the event of a wide-scale disruption. The provisions of § 39.18(e) shall apply to such testing.

* * * * *

Issued in Washington, DC, on December 17, 2015, by the Commission.

Christopher J. Kirkpatrick,

Secretary of the Commission.

NOTE: The following appendices will not appear in the Code of Federal Regulations.

Appendices to System Safeguards Testing Requirements for Derivatives Clearing Organizations – Commission Voting Summary, Chairman's Statement, and Commissioner's Statement

Appendix 1 – Commission Voting Summary

On this matter, Chairman Massad and Commissioners Bowen and Giancarlo voted in the affirmative. No Commissioner voted in the negative.

Appendix 2 – Statement of Chairman Timothy G. Massad

I strongly support this proposed rule.

The risk of cyberattacks is perhaps the most important single issue we face in terms of financial market stability and integrity.

The examples of cyberattacks or significant technological disruptions from inside and outside the financial sector are all too frequent and familiar.

Today, the aims of these attacks can go beyond traditional financial motives. Today, we must be concerned about the possibility of attacks intended to destroy information and disrupt or destabilize our markets.

The risk to American businesses and the economy is dramatic. And the interconnectedness of our financial institutions and markets means that a failure in one institution can have significant repercussions throughout the system.

The proposed rule that we are issuing today is an important step toward enhancing the protections in our markets. It builds on our core principles – which already require clearinghouses to focus on system safeguards – by setting standards consistent with best practices. It requires robust testing of cyber protections, setting forth the types of testing

that must be conducted, the frequency of testing and whether tests should be conducted by independent parties. In addition, it enhances standards for incident response planning and enterprise technology risk assessments.

Our requirements should come as no surprise – clearinghouses should already be doing extensive testing. Indeed, we hope that today's proposal sets a baseline that is already being met.

The proposal also complements what we as a Commission already do. We focus on these issues in our examinations to determine whether an institution is following good practices and paying adequate attention to these risks at the board level and on down.

This rule is largely in line with another system safeguards proposal that the Commission also approved today, which applies the same standards to other critical market infrastructure.

Since the 2009 G-20 agreement and the enactment of Dodd-Frank, clearinghouses have become increasingly important the financial system. As a result, I believe we must do all we can to ensure their strength and stability. This proposed rule is a critical component of this effort.

I thank the staff for their hard work on this proposal. Of course, we welcome public comment on both our system safeguards proposals, which will be carefully taken into account before we take any final action.

Appendix 3 – Statement of Commissioner Sharon Y. Bowen

Today, we are considering two rule proposals that address an issue which is right at the heart of systemic risk in our markets – cybersecurity. The question that we face is: with a problem as immense as cybercrime, and the many measures already being

employed to combat it, what would today's proposed rules accomplish? In answer to that question, I want to say a few words about our cybercrime challenge, what is currently being done to address it, and what I hope these proposed regulations would add to these efforts.

The problem is clear – our firms are facing an unrelenting onslaught of attacks from hackers with a number of motives ranging from petty fraud to international cyberwarfare. We have all heard of notable and sizable companies that have been the victim of cybercrime, including: Sony, eBay, JPMorgan, Target, and Staples – even the US government has fallen victim.

In recent testimony before the House Committee on Financial Services, Subcommittee on Oversight and Investigations about cybercrime, the Director of the Center for Cyber and Homeland Security noted that the "U.S. financial services sector in particular is in the crosshairs as a primary target."[1] He cited one US bank which stated that it faced 30,000 cyber-attacks in one week – averaging an attack every 34 seconds.[2]

Given the magnitude of the problem, it is not at all surprising that a lot is already being done to address it. The Department of Homeland Security and others have been working with private firms to shore up defenses. Regulators have certainly been active. The Securities and Exchange Commission (SEC), the Federal Deposit Insurance

---

[1] Testimony of Frank J. Cilluffo, Director, Center for Cyber and Homeland Security, Before the U.S. House of Representatives, Committee on Financial Services, Subcommittee on Oversight and Investigations, 1 (June 16, 2015) (noting that "the following figures which were provided to me recently by a major U.S. bank on a not-for-attribution basis: just last week, they faced 30,000 cyber-attacks. This amounts to an attack every 34 seconds, each and every day. And these are just the attacks that the bank actually knows about, by virtue of a known malicious signature or IP address. As for the source of the known attacks, approximately 22,000 came from criminal organizations; and 400 from nation-states."), available at https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/A%20Global%20Perspective%20on%20Cyber%20Threats%20-%2015%20June%202015.pdf.

[2] Id.

Corporation (FDIC), the Federal Reserve Board (FRB), the Federal Housing Finance Agency (FHFA), and our self-regulatory organization, the National Futures Association (NFA), have issued cybersecurity guidance. In Europe, the Bank of England (BOE) introduced the CBEST program to conduct penetration testing on firms, based on the latest data on cybercrime. We heard a presentation from the BOE about CBEST at a meeting of the Market Risk Advisory Committee this year.

I wanted to hear what market participants were doing to address the challenge of our cybersecurity landscape so I met with several of our large registrant dealers and asked them about their cybersecurity efforts. After these discussions, I was both alarmed by the immensity of the problem and heartened by efforts of these larger participants to meet that problem head on. They were employing best practices such as reviewing the practices of their third party providers, using third parties to audit systems, sharing information with other market participants, integrating cybersecurity risk management into their governance structure, and staying in communication with their regulators.

We have also been vigilant in our efforts to address cybersecurity. Under our current rule structure, many of our registrants have system safeguards requirements. They require, among other things, that the registrants have policies and resources for risk analysis and oversight with respect to their operations and automated systems, as well as reporting, recordkeeping, testing, and coordination with service providers. These requirements clearly include appropriate cybersecurity measures. We also regularly examine registrants for their adherence to the system safeguards requirements, including effective governance, use of resources, appropriate policies, and vigilant response to attacks.

So if all of this is happening, what would more regulation accomplish? In other words, what is the "value add" of the rules being proposed today? The answer is: a great deal. While some firms are clearly engaging in best practices, we have no guarantee that all of them are. And as I have said before, in a system as electronically interconnected as our financial markets, "we're collectively only as strong as our weakest link, and so we need a high baseline level of protection for everyone…"[3] We need to incentivize all firms under our purview to engage in these effective practices.

We have to do this carefully though because once a regulator inserts itself into the cybersecurity landscape at a firm – the firm now has two concerns: not just fighting the attackers, but managing its reputation with its regulator. So, if not done carefully, a regulator's attempt to bolster cybersecurity at a firm can instead undermine it by incentivizing the firm to cover up any weaknesses in its cybersecurity infrastructure, instead of addressing them. Further, we must be careful not to mandate a one-size-fits-all standard because firms are different. Thus, we must be thoughtful about how to engage on this issue. We need to encourage best practices, while not hampering firms' ability to customize their risk management plan to address their cybersecurity threats.

I think these rulemakings are a great first step in accomplishing that balance. There are many aspects of these proposals that I like. First, they set up a comprehensive testing regime by: (a) defining the types of cybersecurity testing essential to fulfilling system safeguards testing obligations, including vulnerability testing, penetration testing, controls testing, security incident response plan testing, and enterprise technology risk

[3] Commissioner Sharon Y. Bowen, Commodity Futures Trading Commission, "Remarks of CFTC Commissioner Sharon Y. Bowen Before the 17th Annual OpRisk North America," March 25, 2015, available at http://www.cftc.gov/PressRoom/SpeechesTestimony/opabowen-2.

assessment; (b) requiring internal reporting and review of testing results; and (c) mandating remediation of vulnerabilities and deficiencies. Further, for certain significant entities, based on trading volume, it requires heightened measures such as minimum frequency requirements for conducting certain testing, and specific requirements for the use of independent contractors.

Second, there is a focus on governance – requiring, for instance, that firms' Board of Directors receive and review all reports setting forth the results of all testing. And third, these rulemakings are largely based on well-regarded, accepted best practices for cybersecurity, including The National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity ("NIST Framework").[4]

In all, I think the staff has put together two thoughtful proposals. Clearly, however, this is only a first step since all our registrants, not just exchanges, SEFs, SDRs and DCOs, need to have clear cybersecurity measures in place. I am also very eager to hear what the general public has to say about these proposals. Do they go far enough to incentivize appropriate cybersecurity measures? Are they too burdensome for firms that do not pose significant risk to the system? And given that this is a dynamic field with a constantly evolving set of threats, what next steps should we take to address cybercrime? Please send in all your thoughts for our consideration.

[4] NIST Framework, Subcategory PR.IP-10, at 28, and Category DE.DP, at 31, available at http://www.nist.gov/ cyberframework/upload/cybersecurity-framework-021214.pdf.

[FR Doc. 2015-32144 Filed: 12/22/2015 8:45 am; Publication Date: 12/23/2015]