This document is scheduled to be published in the
Federal Register on 09/19/2016 and available online at
https://federalregister.gov/d/2016-22413, and on **FDsys.gov**

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: Final rule.

SUMMARY: The Commodity Futures Trading Commission ("Commission") is adopting enhanced requirements for testing by a derivatives clearing organization ("DCO") 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: Effective date: This rule is effective September 19, 2016.

Compliance dates: DCOs must comply with § 39.18(e)(2) and (6) by March 20, 2017; § 39.18(e)(3) through (5), and (7) by September 19, 2017; and all other provisions of § 39.18 by September 19, 2016.

FOR FURTHER INFORMATION CONTACT: Eileen A. Donovan, Deputy Director, 202-418-5096, edonovan@cftc.gov, 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; Tad Polley, Associate Director, (312) 596-0551, tpolley@cftc.gov; or Scott Sloan, Attorney-Advisor, (312) 596-0708, ssloan@cftc.gov, 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 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, including additional system safeguards requirements,[4] 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").[5]

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 responsibilities, obligations, and recovery time objective of a DCO following a disruption

[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.

[4] 17 CFR 39.34.

[5] Derivatives Clearing Organizations and International Standards, 78 FR 72476 (Dec. 2, 2013) (codified at 17 CFR part 39).

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.

On December 23, 2015, the Commission proposed to enhance its system safeguards requirements for DCOs by revising § 39.18 to require specific types of testing, and specifying the minimum frequency with which such testing must be performed. The Commission also proposed additional amendments to reorder and renumber certain paragraphs and make other minor changes to improve the clarity of the rule text, as well as corresponding technical corrections to § 39.34 (the "Proposal").[6]

The comment period for the Proposal ended on February 22, 2016. The Commission received seven substantive comment letters in response to the Proposal[7] and, in consideration of those comments, is adopting the Proposal subject to certain changes, as noted below.

B. Need for Cybersecurity Testing

In the Proposal, the Commission described the well-documented increase in cyber threats, and the need to enhance its existing requirements for cybersecurity testing in light of this increase.[8] 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

[6] See System Safeguards Testing Requirements for Derivatives Clearing Organizations; Proposed Rule, 80 FR 80114 (Dec. 3, 2015) (to be codified at 17 CFR part 39).

[7] All comment letters are available through the Commission's website at: http://comments.cftc.gov/PublicComments/CommentList.aspx?id=1649. The Commission received comments from the following parties: Intercontinental Exchange, Inc.; NGX; The Options Clearing Corporation; Minneapolis Grain Exchange; North American Derivatives Exchange; LCH.Clearnet Group; and CME Group, Inc.

[8] 80 FR 80114, at 80114-80115.

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.

Cybersecurity testing is a well-established best practice generally and for financial sector entities. 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.[9] 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.[10] The Federal Financial Institutions Examination Council ("FFIEC"),[11] another important source of cybersecurity best practices for financial sector entities, notes that financial institutions should have a testing plan that identifies control objectives; schedules tests of the controls used to meet those objectives; ensures prompt corrective

[9] 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.

[10] 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.

[11] 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.

action where deficiencies are identified; and provides independent assurance for compliance with security policies.[12]

The Commission 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. This requirement must be satisfied by following, at a minimum, generally accepted standards and industry best practices. The final rule being adopted by the Commission herein clarify these requirements by identifying particular types of testing required by relevant generally accepted standards and industry best practices. The Commission is requiring that independent contractors conduct certain testing and specifying a minimum frequency for each testing type, but otherwise is not changing the regulatory requirement for DCOs as it exists today. The additional clarity provided by the specific testing and frequency requirements as well as the independent contractor requirements will help DCOs increase their cyber resiliency and operate in a safe and efficient manner.

II. Comments on the Notice of Proposed Rulemaking

A. Vulnerability Testing

Proposed § 39.18(a) would define "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. Proposed § 39.18(e)(2) would require the testing to be of a scope sufficient to satisfy the testing scope requirements of proposed § 39.18(e)(8). Proposed

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

§ 39.18(e)(2)(i) would require a DCO to conduct vulnerability testing at a frequency determined by an appropriate risk analysis, but at a minimum no less frequently than quarterly. Under proposed § 39.18(e)(2)(ii), the vulnerability tests would have to include automated vulnerability scanning, which would have to be conducted on an authenticated basis where indicated by an appropriate risk analysis. Proposed § 39.18(e)(2)(iii) would require a DCO to engage independent contractors to conduct two of the required quarterly tests each year. The other vulnerability tests could be conducted by employees of the DCO who are not responsible for development or operation of the systems or capabilities being tested.

1. Frequency

CME Group, Inc. ("CME") supported the proposed frequency for the required vulnerability testing. CME stated that testing on at least a quarterly basis is likely an appropriate frequency for most organizations for their most critical assets. Intercontinental Exchange, Inc. ("ICE") supported a quarterly requirement, but believes that DCOs that meet the quarterly requirement should not be subject to a formal risk assessment to potentially determine a higher testing frequency as the Commission has not provided evidence that a higher frequency is warranted.

Minneapolis Grain Exchange ("MGEX") stated that frequency of testing should be determined by the frequency of system changes and the scope of exposure, and should not be reduced to a static minimum. NGX stated that quarterly vulnerability testing is too costly for smaller DCOs, and should be required semi-annually instead.

The Commission does not believe it is prudent to change the frequency requirement for vulnerability tests. The requirement to conduct vulnerability tests at a

frequency based on a risk analysis and at least quarterly is based on industry standards[13] and will help ensure that DCOs are responsive to new vulnerabilities as they arise.

2. Risk Assessment

North American Derivatives Exchange, Inc. ("Nadex") stated that the rule should be clarified to provide that the expected level of detail contained in the risk analysis used to determine the required frequency of overall testing should be based on what is considered reasonable in the industry. The Commission does not believe a clarification is necessary because the rule as proposed is appropriately based on industry standards.[14]

3. Authenticated Scanning

ICE argued that the Commission should eliminate the authenticated vulnerability scanning requirement on the basis that it will increase the cost and time of a scan, increase risk by requiring an operating system login to be created and maintained on a new system, and increase the quantity of findings, potentially diluting and obscuring important results.

The Commission agrees with ICE that an explicit requirement for authenticated scanning should be removed from the regulation. Therefore, the Commission is revising proposed § 39.18(e)(2)(ii) as follows (added text in italics), "Such vulnerability testing shall include automated vulnerability scanning*,* which shall follow generally accepted

[13] 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; Security Standards Council, Payment Card Industry Data Security Standards, Apr. 2016, v. 3.2 ("PCI-DSS"), p. 98, available at: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf; FFIEC, Information Security Booklet, IT Examination Handbook, July 2006 ("FFIEC Handbook"), p. 82, available at: http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_InformationSecurity.pdf.

[14] See FFIEC Handbook, supra note 13, at 82.

best practices." The regulation as adopted thus only requires authenticated scanning to the extent it is required by industry standards.

4. Independence Requirements

Several DCOs did not support the independent contractor requirement, arguing that internal teams should be allowed to conduct vulnerability testing. ICE noted that internal parties have the most knowledge and experience with the systems.

CME, ICE, and MGEX argued that there are inherent risks in providing outside parties access to critical systems and sensitive information. Specifically, MGEX stated that it is concerned about the breadth and volume of proprietary information that vendors would have access to in order to perform the testing required, because having vast quantities of industry information in the hands of vendors may actually cause greater risk of harm as vendors may be at greater risk of a cyber incident.

ICE, LCH.Clearnet Group ("LCH"), The Options Clearing Corporation ("OCC"), and MGEX all noted significant costs associated with hiring outside contractors to conduct vulnerability tests. LCH and MGEX further stated that this requirement is especially burdensome to smaller DCOs.

MGEX opposed the proposed requirement that only independent contractors or employees who are not responsible for development or operation of the systems or capabilities being tested may conduct vulnerability testing. Specifically, MGEX stated that smaller organizations like itself may not have qualified individuals outside of the IT department who would have the needed background and skills while also having the level of independence which the Commission would require. Therefore, an entity like MGEX would be forced to either bear significant cost to hire dedicated employees exclusively

for regulatory testing compliance or bear significant cost to have independent contractors perform all four tests.

OCC believes that requiring a DCO to use an independent contractor to perform vulnerability testing during the same year that such person is performing external penetration testing would unnecessarily increase costs without an added benefit, because vulnerability testing is largely subsumed within external penetration testing.

As explained in the Proposal, the Commission believes it is important that vulnerability testing be conducted from the perspective of an outsider, and as a result does not agree with MGEX that internal employees responsible for development or operation of the tested systems or capabilities should be permitted to conduct the tests. The Commission agrees with various commenters, however, that the regulation should permit but not require a DCO to use independent contractors to conduct the required vulnerability testing. As a result, the Commission is revising proposed § 39.18(e)(2)(iii) as follows (added text in italics), "A derivatives clearing organization shall conduct vulnerability 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." This revision aligns the regulation more closely with industry standards, which call for vulnerability testing to be conducted by independent employees while recognizing the benefits and potential risks of engaging independent contractors.[15]

[15] FFIEC Handbook, supra note 13, at 81 (calling for such tests to be performed "by individuals who are also independent of the design, installation, maintenance, and operation of the tested system"); NIST Special Publication 800-115, Technical Guide to Information Security Testing and Assessment, Sept. 2008 ("NIST SP 800-115"), p. 6-6, available at: http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf (recognizing the benefits and risks of engaging third parties to conduct testing).

B. External Penetration Testing

Proposed § 39.18(a) would define "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) would require the 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 would also provide that independent contractors must perform the required annual external penetration test on behalf of the DCO. However, other external penetration testing could be performed by appropriately qualified DCO employees not responsible for development or operation of the systems or capabilities being tested.

ICE and Nadex supported requiring external penetration testing as a part of a DCO's program of risk analysis and oversight. OCC generally supported external penetration testing by independent third parties. ICE and CME supported performing the testing annually.

ICE suggested that the Commission should amend the definition of "external penetration testing" to include specific types of testing. The Commission is declining to do so. Requiring specific tests would be overly prescriptive and could stifle the development of new, more advanced testing methods. Accordingly, upon review of the comments, the Commission is adopting § 39.18(e)(3) and the definition of "external penetration testing" as proposed.

C. Internal Penetration Testing

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

ICE and Nadex supported requiring internal penetration testing as a part of a DCO's program of risk analysis and oversight.

ICE suggested that the Commission should amend the definition of "internal penetration testing" to include specific types of testing. As with external penetration testing, the Commission is declining to require specific forms of internal penetration tests. Requiring specific tests would be overly prescriptive and could stifle the development of new, more advanced testing methods.

CME stated that DCOs may find it challenging to recruit and retain employees capable of conducting internal penetration testing without introducing unnecessary risks into production and other sensitive environments, because there is a scarcity of qualified professionals with those skills. As a result, CME argued the Commission should clarify that conducting annual internal penetration tests should be an objective, and not a strict requirement, so that DCOs can prioritize effective testing done by independent employees over conducting testing at least annually simply to comply with a prescriptive

testing frequency requirement. ICE stated that the Commission should be silent on parameters for voluntary internal testing, allowing each DCO to determine its own methodology for such testing.

The Commission disagrees with CME's suggestion that internal penetration testing should be merely an objective. The requirement for internal penetration testing is based on industry standards.[16] In addition, because the regulation provides sufficient flexibility regarding the individuals who are permitted to conduct the internal penetration tests, the Commission does not believe a change to the regulation based on CME's comment is necessary. In response to ICE's comment regarding voluntary internal testing, the Commission notes that the final rule does not impose any requirements on testing DCOs conduct on a voluntary basis, beyond the requirements of the regulation. Therefore, the Commission declines to make any changes in response to these comments and confirms that final § 39.18(e)(4) sets forth requirements rather than objectives or a voluntary program.

MGEX stated that the required frequency of testing should be determined by the frequency of systems changes and the scope of exposure, and should not be reduced to a static minimum. The Commission declines to amend the regulation in response to MGEX's comment, and notes that that the frequency requirement in final § 39.18(e)(4)(i) is based on industry standards and is not overly prescriptive.[17]

Accordingly, upon review of the comments, the Commission is adopting § 39.18(e)(4) and the definition of "internal penetration testing" as proposed.

[16] See NIST SP 800-115, supra note 15, at 2-5.
[17] See id.; FFIEC Handbook, supra note 13, at 82.

D. Controls Testing

Proposed § 39.18(a) would define "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 § 39.18. Proposed § 39.18(e)(5) would require 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 would be 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. A DCO 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.

CME and Nadex supported requiring controls testing as a part of a DCO's program of risk analysis and oversight.

ICE recommended that the Commission remove the controls testing requirements and the definition of "key controls." ICE stated that attempting to mandate controls testing will result in inconsistent and confused implementation, distract from useful

security activity, and generate a superset of results that are already published in a more focused fashion through vulnerability, external penetration, internal penetration, or security response plan testing. Moreover, ICE believes that the proposed controls testing requirements are already adequately addressed in existing rules, both in the U.S. and globally, and through current examination coverage. ICE added that the concept of a key control is not universally adopted, and that the goal is not to test such controls, but to eliminate reliance on them. ICE believes that the key controls proposal imposes a large burden for little to no practical improvement in security.

Despite ICE's comments, the Commission is adopting the controls testing requirement, which is based on industry standards.[18] The Commission continues to believe that regular, ongoing testing of all of an organization's system safeguards-related controls is a crucial part of a DCO's risk analysis and oversight program. As NIST notes, 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.[19] The Commission notes that the definition of "key controls" provides adequate flexibility for a DCO to determine which of its controls constitute key controls. While ICE believes that the goal should be to eliminate reliance on key controls, the

[18] See, NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, rev. 4 ("NIST SP 800-53"), pp. app. F-CA at F-55, available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.; FFIEC Handbook, supra note 13, at 12.

[19] 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.

Commission believes that so long as DCOs continue to rely on them, it is crucial for DCOs to test their effectiveness.

1. Frequency

CME and OCC stated that the costs of requiring controls testing every two years outweigh the benefits. CME stated that DCOs should be able to test in line with their risk analysis, which may result in a cycle of longer than two years. CME stated that a three-year cycle requirement would be more appropriate.

OCC agreed with the proposed testing frequency as applied to key controls. However, OCC stated that, consistent with relevant industry best practices, the Commission should alternatively consider permitting a DCO to determine the frequency of controls testing based on the level of risk a control is determined to present following an appropriate controls risk analysis.

The Commission agrees with CME and OCC that requiring controls testing no less frequently than every two years is not necessary. The Commission further agrees with CME that three years is a more appropriate minimum requirement and is revising proposed § 39.18(e)(5)(i) as follows (added text in italics), "A [DCO] 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 shall test and assess key controls no less frequently than every three years. A [DCO] may conduct such testing on a rolling basis over the course of the required period." The final rule would thus require key controls testing to occur at least every three years rather than every two and would not prescribe a minimum frequency for testing of non-key controls. The Commission reiterates, however, that if a DCO's risk analysis indicates a key control

should be tested more frequently than every three years, the DCO must comply with the shorter testing frequency. The changes would further clarify that both key controls and non-key controls can be tested on a rolling basis over the applicable time period.

2. Independence Requirements

CME stated that requiring non-employee independent contractors to test key controls, without involvement by employees, may not provide the most effective or efficient means for continued key controls testing and enhancement. CME also stated that internal audit staff can provide a strong and independent third line of defense where the department is independent from management, objective in its findings, professional, and able to have free and unlimited access to the books, records, and people of a company. CME further stated that while involving external resources may be beneficial, doing so should not exclude participation by employees not involved in the development or operation of the controls, systems, or capabilities being tested.

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

The Commission believes that independent testing provides critical impartiality and credibility, and notes that generally accepted best practices recognize the benefits of using independent contractors.[20] The Commission is clarifying, however, that when a DCO must engage independent contractors to conduct key controls testing, those independent contractors may consult with independent employees of the DCO when conducting the required testing so long as they produce an independent report.

Based on the changes to proposed § 39.18(e)(5)(i), the Commission is revising proposed § 39.18(e)(5)(ii) in part as follows (added text in italics), "A [DCO] shall engage independent contractors to test and assess the key controls included in the [DCO]'s program of risk analysis and oversight no less frequently than every three years." The regulation as finalized would thus require a DCO to engage independent contractors to test each key control at least every three years. If, however, a DCO's risk analysis concludes that certain key controls must be tested more frequently than every three years, the resulting additional tests may be conducted by independent contractors or employees of the DCO who are not responsible for development or operation of the systems or capabilities being tested.

E. Security Incident Response Plan Testing

Proposed § 39.18(a) would define "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

[20] NIST SP 800-115, supra note 15, 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); FFIEC Handbook, supra note 13, at 81.

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 a DCO to conduct the 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 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. Proposed § 39.18(e)(6)(iii) would also permit the DCO to coordinate its security incident response plan testing with other testing required by the regulation 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 employees who are not responsible for development or operation of the systems or capabilities being tested.

CME, ICE, and Nadex supported requiring security incident response plan testing as a part of a DCO's program of risk analysis and oversight.

CME stated that employees responsible for incident response, who would not be responsible for the development or operation of the functional systems or capabilities being tested, should be permitted to both design a DCO's plan and be responsible for testing the plan. CME stated that a DCO should be able to leverage its employees with

expertise in crisis and risk management, and incident response and planning, for both planning and testing purposes.

The Commission agrees with CME that the employees who develop a security incident response plan should be permitted to test the plan. To allow DCOs additional flexibility regarding security incident response plan testing, the Commission is revising proposed § 39.18(e)(6)(iv) by deleting "who are not responsible for development or operation of the systems or capabilities being tested." This revision allows security incident response plan testing to be conducted by either independent contractors or employees, without restricting which employees may lead or conduct the testing.

OCC noted that under the proposed rules, "security incident" is defined as "a cybersecurity or physical security event that actually or potentially jeopardizes automated system operation, reliability, security, or capacity, or the availability, confidentiality or integrity of data." OCC argued that the inclusion of the term "potentially" renders the definition vague, and could be interpreted to include most, if not all, cybersecurity events experienced by a DCO. OCC suggested that the Commission revise its definition to either: (i) defer to the DCO's definition as set forth in its risk analysis plan; or (ii) replace "potentially jeopardizes" with "has a significant likelihood of jeopardizing."

The Commission recognizes OCC's concern and is amending the proposed definition of "security incident" as follows (added text in italics), "Security incident means a cybersecurity or physical security event that actually <u>jeopardizes</u> or <u>has a significant likelihood of jeopardizing</u> automated system operation, reliability, security, or capacity, or the availability, confidentiality or integrity of data." This change provides

additional clarity regarding which cybersecurity events are considered a security incident for the purposes of the regulation.

F. Enterprise Technology Risk Assessment

Proposed § 39.18(a) would define 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) would also provide 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) would require such assessment to be of a scope sufficient to satisfy the requirements of proposed § 39.18(e)(8). Proposed § 39.18(e)(7)(i) would require 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) would permit a DCO to 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.

Nadex requested that the Commission clarify whether information related to the enterprise technology risk assessment could be combined with the regular testing results presented to management and the board of directors based on the internal reporting and review requirements.

In response to Nadex's comment, the Commission is clarifying that the information required under the regulation can be presented to management and the board

of directors in the manner each DCO deems appropriate, including by presenting it together with other information DCOs must provide to management and the board of directors.

1. Frequency

ICE recommended that the Commission not adopt the enterprise technology risk assessment requirements. ICE stated that attempting to mandate enterprise technology risk assessments will result in inconsistent and confused implementation, distract from useful security activity, and generate a superset of results that are already published in a more focused fashion through vulnerability, external penetration, internal penetration or security response plan testing. Moreover, ICE believes that the proposed enterprise technology risk assessment requirements are already adequately addressed in existing rules, both in the U.S. and globally, and through current examination coverage.

CME supported requiring DCOs to conduct an enterprise technology risk assessment as a part of a DCO's program of risk analysis and oversight, but believes an assessment should be required at least every two years, rather than annually, to match the controls testing cycle.

The Commission is adopting the enterprise technology risk assessment requirements generally as proposed. The regulation is based on industry standards[21] and will help each DCO produce a broad determination of its system safeguards-related risks, regardless of the source of the risks.

The Commission is, however, revising proposed § 39.18(e)(7)(i) to read as follows (added text in italics), "A [DCO] shall conduct an enterprise technology risk

[21] See PCI-DSS, supra note 13, at 105; FINRA Report, supra note 10, at 14.

assessment at a frequency determined by an appropriate risk analysis, but no less frequently than annually. A [DCO] that has conducted an enterprise technology risk assessment that complies with this section may conduct subsequent assessments by updating the previous assessment." This change responds to a comment received by the Commission on its system safeguards proposal for DCMs and SDRs[22] and clarifies that the required enterprise technology risk assessment may build upon previous assessments. The comment noted the burden and cost of an annual full assessment, and the Commission believes this is a reasonable means to reduce both.

2. Independence Requirements

CME suggested that the Commission permit DCOs to allow internal groups outside of the enterprise risk management function to handle components of the enterprise technology risk assessment.

ICE stated that the enterprise technology risk assessment should be the function of an enterprise risk program separate from the information security groups.

In response to the comments, the Commission emphasizes that the final regulation provides flexibility regarding who may conduct the enterprise technology risk assessment. If a DCO chooses not to use independent contractors, the enterprise technology risk assessment may be conducted by employees who are not responsible for the development or operation of the systems or capabilities being assessed.

G. Scope of Testing

[22] Tradeweb Markets, LLC, Comment Letter on System Safeguards Testing Requirements Proposed Rule (Feb. 22, 2016), http://comments.cftc.gov/PublicComments/ViewComment.aspx?id=60657&SearchText.

Proposed § 39.18(e)(8) would provide that the scope of all system safeguards testing and assessment required by § 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; or (4) undertake any other unauthorized action affecting the entity's regulated activities or the hardware or software used in connection with those activities.

CME and Nadex stated that the requirement to identify "any vulnerability" that could compromise "any data," or allow an intruder to undertake "any other unauthorized action" is too broad. CME argued that in being so broad, the Commission undermines the value of a risk-based approach. Nadex suggested that the proposed requirement be amended to limit responsibility to a reasonableness standard.

The Commission agrees that the proposed language is overly broad and undermines a risk-based approach to system safeguards testing. Therefore, the Commission is revising proposed § 39.18(e)(8) as follows (added text in italics), "The scope of testing and assessment required by this section shall be broad enough to include the testing of automated systems and controls that a [DCO]'s required program of risk analysis and oversight and its current cybersecurity threat analysis indicate is necessary to identify risks and vulnerabilities that could enable an intruder or unauthorized user or insider. . . ." The revisions reinforce a risk-based approach to system safeguards testing

by basing the scope of testing on the DCO's program of risk analysis and oversight and current cybersecurity threat assessment.

Nadex noted that the "current cybersecurity threat analysis" the DCO would use to assess its possible adversaries' capabilities could be interpreted to include not only the DCO's internal risk assessment, but also warnings/notices generated from third party entities. Nadex requested that the Commission confirm that the "current cybersecurity threat analysis" refers only to the DCO's internal risk assessment.

The Commission does not believe that a DCO preparing a cybersecurity threat assessment can appropriately ignore available external warnings or notices. Thus, contrary to Nadex's recommendation, the Commission is clarifying that a DCO is required to consider reasonably available external analyses when preparing a current cybersecurity threat assessment.

CME stated that adopting regulations requiring DCOs to identify "any vulnerability" underlies an assumption that DCOs falling victim to the most sophisticated threats are singularly responsible for being attacked. Therefore, CME recommended that the Commission adopt safe harbors for DCOs who seek to comply with their core principle responsibilities in order to encourage DCOs to seek out partnerships and best serve the common goal of improving the industry's overall state of cyber resilience.

In light of the revisions to proposed § 39.18(e)(8) discussed above, the Commission declines to provide a "safe harbor" for DCOs "who seek to comply with their core principle responsibilities." As the revisions make clear, the Commission is not seeking to hold DCOs strictly liable for every cyber attack they might face.

H. Internal Reporting and Review

Proposed § 39.18(e)(9) would provide 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 § 39.18. Moreover, the DCO would be required to establish and follow appropriate procedures for the remediation of issues identified through this review, as provided in proposed § 39.18(e)(10), and for evaluation of the effectiveness of testing and assessment protocols.

Nadex stated that reports generated based on system testing are often lengthy and technical, and that requiring management and the board to review technical testing results would require individuals in those positions to have a level of technical knowledge and sophistication that may not otherwise be required of the position. Therefore, Nadex requested that the Commission clarify whether a narrative executive summary would satisfy the proposed requirement. Additionally, Nadex requested that the Commission clarify whether the reports may be presented to the board at its regularly scheduled quarterly meetings.

CME, MGEX, and OCC stated that a DCO's board of directors should be able to delegate the review required by proposed § 39.18(e)(9) to a board-level committee.

In response to Nadex, the Commission notes that providing a DCO's board with a narrative executive summary is not sufficient to satisfy the requirements of the regulation. Consistent with generally accepted best practices, the final regulation requires that the board must instead receive and review the technical reports containing testing results and assessments.[23] To the extent there is concern regarding management's or the board of directors' ability to understand the required reports, the Commission notes

[23] FFIEC Handbook, supra note 13, at 5.

that nothing in the regulation prevents a DCO from including additional, clarifying documents, such as executive summaries or compilations, with the required reports. The Commission believes that providing management or the board of directors with appropriate summaries or compilations can be an effective way to help a DCO fulfill the requirement in final § 39.18(e)(9). The Commission is further clarifying that the board may receive the materials at a regularly scheduled board meeting and that the board may delegate the review required under final § 39.18(e)(9) to an appropriate board-level committee. The Commission is adopting § 39.18(e)(9) as proposed.

I. Remediation

Proposed § 39.18(e)(10) would require a DCO to analyze the results of the testing and assessment required by § 39.18 to identify all vulnerabilities and deficiencies in its systems. The proposed regulation would require a DCO to remediate those vulnerabilities and deficiencies to the extent necessary to enable it to fulfill its statutory and regulatory obligations. In addition, the remediation would have to be timely in light of appropriate risk analysis with respect to the risks presented by such vulnerabilities and deficiencies.

Nadex stated that while it agrees with the proposed remediation requirements generally, the language requiring identification of "all" vulnerabilities and deficiencies would essentially impose strict liability on the firm for any breach of its security.

In response to Nadex's comment, the Commission is revising proposed § 39.18(e)(10) as follows, "A [DCO] shall identify and document vulnerabilities and deficiencies in its systems revealed by the testing and assessment required by this section. The [DCO] shall conduct and document an appropriate analysis of the risks presented by

each vulnerability or deficiency to determine and document whether to remediate the vulnerability or deficiency or accept the associated risk. When a [DCO] determines to remediate a vulnerability or deficiency, it must remediate in a timely manner given the nature and magnitude of the associated risk." The revisions require a DCO to determine whether to remediate or accept the risks presented by a vulnerability or deficiency based on an analysis of those risks, and to document that analysis. The changes acknowledge that in some instances, depending on the results of an appropriate risk analysis, a DCO may reasonably choose to accept a given risk. The changes also remove any suggestion that testing would necessarily identify every vulnerability, or that a DCO must remediate all vulnerabilities.

The Commission believes that the terms "remediate" and "accept" provide the universe of appropriate responses to identified vulnerabilities and deficiencies. Industry standards outlining potential responses to cyber risks speak in terms of mitigating, accepting, avoiding, and sharing or transfer[24] of risk.[25] NIST describes risk mitigation as risk reduction, and the appropriate risk response for that portion of risk that cannot be accepted, avoided, shared, or transferred.[26] The Commission believes that the term

[24] The Commission does not believe that risk sharing or transfer is an appropriate response to systems risks, and does not intend for it to constitute remediation under § 39.18(e)(10) as finalized. NIST describes risk sharing or transfer as the appropriate risk response when organizations desire and have the means to shift risk liability and responsibility to other organizations. NIST SP 800-39, supra note 13, at 43. The Commission's regulatory approach in this area, however, requires that a DCO retain complete responsibility for its risk program. See 17 CFR 39.18(f)(2)(i) (to be re-codified as § 39.18(d)(2)). Additionally, NIST cautions that risk transfer reduces neither the likelihood of harmful events occurring nor the consequences in terms of harm to organizational operations and assets, individuals, other organizations, or the nation. NIST SP 800-39, supra note 13, pp. 43. The Commission does not believe that a risk response that does not address the likelihood of a harmful event or its consequences is an appropriate response.

[25] See, e.g., NIST SP 800-39, supra note 13, at 41-43.

[26] Id. at 42-43.

"remediate" as used in final § 39.18(e)(10) captures mitigation. NIST describes risk avoidance as taking specific actions to eliminate the activities or technologies that are the basis for the risk or to revise or reposition these activities or technologies in the organizational mission/business processes to avoid the potential for unacceptable risk.[27] The Commission believes these types of avoidance actions are also properly considered risk remediation.

Nadex also urged the Commission to establish safe harbor provisions offering protection where it is apparent the DCO has acted in good faith and maintains reasonable standards, consistent with at least the minimum requirements prescribed by the regulations, to prevent, monitor, detect, and address internal and external cyber threats. In light of the revisions to § 39.18(e)(10), the Commission does not believe the addition of any safe harbor provision is necessary. The final regulation imposes specific system safeguards testing and remediation requirements, and does not seek to hold DCOs strictly liable for every cyber attack.

J. Recovery Time Objective

Proposed § 39.18(a) would revise the definition of "recovery time objective" to make the language consistent with that used elsewhere in § 39.18.

OCC stated that it agrees with the 2-hour recovery time objective for physical events, but believes that a reasonableness standard is more appropriate for cybersecurity events. OCC's comment relates to the recovery time objective period, which is addressed in § 39.34, rather than the "recovery time objective" definition that is at issue here. The Commission will take the comment under advisement, but it is beyond the scope of this

[27] Id. at 42.

rulemaking. Accordingly, the Commission is adopting the definition of "recovery time objective" as proposed.

K. Additional Comments

The Commission received several general comments on the proposed rule. CME, ICE, LCH, MGEX, and Nadex generally expressed support for the Commission's rulemaking efforts.

1. Principles-Based Requirements

ICE, MGEX, and OCC favored a principles-based approach, and argue that the Commission's approach is overly prescriptive. Specifically, OCC suggested that the Commission adopt a framework similar to SEC Regulation Systems Compliance and Integrity, which allows registrants to design their own compliance plans using industry standards that meet specified requirements that further the goals intended by the regulation.

CME noted that it is important to allow entities, especially those operating within multiple jurisdictions, the flexibility to look to the best practices and standards that are most appropriate for addressing their unique risks, noting that best practices and generally accepted standards were not designed for the financial services industry.

MGEX stated that the expanded definition of "information security" in proposed § 39.18(b)(2) is overly prescriptive, and that this "check-the-box" list would not keep up with evolving markets, potentially giving the Commission a false sense of security.

The Commission declines to alter its approach of basing this regulation on industry standards. This approach results in a regulation that is not overly prescriptive

and will provide DCOs with flexibility to design systems and testing procedures based on the best practices that are most appropriate for that DCO's risks.

2. International Harmonization

ICE, LCH, and OCC stated that it is important for the Commission to consider harmonizing its regulations with international standards for system safeguards testing. Specifically, OCC stated that it is concerned that systemically important clearing houses that are subject to multiple regulatory regimes will face compliance challenges, particularly during regulatory exams, if regulators fail to coordinate and align on a common set of guidelines or standards.

As stated above, the Commission believes that this regulation's reliance on industry standards will provide DCOs, including those subject to multiple regulatory regimes, with flexibility to design systems and testing procedures based on the best practices that are most appropriate for that DCO's risks. Additionally, the Commission notes that the rule is consistent with the Guidance on Cyber Resilience for Financial Market Infrastructures published by the Committee on Payments and Market Infrastructures ("CPMI") and the International Organization of Securities Commissions ("IOSCO") (together, "CPMI-IOSCO"). The report sets out internationally agreed upon guidelines designed to help financial market infrastructures, including central counterparties, enhance their cyber resilience.[28]

3. DCO / DCM Harmonization

[28] CPMI-IOSCO Guidance on Cyber Resilience for Financial Market Infrastructures, June 29, 2016, available at: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf.

MGEX noted that because it is registered with the Commission as both a DCO and a DCM, it cannot avail itself of the benefits of the 5% carve-out from the definition of "covered designated contract market" provided in the Commission's proposed regulation applicable to DCMs.[29] MGEX recommended that a 5% threshold be added to the DCO rulemaking, and that the Commission provide adequate ramp-up and ramp-down periods for organizations moving above or below this threshold.

MGEX also stated that the Commission should more closely harmonize its DCO and DCM cybersecurity requirements. For example, with respect to business continuity and disaster recovery plans, DCMs are required to coordinate with members and other market participants upon whom the DCM depends to provide liquidity, while a DCO is required to coordinate with its clearing members. MGEX believes these requirements should be harmonized and provide for coordination with other entities deemed appropriate by an organization. MGEX is concerned that if clearing members or other participants are required to coordinate extensively with DCMs or DCOs there will be an incentive for them to work with fewer organizations.

The Commission has worked to harmonize the regulations applicable to DCOs and DCMs, and as a result, the regulations track each other very closely. The Commission declines, however, to impose lighter regulation on those DCOs that are also DCMs, but are not covered DCMs. Unlike DCMs, DCOs hold member and customer funds, as well as records of member and customer positions, which would be at risk in the event of a cyber attack. Therefore the Commission believes that all DCOs must satisfy a uniform set of requirements with respect to system safeguards. With respect to the

[29] System Safeguards Testing Requirements, 80 FR 80140 (Dec. 23, 2015) (to be codified at 17 CFR part 38).

coordination requirement, DCMs and DCOs by their nature have different interested parties, and the need for a DCO to coordinate its business continuity and disaster recovery plan with its clearing members has not changed as a result of this rulemaking.

4. Independence Generally

CME, ICE, and MGEX stated that internal audit groups should be permitted to continue in their current roles at those DCOs. CME noted that industry standards and best practices recognize that independence is determined not by employment, but impartiality. MGEX stated that the independence requirements present a competitive disadvantage for smaller entities that cannot afford full-time independent staff.

The Commission believes that the regulation adequately addresses the use of independent employees in carrying out the requirements of the regulation, and declines to make any changes to specifically address the use of internal audit personnel. In addition, the Commission does not believe it is necessary to change the independence requirements for DCOs that do not want to pay for full-time independent staff to conduct various required activities, as those DCOs are free to engage outside consultants to conduct activities that do not warrant full-time hires.

In the Proposal, the Commission requested comment on whether it should define the term "independent contractor" and if so, how it should define the term. LCH recommended that the Commission provide further guidance or a specific definition of "independent contractor" to maintain a consistent approach by all DCOs, but did not identify any specific lack of clarity that may result from use of the term absent a Commission definition. After consideration, the Commission is clarifying that as used in § 39.18, the term independent contractor does not include employees of a DCO's parent

or affiliate company or co-sourced individuals.[30] In light of this clarification, the Commission does not believe that a definition of "independent contractor" is necessary.

5. Books and Records

ICE stated that the Commission should only require regulated entities, and not the entire firm of which the regulated entity is a part, to produce books and records relevant to a particular examination. According to ICE, overly burdensome production requirements will limit the regulated entities from having open and honest conversations related to risk. For example, risk is often discussed at a firm-wide level and not by a specific regulated entity. ICE contends that discussion regarding risks for non-CFTC regulated companies is not of interest to the Commission, and jeopardizes the confidentiality of those non-CFTC regulated companies. Further, ICE believes that CFTC requests for information from non-CFTC regulated companies would likely cause conflicts with other regulators and could violate foreign laws or regulations.

The Commission believes that document production obligations during the course of an examination are beyond the scope of the rulemaking, but notes that Commission registrants are expected to produce required materials to the Commission regardless of whether that information resides at the registrant, at a related entity, or at an outside consultant. In many cases, a DCO shares system safeguard programs with other entities within the corporate structure. In these instances, the Commission will continue to require production of all books and records relating to the system safeguards of DCOs, including those relating to the system safeguards risks and risk analysis and oversight

[30] Co-sourced individuals are non-employees who are integrated directly into a business's organizational structure to perform an ongoing function. The co-sourced individuals typically work in collaboration with the business's employees.

programs of parent companies where such risks or such programs are shared in whole or in part by a DCO.

6. Indemnification

CME stated that removing language from the current version of § 39.18 that expressly provides that a DCO is "free to seek indemnification" from outside service providers reduces certainty for the industry. CME added that because there is nothing within the regulation to prohibit the use of indemnification, as the Commission itself acknowledges, the Commission should not unnecessarily remove the certainty the current language provides.

The Commission does not believe the "free to seek indemnification" language suggested by CME is necessary and is not changing the proposed regulation in this regard. Nothing in the final rule suggests that a DCO could not seek indemnification, and the Commission need not address the legal rights of DCOs with respect to third parties.

7. Systems Developments

MGEX stated that the systems development requirements contained in proposed § 39.18(b)(2)(v) should be required on an "as needed" or "as reasonable" basis. The Commission is declining to make changes to §39.18(b)(2)(v) based on MGEX's suggestion. Information regarding systems development and quality assurance is appropriately part of the DCO's program of risk analysis and oversight. If a DCO believes that it does not have any information to include on this topic in its program of risk analysis and oversight, it can document that position, and the basis for it, in the program.

III. Dates

LCH stated that in setting a compliance date, the Commission should consider the size and complexity of a DCO as well as the resources a DCO will need to procure in order to comply with the new regulations. The Commission has determined the following compliance dates on a provision-by-provision basis, determining appropriate compliance dates that it believes all DCOs, regardless of their size, complexity, or resources, should reasonably be able to meet.

All of the regulations adopted herein will be effective upon publication in the Federal Register. Except as otherwise provided below, DCOs must comply with the requirements in § 39.18 as of the effective date. Based on comments that discussed a DCO's need for time to develop appropriate policies and procedures to come into compliance, the Commission is extending the date by which DCOs must come into compliance for certain provisions as follows:

DCOs must comply with the following provisions 180 days after the effective date: vulnerability testing – § 39.18(e)(2); and security incident response plan testing – § 39.18(e)(6).

DCOs must comply with the following provisions 1 year after the effective date: external penetration testing – § 39.18(e)(3); internal penetration testing – § 39.18(e)(4); controls testing – § 39.18(e)(5); and enterprise technology risk assessment – § 39.18(e)(7).

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.[31] The final rule adopted 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.[32] The Commission has previously determined that DCOs are not small entities for the purpose of the RFA.[33] Accordingly, the Chairman, on behalf of the Commission, hereby certifies pursuant to 5 U.S.C. 605(b) that the rule adopted herein will not have a significant economic impact on a substantial number of small entities. The Chairman made the same certification in the proposed rulemaking, and the Commission did not receive any comments on the RFA.

B. Paperwork Reduction Act

The Paperwork Reduction Act of 1995 ("PRA")[34] 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 unless it displays a currently valid control number. This rulemaking contains recordkeeping and reporting requirements that are collections of information within the meaning of the PRA.

The final rule contains provisions that would qualify as collections of information, for which the Commission has already sought and obtained a control number from the

[31] 5 U.S.C. 601 et seq.

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

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

[34] 44 U.S.C. 3501 et seq.

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). Responses to this collection of information are mandatory. As discussed in the Proposal, the Commission believes that the final rule does not impose any new recordkeeping or reporting requirements that are not already accounted for in collection 3038-0076.[35] The Commission did not receive any comments on its assumptions regarding the recordkeeping or information collection requirements resulting from the rule as proposed.

The Commission notes that DCOs are already subject to system safeguard-related recordkeeping and reporting requirements. As discussed in the Proposal, the Commission is amending and renumbering current § 39.18(i) as § 39.18(f), to clarify the system safeguard recordkeeping and reporting requirements for DCOs. The regulation requires DCOs, in accordance with § 1.31,[36] 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

[35] 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.

[36] 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).

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 final § 39.18(f) are contained in the provisions of current § 39.18(i), which was adopted on November 8, 2011.[37] Accordingly, the Commission believes that final § 39.18(f) would not impact the burden estimates currently provided for in collection 3038-0076.

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.[38] 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.

To further the Commission's consideration of the costs and benefits imposed by its regulation, the Commission invited comments from the public on the costs and benefits associated with the proposed regulation, and included a series of specific requests for comment related to the potential costs and benefits resulting from, or arising

[37] 76 FR 69334, at 69428.

[38] 7 U.S.C. 19(a).

out of, requiring DCOs to comply with the proposed changes to § 39.18.[39] A number of commenters addressed the costs and benefits of the Proposal, which the Commission addresses in the discussion that follows. The Commission believes that the changes in the final regulation will reduce the costs of compliance as compared to the Proposal, which itself imposed only modest costs relative to those that already exist under current § 39.18.

2. Background and Baseline for the Final Rule

As an initial matter, the Commission considers the incremental costs and benefits of this regulation, meaning 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 quantifiable costs and benefits. Where quantification is not feasible, the Commission identifies and describes costs and benefits qualitatively.[40]

As discussed in the Proposal, the Commission believes that cyber threats to the financial sector have expanded dramatically in recent years.[41] 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 amendments would likely result in some additional costs for DCOs, the final rule 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

[39] 80 FR 80114, at 80133.

[40] 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.

[41] See 80 FR 80114, at 80114-80115.

efforts by DCOs to strengthen cyber defenses, to mitigate operational, reputational, and financial risk, and to maintain cyber resilience and ability to recover from cyber attack. 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.

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.[42] 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."[43] Further, current § 39.18(j)(2) requires that this testing be conducted by independent contractors or employees of the DCO not responsible for development or operation of the systems or capabilities being tested.[44]

In addition to referencing generally accepted standards and industry best practices, this cost and benefit discussion uses information provided by DCOs in connection with a survey of DCO system safeguard costs and practices conducted by

[42] 17 CFR 39.18(j).

[43] See 17 CFR 39.18(d).

[44] 17 CFR 39.18(j).

Commission staff ("February 2015 DCR Survey").[45] 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.

In general, the final regulation clarifies existing system safeguards requirements under current § 39.18 by identifying specific testing required by industry best practices. To the extent the final rule imposes new requirements and thus additional costs, the primary costs will result from more frequent testing, including some testing that must be carried out by independent contractors on behalf of the DCO. As a result, the final rule may increase operational costs for DCOs by requiring additional resources. In addition, the Commission notes that some DCOs are larger or more complex than others, and the

[45] 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.

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 is sensitive to the economic effects of the regulation, including costs and benefits.

While certain costs are amenable to quantification, other costs cannot be reasonably estimated, such as the costs to the public or market participants in the event of a cybersecurity incident at a DCO. The Commission's final regulation is 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 discussion of the comments received regarding the costs and benefits of the Proposal generally. Following the general discussion, the Commission provides a summary of changes to the proposed rule that resulted in the final rule, discusses the costs and benefits of the final rule, and where relevant, the costs of the final rule relative to the Proposal and addresses comments specific to the costs and benefits of each proposal. At the conclusion of this discussion, the Commission considers the costs and benefits of the final regulation collectively in light of the five factors set forth in section 15(a) of the CEA.

3. General Comments Received

CME estimates that the proposed rule would cost CME Group approximately $7.2 million over a two-year period. CME noted that its cost estimate also includes the

Commission's proposal applicable to DCMs and does not separately estimate costs for clearing, trading, or data reporting. As described more fully below, the Commission is adopting the final regulation with modifications in certain key areas, which should result in less cost and burden for DCOs relative to the Proposal.

LCH recommended that the Commission consider the complexity created by multiple standards coming into effect in different major jurisdictions within the same timeframe. LCH stated that although international DCOs will achieve compliance against the highest minimum standards, the lead time for building testing programs and supportive compliance controls to meet many sets of new standards could be longer for larger and more complex DCOs than for smaller, regional DCO operations. The Commission agrees with LCH and, as discussed above in section III, has set individualized compliance dates for different aspects of the regulation. The Commission believes that all DCOs, regardless of their size, complexity, or resources, should generally be able to comply by the specified dates.

MGEX stated that some entities may incur additional costs due to the divergence between the Commission's proposed rules for DCMs and DCOs, including the programs of risk analysis and oversight and coordination of the business continuity and disaster recovery plan with industry participants. The Commission notes that the rules for DCMs and DCOs are largely harmonized, and that differences in the programs of risk analysis and oversight for DCOs and DCMs are largely attributable to the different risks faced by the two types of entities. The new rules applicable to DCMs require that the program of risk analysis and oversight include enterprise risk management and governance applicable specifically to security and technology, but as noted in the Proposal, any

parallel requirements for DCOs must be addressed in a more comprehensive fashion involving more than the system safeguards context alone, and thus are not appropriate for this rulemaking.[46] Additionally, the requirement for a DCO to coordinate its business continuity and disaster recovery plan with clearing members is not a new requirement, and has not been amended by this rulemaking. That requirement has only been renumbered, and any compliance costs are not properly attributed to this rulemaking.

LCH and MGEX stated that the Commission should consider the size and complexity of the DCO in calculating the cost of the proposed requirements. Specifically, MGEX noted that $8,383,222, a figure drawn from the notice of proposed rulemaking for the system safeguards rules applicable to DCMs, is "excessively punitive" for smaller entities. It further stated that organizations like MGEX cannot bear these costs, and that the Commission should not require them to comply because they present lower overall risk to the industry, and have dramatically smaller exposure to vulnerabilities compared to SIDCOs. The Commission notes that the figure cited by MGEX is not an estimate of new costs arising from this rulemaking. It was instead an average calculated from preliminary information collected from some DCMs and SDRs regarding their current costs associated with conducting vulnerability testing, external and internal penetration testing, controls testing, and enterprise technology risk assessments. The Commission nevertheless acknowledges that this rulemaking will impose new costs on DCOs beyond the current cost of compliance, and recognizes that the actual costs may vary widely as a result of numerous factors including the size of the organization, the complexity of the automated systems, and the scope of the test. The

[46] 80 FR 80114, at 80123 n. 127.

Commission has attempted to limit costs for smaller DCOs by providing the flexibility to design systems and testing procedures that are appropriate for each DCO's individual risks.

CME and LCH noted that the shortage of skilled professionals could increase costs directly and indirectly as a result of the proposed rule. The Commission notes that where appropriate, the final rule provides additional flexibility regarding the ability of DCOs to choose whether to use internal or external personnel to conduct certain tests.

MGEX noted that implementation on the scale required by this rulemaking will include significant personnel and non-personnel resources. These additional costs include IT and operations personnel costs, purchase of software and hardware, legal and compliance costs, and the cost of third-party testing vendors. MGEX anticipated that its costs will go up two or three times if the rulemakings are made final in their proposed form, explaining that the highest cost of compliance would result from hiring of independent contractors/professionals. As discussed more fully below and in the Proposal, the Commission acknowledges that there will be some increases in the costs described by MGEX. In the final rule, the Commission, where appropriate, has provided DCOs with additional flexibility regarding who may conduct certain tests. The Commission notes, however, that many of the costs described by MGEX are attributable to compliance with the current rule and not to additional requirements imposed by this rulemaking. For example, the requirement to conduct testing with independent contractors or independent employees already exists under current § 39.18(j)(2). Further, based on industry standards, current § 39.18 requires DCOs to conduct external penetration testing using an independent contractor.

4. Consideration of Costs and Benefits Related to the Final Rule

This section discusses cost and benefit considerations related to the final rule, including those aspects of the regulation that have changed since the proposed rule, and those aspects of the regulation on which the Commission received comments.

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

i. Summary of Final Regulation

As discussed above in section II(A), the Commission is revising proposed § 39.18(e)(2)(ii) to remove the explicit requirement for authenticated scanning where indicated by appropriate risk analysis. The final rule requires that a DCO conduct automated vulnerability scanning, which complies with generally accepted best practices. The Commission is also revising § 39.18(e)(2)(iii) to remove the proposed requirement that two of the required quarterly vulnerability tests be conducted by independent contractors. Under the final rule, all four required tests may be conducted by independent contractors or employees of the DCO who are not responsible for development or operation of the systems or capabilities being tested. The Commission is otherwise finalizing § 39.18(e)(2) and the definition of "vulnerability testing" as proposed, and the Commission's consideration of the costs and benefits associated with those sections does not differ from those discussed in the Proposal.

ii. Costs

NGX commented that compliance with the proposed rule would not be inordinately costly relative to the benefits, with the exception of the requirements in § 39.18(e)(2)(i) to conduct vulnerability testing on a quarterly basis. NGX estimates that testing quarterly would cost over $100,000 more per year than testing annually, and

stated that the costs were not warranted because little changes from quarter to quarter. The Commission notes that industry best practices state that vulnerability testing should be conducted "at least quarterly."[47] Accordingly, current § 39.18 requires DCOs to conduct vulnerability testing on a quarterly basis. Therefore, the Commission does not believe that the frequency requirement of § 39.18(e)(2)(i) will impose new costs on DCOs.

The Commission has determined not to adopt the proposed requirement for authenticated scanning where indicated by appropriate risk analysis in the final § 39.18(e)(2)(ii). The rule as adopted will require automated vulnerability scanning to comply with best practices. Because current § 39.18 requires DCOs to comply with industry best practices, the Commission does not believe that DCOs will incur additional costs as a result of the adoption of § 39.18(e)(2)(ii).

ICE, LCH, OCC, and MGEX all noted significant costs associated with hiring outside contractors to conduct vulnerability tests. OCC believes that requiring a DCO to use an independent contractor to perform vulnerability testing during the same year that such person is performing external penetration testing would unnecessarily increase costs without an added benefit, because vulnerability testing is largely subsumed within external penetration testing. As discussed above, the Commission has determined not to adopt the proposed independent contractor requirement in final § 39.18(e)(2)(iii). Under the final rule, all required testing may be done by an independent contractor or by independent employees. The final rule is thus consistent with current § 39.18(j)(2), which requires systems safeguards testing to be conducted by independent contractors or

[47] See FFIEC Handbook supra note 13 at 82.

independent employees of the DCO. Because final § 39.18(e)(2)(iii) does not change the current requirement, it will not impose additional costs on DCOs.

iii. Benefits

The Commission did not receive any comments specific to the benefits of vulnerability testing and believes the benefits of final § 39.18(e)(2) do not differ from those discussed in the Proposal.

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

As discussed above in section II(B), the Commission is adopting § 39.18(e)(3) and the definition of "external penetration testing" as proposed. The Commission did not receive any comments specific to the costs or benefits of external penetration testing. The Commission believes that the costs and benefits of § 39.18(e)(3) do not differ from those discussed in the Proposal.

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

As discussed above in section II(C), the Commission is adopting § 39.18(e)(4) and the definition of "internal penetration testing" as proposed. The Commission did not receive any comments specific to the costs or benefits of internal penetration testing. The Commission believes that the costs and benefits of § 39.18(e)(4) do not differ from those discussed in the Proposal.

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

i. Summary of Final Regulation

As discussed above in section II(D), the Commission is revising proposed § 39.18(e)(5)(i) to remove a prescribed two-year minimum testing period for all controls testing, and instead require that (a) key controls be tested every three years; and (b) non-

key controls be tested at a frequency determined by an appropriate risk analysis. The Commission is making a corresponding change to proposed § 39.18(e)(5)(ii) to require that independent contractors test each key control at least every three years rather than every two. The Commission is otherwise finalizing § 39.18(e)(5) as well as the definitions of "controls," "controls testing," and "key controls" as proposed, and the Commission's consideration of the costs and benefits associated with those sections does not differ from those discussed in the Proposal.

ii. Costs

CME and OCC stated that the costs of requiring controls testing every two years outweigh the benefits. As discussed above, the Commission is adopting proposed § 39.18(e)(5)(i) with modifications to require key controls testing to be conducted at a frequency determined by an appropriate risk analysis, but no less frequently than every three years. The Commission has determined not to adopt the proposed minimum frequency requirement for non-key controls. As discussed in the Proposal, the Commission acknowledges that the minimum frequency requirement for key controls testing may increase costs for DCOs. The Commission notes, however, that the February 2015 DCR Survey indicated that most DCOs currently conduct controls testing at least annually and some DCOs may not face an increase in costs based on this requirement. Further, because of the modifications from the Proposal, the testing frequency for some DCOs could be reduced, and therefore may be less costly relative to the Proposal.

iii. Benefits

The Commission did not receive any comments specific to the benefits of controls testing and believes the benefits of final § 39.18(e)(5) do not differ from those discussed in the Proposal.

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

i. Summary of Final Regulation

As discussed above in section II(E), the Commission is amending the definition of "security incident" in proposed § 39.18(a) in order to provide additional clarity. Further, the Commission is adopting proposed § 39.18(e)(6)(iv) with modifications to remove the restrictions on which employees are permitted to conduct security incident response plan testing. The Commission is otherwise finalizing § 39.18(e)(6) as well as the definitions of "security incident response plan" and "security incident response plan testing" as proposed, and the Commission's consideration of the costs and benefits associated with those sections does not differ from those discussed in the Proposal.

ii. Costs

The Commission does not believe that the changes to the definition of "security incident" will affect the costs of the rule. As explained in the Proposal, the Commission does not believe proposed § 39.18(e)(6)(iv) will impose new costs on DCOs, because it is consistent with current § 39.18(j)(2). Further, without the proposed restrictions regarding which employees may conduct security incident response plan testing, § 39.18(e)(6)(iv) as finalized may lower costs for some DCOs by providing flexibility that does not exist in the current rule.

The Commission did not receive any comments related to the costs of security incident response plan testing.

iii. Benefits

The Commission did not receive any comments specific to the benefits of security incident response plan testing and believes that the benefits of final § 39.18(e)(6) do not differ from those discussed in the Proposal.

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

In the Proposal, the Commission concluded that proposed § 39.18(e)(7) is consistent with current industry standards[48] and would not impose additional costs on DCOs. As discussed above in section II(F), the Commission is adopting § 39.18(e)(7) and the definition of "enterprise technology risk assessment" as proposed, except for changes to § 39.18(e)(7)(i) to clarify that a DCO that has conducted an enterprise technology risk assessment that complies with this section may conduct subsequent assessments by updating the previous assessment. This was intended as a clarification rather than a substantive change, and in any event will not impose any additional costs on DCOs.

The Commission did not receive any comments specific to the costs or benefits of enterprise technology risk assessment testing. The Commission believes that the costs and benefits of final § 39.18(e)(7) do not differ from those discussed in the Proposal.

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

i. Summary of Proposed Regulation

As discussed above in section II(G), the Commission is revising proposed § 39.18(e)(8) to state that that the scope of testing and assessment required by § 39.18 shall be broad enough to include the testing of automated systems and controls that a

[48] See, e.g., PCI-DSS, supra note 13, at 105.

DCO's required program of risk analysis and oversight and its current cybersecurity threat analysis indicate is necessary to identify risks and vulnerabilities that 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

In the Proposal, the Commission discussed the costs of proposed § 39.18(e)(8) in relation to each substantive testing requirement. In each case, the Commission concluded that proposed § 39.18(e)(8) would not impose new costs on DCOs. The Commission believes that the changes to proposed § 39.18(e)(8) narrow the scope of testing in the final rule. Rather than requiring that DCOs test all automated systems and controls necessary to identify any of the enumerated risks and vulnerabilities, the scope of testing under the final rule is determined by a DCO's required program of risk analysis and oversight and its current cybersecurity threat analysis. Therefore, the Commission does not believe that final § 39.18(e)(8) will impose new costs on DCOs compared to the proposed rule or the current rule. The Commission believes this risk-based approach will result in improved and more cost-effective testing.

The Commission did not receive any comments specific to the costs or benefits of the scope of testing.

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

As discussed above in section II(H), the Commission is adopting § 39.18(e)(9) as proposed. The Commission did not receive any comments specific to the costs or benefits of internal reporting and review. The Commission believes that the costs and benefits of final § 39.18(e)(9) do not differ from those discussed in the Proposal.

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

i. Summary of Final Regulation

As discussed above in section II(I), the Commission is revising proposed § 39.18(e)(10) to require a DCO to identify and document the vulnerabilities and deficiencies in its systems revealed by the testing and assessment required by the regulation and to conduct and document an appropriate analysis of the risks presented by such vulnerabilities and deficiencies to determine and document whether to remediate or accept each risk.

ii. Costs

The final rule makes clear that a DCO is only required to consider remediation of those vulnerabilities and deficiencies revealed through testing, rather than all vulnerabilities and deficiencies. Further, the final rule specifically allows DCOs to accept certain risks presented by vulnerabilities and deficiencies when that is appropriate based on an analysis of the risk presented. These changes to the Proposal will, if anything, result in lower costs to DCOs relative to the proposed rule. In any event, responding to vulnerabilities and deficiencies revealed by cybersecurity testing is an

industry best practice,[49] and DCOs are already required to comply with this requirement under current § 39.18.

The aspect of the final rule that could impose additional costs on DCOs relative to the current rule is the express requirement that DCOs document the vulnerabilities and deficiencies in its systems revealed by the required testing and assessment, document an appropriate analysis of the risks presented by such vulnerabilities, and document whether to remediate or accept each risk. DCOs would have been required under the proposed rule to analyze their testing results to determine the extent of their required remediation, so the difference in the final rule is the express documentation requirement. The express requirement that DCOs document their analysis imposes at most a slight additional cost on DCOs, particularly given that DCOs would likely have documented the required analysis even absent the express requirement.

The Commission did not receive any comments specific to the costs of remediation.

iii. Benefits

The documentation requirement described above has the joint benefits of helping to ensure that DCOs carefully consider whether to remediate or accept risks, and of allowing the Commission to review the thought process behind these significant decisions. The Commission did not receive any comments specific to the benefits of remediation.

5. Section 15(a) Factors

[49] See, e.g., NIST SP 800-39, supra note 13, at 41-43; FFIEC Handbook, supra note 13, at 5.

In addition to the discussion above, the Commission has evaluated the costs and benefits of § 39.18 in light of the specific considerations identified in section 15(a) of the CEA as follows:

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. Final § 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 final rule 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. Preventing disruptions helps to ensure that market participants will have continuous access to central clearing.

Additionally, providing the Commission with reports concerning the system safeguards testing and assessments required by the final regulation 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 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 amendments to § 39.18 will 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 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 final rule to have a significant impact on the competitiveness of the derivatives markets.

c. Price Discovery

The Commission does not anticipate the 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 amendments to § 39.18 will strengthen and promote sound risk management practices across DCOs. Specifically, the amendments will 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 final rule 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 final regulation 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. Regulation 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.

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 amends 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, and 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 jeopardizes or has a significant likelihood of jeopardizing 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 (including, 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 (including, network port control, boundary defenses, encryption); system and information integrity (including, 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 (including, 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 (including, 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, which shall follow generally accepted best practices.

(iii) A derivatives clearing organization shall conduct vulnerability 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.

(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 shall test and assess key controls no less frequently than every three years. A derivatives clearing organization may conduct such testing on a rolling basis over the course of the required period.

(ii) A derivatives clearing organization shall engage independent contractors to test and assess the key controls included in the derivatives clearing organization's program of risk analysis and oversight no less frequently than every three 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.

(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. A derivatives clearing organization that has conducted an enterprise technology risk assessment that complies with this section may conduct subsequent assessments by updating the previous assessment.

(ii) A derivatives clearing organization may conduct enterprise technology risk assessments 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 assessed.

(8) Scope of testing and assessment. The scope of testing and assessment required by this section shall be broad enough to include the testing of automated systems and controls that a derivatives clearing organization's required program of risk analysis and oversight and its current cybersecurity threat analysis indicate is necessary to identify risks and vulnerabilities that 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 identify and document the vulnerabilities and deficiencies in its systems revealed by the testing and assessment required by this section. The derivatives clearing organization shall conduct

and document an appropriate analysis of the risks presented by each vulnerability or deficiency to determine and document whether to remediate the vulnerability or deficiency or accept the associated risk. When a derivatives clearing organization determines to remediate a vulnerability or deficiency, it must remediate in a timely manner given the nature and magnitude of the associated risk.

(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 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. In § 39.34, revise paragraphs (a), (b)(3), and (c) 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 September 9, 2016, 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 Commissioners' Statements

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 the two rules the Commission has finalized today.

The risk of cyberattack probably represents the single greatest threat to the stability and integrity of our markets today. Instances of cyberattacks are all too familiar both inside and outside the financial sector. Today, they often are motivated not just by those with a desire to profit, but by those with a desire deliberately to disrupt or destabilize orderly operations.

That is why these system safeguard rules are so important. The rules we have finalized today will apply to the core infrastructure in our markets—the exchanges, clearinghouses, trading platforms, and trade repositories. And they will ensure that those private companies are regularly evaluating cyber risks and testing their cybersecurity and operational risk defenses. While our rules already require this generally, the measures we approved today add greater definition—not by being overly prescriptive, but by setting some principles-based standards, and requiring specific types of testing, all rooted in industry best practices.

I've said many times that as regulators, we must not just look backwards to address the causes of past failures or crises. We also must look ahead—ahead to the new opportunities and challenges facing our markets. Financial markets constantly evolve, and we must ensure our regulatory framework is adapting to these changes.

These new rules are one good example of how we are looking ahead and addressing these new challenges. They will serve as a strong and important complement

to the many other steps being taken by regulators and market participants to address cybersecurity. For example, government agencies and market participants are already working together to share information about potential threats and risks – and learn from one another.

I want to thank all those who provided feedback on the proposed rules the Commission approved last December. We received a number of thoughtful comments from market participants, most of which expressed broad support for the proposals. Commenters also highlighted some areas of concern, and we made adjustments based on that feedback. For example, we have reduced the frequency of controls testing and narrowed the instances where independent contractor testing is required. We have also clarified definitions of key terms, and made clear that the scope of required testing will be based on appropriate risk and threat analysis.

I also thank Commission staff for their hard work on these measures, particularly our staff in the Division of Market Oversight and Division of Clearing and Risk, as well as the support that is always provided by staff in the Office of General Counsel, the Office of Chief Economist and other staff who comment on the rules. I also thank my fellow Commissioners Bowen and Giancarlo for their support of and suggestions regarding these final rules.

Appendix 3 – Concurring Statement of Commissioner Sharon Y. Bowen

I will be voting yes on both systems safeguards rules. There is not much more to say than what I said when these rules were proposed on December 10, 2015.[1]

[1] Concurring Statement of Commissioner Sharon Y. Bowen Regarding Notice of Proposed Rulemaking on System Safeguards Testing Requirements (Dec. 10, 2015), *available at* http://www.cftc.gov/PressRoom/SpeechesTestimony/bowenstatement121615b.

Cybersecurity is a top concern for American companies, especially financial firms. These rules are a good step forward in addressing these concerns.

As I noted when they were proposed, 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 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").[2]

I was also an early proponent of including all registered entities, including SEFs, in this rule. I am glad to see them included, and look forward to the staff roundtable to

[2] Id. See also 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.

discuss how to apply heightened standards to the significant SEFs. Thank you and I look forward to the staff's presentation.

[Appendices continue on next page]

Appendix 4 – Statement of Commissioner J. Christopher Giancarlo

Good regulation should be balanced. It should have a positive impact on the marketplace while mitigating costs to the extent possible. I believe today's system safeguards final rule for derivatives clearing organizations (DCOs) generally achieves such balance although I have concerns about the cost impact on smaller DCOs.

As I have said, cyber and system security is one of the most important issues facing markets today in terms of integrity and financial stability.[1] Given its importance, it is right that the Commission implements rules requiring DCOs and other registrants to conduct regular testing of their systems. I am pleased that the final rule requires DCOs to follow industry adopted standards and best practices. I believe this approach recognizes the rapid evolution of cyber threats and will allow DCOs the flexibility to continually update their cyber defenses in response to these threats. I also recognize that the final rule addresses my concern that being hacked by itself cannot be considered a rule violation subject to enforcement. The final rule clarifies that the Commission it is not seeking to hold DCOs strictly liable for being attacked.

While the final rule generally takes the right approach, I am concerned about its cost on smaller DCOs. I have expressed my concern about the cost of regulation on

[1] System Safeguards Testing Requirements, 80 FR 80140, 80190-191 (Dec. 23, 2015).

smaller market participants on numerous past occasions.[2] One commenter to this rulemaking noted that its costs will likely increase two to three times if these rules are finalized as proposed.[3] The independent contractor and employee testing requirement is especially costly for these small DCOs. While the parallel designated contract market (DCM) system safeguards rulemaking addresses this cost concern through the "covered-DCM" concept, the DCO rule does not. Although the DCO rule does not have such a concept, I understand from our Division of Clearing and Risk that they are willing to discuss the concerns of smaller DCOs. I encourage those DCOs to raise their concerns with the Division and encourage the Division to act with appropriate practicality.

I note approvingly that the Commission has alleviated some burdens from the proposed rulemaking such as increasing the frequency of key controls testing from two years to three years, removing the requirement for independent contractors to conduct vulnerability testing and removing the explicit requirement for authenticated scanning, among other requirements.

I support the final DCO system safeguards rule despite concerns about its costs. Although I would have preferred that the rule take a less one-size-fits-all approach, I am a firm supporter of effective cyber and system security policies and procedures given the serious threat that cyber belligerents pose. I commend staff for their hard work and generally practical approach to system safeguards for DCOs. I also appreciate that they

[2] See e.g., Regulation Automated Trading, 80 FR 78824, 78946 (Dec. 17, 2015); Guest Lecture of Commissioner J. Christopher Giancarlo, Harvard Law School, Fidelity Guest Lecture Series on International Finance, Dec. 1, 2015.

[3] Minneapolis Grain Exchange, Inc. Comment Letter at 13, Feb. 22, 2016.

responded to many comments in an effort to reduce some of the burdens of the final rule. I therefore vote to adopt this rule.

[FR Doc. 2016-22413 Filed: 9/16/2016 8:45 am; Publication Date: 9/19/2016]