COMMODITY FUTURES TRADING COMMISSION

17 CFR Parts 37, 38, and 49

RIN 3038-AE30

System Safeguards Testing Requirements

AGENCY: Commodity Futures Trading Commission (CFTC).

ACTION: Final Rulemaking.

SUMMARY: The Commodity Futures Trading Commission is adopting final rules amending its current system safeguards rules for designated contract markets, swap execution facilities, and swap data repositories, by enhancing and clarifying current provisions relating to system safeguards risk analysis and oversight and cybersecurity testing, and adding new provisions concerning certain aspects of cybersecurity testing. The final rules clarify the Commission's current system safeguards rules for all designated contract markets, swap execution facilities, and swap data repositories by specifying and defining the types of cybersecurity testing essential to fulfilling system safeguards testing obligations. These testing types are vulnerability testing, penetration testing, controls testing, security incident response plan testing, and enterprise technology risk assessment. The final rules also clarify current rule provisions respecting: the categories of risk analysis and oversight that statutorily-required programs of system safeguards-related risk analysis and oversight must address; system safeguards-related books and records obligations; the scope of system safeguards testing; internal reporting and review of testing results; and remediation of vulnerabilities and deficiencies. In addition, the final rules adopt new provisions set forth in the Commission's Notice of Proposed Rulemaking, applicable to covered designated contract markets (as defined)

and all swap data repositories, establishing minimum frequency requirements for conducting certain types of cybersecurity testing, and requiring performance of certain tests by independent contractors.

DATES: The effective date of this rule is [INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER]. Compliance dates: (1) Designated contract markets, swap execution facilities, and swap data repositories must be in full compliance with the vulnerability testing requirements of this part within 180 calendar days after the effective date. (2) Designated contract markets, swap execution facilities, and swap data repositories must be in full compliance with the penetration testing requirements of this part within one year after the effective date. Such compliance must include having conducted and completed penetration testing that complies with this part within one year after the effective date. In the case of covered designated contract markets and swap data repositories, such compliance must include penetration testing conducted and completed by an independent contractor as required by this part. (3) Designated contract markets, swap execution facilities, and swap data repositories must be in full compliance with the controls testing requirements of this part within one year after the effective date. Covered designated contract markets and swap data repositories must have testing of key controls by an independent contractor as required by this part completed within three years after the effective date. (4) Designated contract markets, swap execution facilities, and swap data repositories must be in full compliance with the security incident response plan testing requirements of this part within 180 calendar days after the effective date. Such compliance must include having created and completed testing of a security incident response plan within 180 days after the effective date. (5) Designated contract

markets, swap execution facilities, and swap data repositories must be in full compliance with the enterprise technology risk assessment requirements of this part within one year after the effective date. Such compliance must include having completed an enterprise technology risk assessment that complies with this part within one year after the effective date. (6) Designated contract markets, swap execution facilities, and swap data repositories must be in full compliance with the requirements of this part for updating their business continuity-disaster recovery plans and emergency procedures within one year after the effective date. Such compliance must include having completed an update of such plans and procedures within one year after the effective date. (7) Designated contract markets must be in full compliance with the requirements of this part respecting required production of annual total trading volume within 30 calendar days of the effective date. (8) Designated contract markets, swap execution facilities, and swap data repositories must be in full compliance with the system safeguards-related books and records requirements of this part, which are part of such entities' current books and records requirements under current Commission regulations and statutory core principles, as of the effective date. (9) Designated contract markets, swap execution facilities, and swap data repositories must be in full compliance with all other provisions of these final rules within one year after the effective date.

FOR FURTHER INFORMATION CONTACT: Rachel Berdansky, Deputy Director, Division of Market Oversight, 202-418-5429, rberdansky@cftc.gov; David Taylor, Associate Director, Division of Market Oversight, 202-418-5488, dtaylor@cftc.gov, or David Steinberg, Associate Director, Division of Market Oversight, 202-418-5102,

dsteinberg@cftc.gov; Commodity Futures Trading Commission, Three Lafayette Centre, 1155 21st Street NW, Washington, DC 20851.

SUPPLEMENTARY INFORMATION:

I. BACKGROUND

A. The Need for Cybersecurity Testing

On December 15, 2015, the Commission issued a Notice of Proposed Rulemaking ("NPRM") proposing to amend its system safeguards rules for designated contract markets ("DCMs"), swap execution facilities ("SEFs"), and swap data repositories ("SDRs").[1]

As detailed in the NPRM, cyber threats to the financial sector continue to expand, increasing the need for enhanced cybersecurity testing. Such testing should focus on the entity's ability to detect, contain, respond to, and recover from cyber attacks. It should also address detection, containment, and recovery from compromise of data integrity—perhaps the greatest threat with respect to financial sector data—in addition to compromise of data availability or confidentiality. As noted in the NPRM, cybersecurity testing is a well-established best practice both generally and for financial sector entities.[2]

Cybersecurity testing is also supported internationally. The recently published *Guidance on cyber resilience for financial market infrastructures* issued by the Committee on Payments and Market Infrastructures and the Board of the International Organization of Securities Commissions ("CPMI-IOSCO Guidance") provides that:

---

[1] System Safeguards Testing Requirements, Proposed Rule 80 FR 80139, 80140 (Dec. 23, 2015).

[2] Id. at 80142.

> Testing is an integral component of any cyber resilience framework. All elements of a cyber resilience framework should be rigorously tested to determine their overall effectiveness before being deployed within an FMI, and regularly thereafter. This includes the extent to which the framework is implemented correctly, operating as intended and producing desired outcomes. Understanding the overall effectiveness of the cyber resilience framework in the FMI and its environment is essential in determining the residual cyber risk to the FMI's operations, assets, and ecosystem. [3]

The CPMI-IOSCO Guidance also states that a financial market infrastructure "should establish a comprehensive testing program to validate the effectiveness of its cyber resilience framework on a regular and frequent basis," employing appropriate cyber threat intelligence to inform its testing methods, and using the results to support ongoing improvement of its cyber resilience.[4]

B. Summary of the Proposed System Safeguards Testing Requirements Rule

1. Fundamental Goals.

The NPRM identified two principal goals. The first goal was clarification of current cybersecurity testing requirements for all DCMs, SEFs, and SDRs, along with clarification, amplification, and harmonization of other current system safeguards rule provisions. The second goal was the addition of new rule provisions for covered DCMs (as defined) and SDRs, establishing minimum frequency requirements for conducting certain types of cybersecurity testing, and requiring performance of certain tests by independent contractors.

[3] Committee on Payments and Market Infrastructures (CPMI) and Board of the International Organization of Securities Commissions (IOSCO) Guidance on cyber resilience for financial market infrastructures (June 2016) § 7.1, at 18, available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf.

[4] Id., § 7.2 at 18.

2. Categories of Risk Analysis and Oversight Applicable to All DCMs, SEFs, and SDRs.

The system safeguards provisions of the Commodity Exchange Act ("Act" or "CEA") and Commission regulations applicable to all DCMs, SEFs, and SDRs require these entities to maintain a program of risk analysis and oversight to identify and minimize sources of operational risk.[5] Commission regulations concerning system safeguards provide that the program of risk analysis and oversight required of each such entity must address specified categories of risk analysis and oversight to identify and minimize sources of operational risk.[6] The NPRM proposed clarification of what is already required of all DCMs, SEFs, and SDRs regarding the six current categories which their programs of risk analysis and oversight must address, by further defining those categories.[7] It also added and defined another category, enterprise risk management and governance, in order to clarify a requirement already implicit in the statutory mandate to maintain a program of system safeguards risk analysis and oversight. As set out in the NPRM, all seven categories and their definitions are grounded in generally accepted best practices.[8]

[5] 7 U.S.C. 7(d)(20); 7 U.S.C. 5h(f)(14); 7 U.S.C. 24a(c)(8); 17 CFR 38.1050; 17 CFR 37.1400; 17 CFR 49.24(a)(1).

[6] 17 CFR 38.1051(a) and (b) (for DCMs); 17 CFR 37.1401(a); Appendix A to Part 37, Core Principle 14 of Section 5h of the Act—System Safeguards (a) Guidance (1) Risk analysis and oversight program (for SEFs); 17 CFR 49.24(b) and (c) (for SDRs).

[7] The six current categories include information security; business continuity-disaster recovery ("BC-DR") planning and resources; capacity and performance planning; systems operations; systems development and quality assurance; and physical security and environmental controls.

[8] 80 FR 80139, 80143 (Dec. 23, 2015).

3. Requirements to Follow Best Practices, Ensure Testing Independence, and Coordinate BC-DR Plans.

The Commission's current regulations for DCMs and SDRs and its guidance for SEFs provide that such entities should follow best practices in addressing the categories which their programs of system safeguards risk analysis and oversight are required to include.[9] They provide that such entities should ensure that their system safeguards testing, whether conducted by contractors or employees, is conducted by independent professionals (i.e., persons not responsible for development or operation of the systems or capabilities being tested).[10] They further provide that such entities should coordinate their business continuity-disaster recovery ("BC-DR") plans with the BC-DR plans of market participants and essential service providers.[11] The NPRM proposed making these provisions mandatory for all DCMs, SEFs, and SDRs, thus aligning the rules for these entities with the Commission's rules for derivatives clearing organizations ("DCOs").[12]

4. Updating of Business Continuity-Disaster Recovery Plans and Emergency Procedures.

The NPRM proposed amending the current system safeguards rules requiring all DCMs, SEFs, and SDRs to maintain a business continuity-disaster recovery plan and emergency procedures, by adding a requirement for such plans and procedures to be

[9] See § 38.1051(b) (for DCMs); Appendix A to Part 37, Core Principle 14 of Section 5h of the Act—System Safeguards (a) Guidance (1) Risk analysis and oversight program (for SEFs); § 49.24 (c) (for SDRs).

[10] See § 38.1051(h) (for DCMs); Appendix A to Part 37, Core Principle 14 of Section 5h of the Act—System Safeguards (a) Guidance (2) Testing (for SEFs); § 49.24(j) (for SDRs).

[11] See § 38.1051(i) (for DCMs); Appendix A to Part 37, Core Principle 14 of Section 5h of the Act—System Safeguards (a) Guidance (3) Coordination (for SEFs); § 49.24(k) (for SDRs).

[12] 80 FR 80139, 80146 (Dec. 23, 2015).

updated as frequently as required by appropriate risk analysis, but at a minimum at least annually.[13]

5. System Safeguards-Related Books and Records Obligations.

The Commission's current system safeguards rules for all DCMs, SEFs, and SDRs contain a provision addressing required production of system safeguards-related documents to the Commission on request.[14] As noted in the NPRM, production of all such books and records is already required by the Act and Commission regulations, notably by Commission regulation § 1.31.[15] The NPRM proposed amending these document production provisions to further clarify requirements for document production by all DCMs, SEFs, and SDRs relating to system safeguards.[16]

6. Cybersecurity Testing Requirements for DCMs, SEFs and SDRs.

a. Clarification of Current Testing Requirements for All DCMs, SEFs, and SDRs.

The Commission's current system safeguards rules for DCMs, SEFs, and SDRs mandate that each such entity must conduct testing and review sufficient to ensure that its automated systems are reliable, secure, and have adequate scalable capacity.[17] The NPRM proposed clarifying this system safeguards and cybersecurity testing requirement, by specifying and defining five types of system safeguards testing and assessment that a

---

[13] Id. at 80147.

[14] 17 CFR 38.1051(g) and (h) (for DCMs); 17 CFR 37.1401(f) and (g) (for SEFs); 17 CFR 49.24(i) and (j) (for SDRs).

[15] 17 CFR 1.31; see also 17 CFR 38.1051(g) and (h); 17 CFR 37.1401(f) and (g); 17 CFR 49.24(i) and (j).

[16] 80 FR 80139, 80147 (Dec. 23, 2015). The NPRM specified that the obligation to produce books and records includes production of: current copies of BC-DR plans and emergency procedures; assessments of operational risks or system safeguards-related controls; reports concerning system safeguards testing and assessment, whether performed by independent contractors or employees; and all other books and records requested by Commission staff in connection with Commission oversight of system safeguards.

[17] 17 CFR 38.1051(h) (for DCMs); 17 CFR 37.1401(g) (for SEFs); 17 CFR 49.24(j) (for SDRs).

DCM, SEF, or SDR necessarily must perform to fulfill the requirement.[18] These testing and assessment types included vulnerability testing, both external and internal penetration testing, controls testing, security incident response plan testing, and enterprise technology risk assessment. As set out in the NPRM, each of these types of testing is a generally recognized best practice for system safeguards.[19] Providing this clarification of the testing provisions of the current system safeguards rules is a primary purpose of this final rule. The NPRM proposed high-level, minimum requirements for these types of testing, recognizing that the particular ways in which DCMs, SEFs, and SDRs conduct such testing may change as accepted standards and industry best practices develop over time and are reflected in the DCM's, SEF's, or SDR's risk analysis. The NPRM provisions

[18] 80 FR 80139, 80147 (Dec. 23, 2015).

[19] The Commission's current rules and guidance provide that a DCM's, SEF's, or SDR's entire program of risk analysis and oversight, which includes testing, should be based on generally accepted standards and best practices with respect to the development, operation, reliability, security, and capacity of automated systems. See 17 CFR 38.1051(h) (for DCMs); Appendix A to Part 37, Core Principle 14 of Section 5h of the Act—System Safeguards (a) Guidance (1) Risk analysis and oversight program (for SEFs); 17 CFR 49.24(j) (for SDRs). Each of the types of testing addressed in this NPRM—vulnerability testing, penetration testing, controls testing, security incident response plan testing, and enterprise technology risk assessment—has been a generally recognized best practice for system safeguards since before the testing requirements of the Act and the current regulations were adopted. The current system safeguards provisions of the CEA and the Commission's regulations became effective in August 2012. Generally accepted best practices called for each type of testing specified in the proposed rule well before that date, as shown in the following examples. Regarding all five types of testing, see, e.g., NIST SP 800-53A, Rev. 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations ("NIST 800-53A Rev.1"), at E1, F67, F230, F148, and F226, June 2010, available at http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf. Regarding vulnerability testing, see, e.g., NIST SP 800-53A Rev. 1, at F67, June 2010, available at http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf; and NIST SP 800-115, Technical Guide to Information Security Testing and Assessment, at 5-2, September 2008, available at http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf. Regarding penetration testing, see, e.g., NIST Special Publication ("SP") 800-53A, Rev. 1, at E1, June 2010, available at: http://csc.nist.gov/ publications/nistpubs/ 800-53A-rev1/sp800-53A-rev1-final.pdf; and NIST 800-115, at 4-4, September 2008, available at: http://csrc.nist.gov /publications/nistpubs/800-115/SP800-115.pdf. Regarding controls testing, see, e.g., NIST 800-53A, Rev. 1, at 13 and Appendix F1, June 2010, available at http://csrc.nist.gov/publications/nistpubs/ 800-53A-rev1/sp800-53A-rev1-final.pdf. Regarding security incident response plan testing, see, e.g., NIST 800-53A, Rev. 1, at F148, June 2010, available at http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf. Regarding enterprise technology risk assessment, see, e.g., NIST 800-53A, Rev.1, at F226, June 2010, available at http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf.

regarding each of the testing types are set out in additional detail in the discussion below concerning comments received.

b. New Minimum Testing Frequency and Independent Contractor Testing Requirements for Covered DCMs and All SDRs.

The NPRM proposed that covered DCMs (as defined) and all SDRs would be subject to new minimum testing frequency requirements with respect to some of the proposed types of system safeguards testing.[20] To strengthen the objectivity and reliability of the testing, assessment, and information available to the Commission regarding covered DCM and SDR system safeguards, the NPRM also proposed that for certain types of testing, covered DCMs and SDRs would be subject to new independent contractor testing requirements.[21] Establishing such minimum frequency and independent contractor requirements regarding cybersecurity testing by covered DCMs and SDRs is a primary purpose of this final rule. As noted in the NPRM, the proposed minimum frequency requirements and the requirement for some testing to be conducted by independent contractors are grounded in generally accepted standards and best practices.[22] The NPRM provisions regarding the minimum frequency and independent contractor requirements are set out in additional detail below in the discussion of comments received.

7. Additional Testing-Related Risk Analysis and Oversight Program Requirements Applicable to All DCMs, SEFs, and SDRs.

The NPRM also clarified the current testing requirements for DCMs, SEFs, and SDRs by specifying and defining three other aspects of risk analysis and oversight

[20] 80 FR 80139, 80148 (Dec. 23, 2015).

[21] Id.

[22] Id.

programs that are necessary to fulfillment of the testing requirements and achievement of their purposes.[23] These three aspects are: (1) the scope of testing and assessment, (2) internal reporting and review of test results, and (3) remediation of vulnerabilities and deficiencies revealed by testing. As set out in the NPRM, all three of these risk analysis and oversight program aspects are grounded in generally recognized best practices for system safeguards.[24]

a. Scope of Testing and Assessment.

The NPRM proposed that the scope of all testing and assessment required by the Commission's system safeguards regulations for DCMs, SEFs, and SDRs should be broad enough to include all testing of automated systems and controls necessary to identify any vulnerability which, if exploited or accidentally triggered, could enable an intruder or unauthorized user or insider to interfere with the entity's operations or with fulfillment of its statutory and regulatory responsibilities; to impair or degrade the reliability, security, or capacity of the entity's automated systems; to add to, delete, modify, exfiltrate, or compromise the integrity of any data related to the entity's regulated activities; or to undertake any other unauthorized action affecting the entity's regulated activities or the hardware or software used in connection with those activities.[25] The NPRM noted that testing scope should be based on proper risk analysis.[26]

[23] 80 FR 80139, 80159 (Dec. 23, 2015).

[24] Id.

[25] Id.

[26] Id. at 80160.

b. Internal Reporting and Review.

The NPRM called for a DCM's, SEF's, or SDR's senior management and its Board of Directors receive and review reports of the results of all testing and assessment required by Commission rules.[27] It also called for DCMs, SEFs, and SDRs to establish and follow appropriate procedures for remediation of issues identified through such review, and for evaluation of the effectiveness of the organization's testing and assessment protocols.[28] As noted in the NPRM, these requirements are grounded in best practices.[29]

c. Remediation.

The NPRM called for each DCM, SEF, and SDR to analyze the results of the testing and assessment required by the applicable system safeguards rules, in order to identify all vulnerabilities and deficiencies in its systems, and to remediate those vulnerabilities and deficiencies to the extent necessary to enable it to fulfill the applicable system safeguards requirements and meet its statutory and regulatory obligations.[30] The NPRM proposed requiring that such remediation be timely in light of appropriate risk analysis with respect to the risks presented.[31] As noted in the NPRM, such remediation is grounded in best practices.[32]

---

[27] Id.

[28] Id.

[29] Id.

[30] Id.

[31] Id.

[32] Id.

8. Required Production of Annual Total Trading Volume.

The NPRM defined "covered DCM" as a DCM whose annual total trading volume is five percent or more of the annual total trading volume of all DCMs regulated by the Commission.[33] It did so for the purpose of applying the proposed minimum system safeguards testing frequency and independent contractor testing requirements, discussed above, to such covered DCMs. The NPRM noted that this would give DCMs that have less than five percent of the annual total trading volume of all DCMs more flexibility regarding the testing they must conduct, while still requiring all DCMs to conduct testing of all the types addressed in the NPRM.[34] To provide certainty to DCMs as to whether they currently met the definition of a covered DCM, the NPRM called for each DCM to report to the Commission annually its annual total trading volume for the preceding year, and for the Commission to notify each DCM annually of the percentage of the annual total trading volume of all DCMs which is constituted by that DCM's annual total trading volume for the preceding year.[35] The NPRM therefore called for each DCM to report its annual total trading volume for 2015 to the Commission within 30 calendar days of the effective date of the final rule, and to report its annual total volume for 2016 and each subsequent year thereafter to the Commission by January 31 of 2017 and of each calendar year thereafter.[36] The NPRM's definition of covered DCM also addressed cases where a DCM that had been a covered DCM ceased to meet the definitional requirements for covered DCM status, by providing that a covered DCM

[33] Id. at 80148.

[34] Id.

[35] Id. at 80160, 80161.

[36] Id.

having annual total trading volume of less than five percent of the combined annual total trading volume of all regulated DCMs for two consecutive calendar years would cease to be a covered DCM as of March 1 of the calendar year following such two consecutive calendar years.[37] This two-year period permitted completion of the proposed two-year cycle for independent contractor-conducted controls testing.

C. Overview of Comments Received

The comment period for the NPRM closed on February 23, 2016. The Commission received nine comment letters addressing the NPRM. Comments were provided by: the Chicago Mercantile Exchange ("CME") Group DCMs, the CME SEF, and the CME SDR (collectively, "CME"); Intercontinental Exchange, Inc. ("ICE") Futures U.S., ICE Swap Trade, and ICE Trade Vault (collectively, "ICE"); the Minneapolis Grain Exchange ("MGEX"); the North American Derivatives Exchange ("Nadex"); the CBOE Futures Exchange ("CFE"); the Depository Trust and Clearing Corporation Data Repository ("DDR"); Tradeweb Markets LLC ("Tradeweb"); the Wholesale Markets Broker's Association, Americas ("WMBAA"), whose members include BGC SEF, GFI SEF, Tradition SEF, and Tullett Prebon SEF; and FireEye, a third-party cybersecurity service provider.[38]

Most commenters expressed broad support for the proposed system safeguards testing rules. ICE stated that it supports the Commission's efforts to improve, clarify, and enhance its rules relating to system safeguards and address cybersecurity testing, calling clarification and enhancement of these rules in response to escalating and

[37] Id. at 80148.

[38] All comment letters are available on the Commission web site at http://comments.cftc.gov/PublicComments/ CommentList.aspx?id=1650.

evolving cybersecurity threats "timely and welcome," and noting that cybersecurity and system safeguards are paramount to the functioning of the derivatives markets. MGEX said it appreciates and supports the efforts the Commission has put forth to address the growing risk that cyber threats pose to trading markets. Nadex stated that it "commends the Commission's undertaking of this endeavor," that it agrees with the general thrust of the proposed rule, and that it appreciates the Commission's efforts to clarify and enhance the current system safeguards regulations, align requirements with industry standards, and ensure that registrants are meeting compliance thresholds. CFE noted its agreement with the NPRM's approach featuring principles-based testing standards deeply rooted in industry best practices. DDR commended the Commission for its efforts to strengthen system safeguards and cybersecurity testing, and called the proposed rules "constructive steps in addressing key issues." Tradeweb stated that it strongly supports the principles-based testing standards in the NPRM. WMBAA said that it appreciates the Commission's efforts to clarify current system safeguards rule and cybersecurity testing requirements.

Many commenters also offered suggestions and recommendations for clarification or modification of specific NPRM provisions. These comments are addressed as appropriate in connection with the discussion below of the final rule provisions to which they relate. Certain comments requested further clarification relating to definitions provided in the NPRM. Any definitional changes in the final rule are provided for clarification only and do not impose new substantive obligations not included in the NPRM.

D. Advanced Notice of Proposed Rulemaking Regarding Minimum Testing Frequency and Independent Contractor Testing Requirements for Covered SEFs

1. ANPRM Provisions.

The NPRM included an Advanced Notice of Proposed Rulemaking ("ANPRM") concerning Commission consideration of whether to propose in a future NPRM that the most systemically important SEFs should be subject to the same minimum testing frequency and independent contractor testing requirements proposed in the NPRM for covered DCMs and SDRs.[39] In announcing its intent to consider such a proposal, the Commission expressed its belief that, because these requirements were essential to the effectiveness of covered DCM cybersecurity testing and the adequacy of their programs of risk analysis and oversight, it is appropriate to consider whether the same requirements should be applied to the most systemically important SEFs. In the ANPRM, the Commission took note that the SEF market is still in the early stages of development. It also suggested that one possible definition of "covered SEF" could be SEFs for which the annual total notional value of all swaps traded on or pursuant to the rules of the SEF is ten percent or more of the annual total notional value of all swaps traded on or pursuant to the rules of all SEFs regulated by the Commission. However, the ANPRM stated that the Commission would also consider whether annual total notional value or annual total number of swaps traded would provide a more appropriate definition, and whether any definition should apply to swaps in each asset class separately or to all swaps combined regardless of asset class. The Commission requested comments regarding each of these

[39] 80 FR 80139, 80148 (Dec. 23, 2015).

considerations, possible costs and benefits and how they could be quantified or estimated, and any other aspects of the ANPRM.

2. Comments Received.

The Commission received several comments concerning the ANPRM.

Tradeweb called for careful consideration by the Commission, in dialogue with the SEFs to whom any proposal would potentially apply, before issuance of an NPRM on this subject. Tradeweb suggested that, because the SEF market is still in an early stage of development and a covered SEF concept could have a disproportionate impact on the commercial viability of certain SEFs, both the definition of "covered SEF" and the potential costs and benefits involved would require further study and discussion with the industry. To that end, Tradeweb urged the Commission to convene a roundtable or working group of SEFs to discuss the nature and scope of any future SEF-specific system safeguards NPRM before moving forward with such a proposal. Tradeweb advised the Commission to consider the cross-border scope and impact of any future NPRM, and to solicit comment from international regulators either independently or as part of the suggested roundtable or working group.

Several commenters suggested that any future requirements proposed should apply to all SEFs. Tradeweb called for any future proposal to avoid putting certain SEFs at a competitive disadvantage, and to cover all SEFs rather than only systemically important SEFS. WMBAA recommended that the Commission decline to propose a "covered SEF" concept, arguing that: (1) SEF operations do not raise the same systemic concerns attendant on failure of major DCMs or DCOs; (2) products traded on SEFs are fungible across multiple platforms; (3) in the present early stage of the SEF market,

individual SEFs could be "covered" one year but not the next, leading to uncertainty; and (4) the present unsettled nature of the SEF regulatory environment would make adoption of a "covered SEF" concept premature. CME called for the Commission to adopt the same risk based system safeguards requirements for all SEFs, leaving testing frequency to be determined by risk analysis, and avoiding an independent contractor testing requirement.

Tradeweb and WMBAA also suggested that the costs associated with imposition of "covered SEF" requirements could well exceed any benefits derived. However, no commenters offered specific information concerning possible costs.

3. Further Commission Consideration.

The Commission has considered and evaluated the comments received concerning the ANPRM. The Commission agrees with the comments suggesting that further consideration and consultation with both the industry and other relevant regulators and stakeholders would be appropriate and helpful before issuance of any future NPRM regarding "covered SEFs." The Commission also notes the current lack of specific cost and benefit information regarding this concept, and the current absence of a consensus on how "covered SEF" would be best defined in light of the characteristics of swaps and the swap market. Accordingly, the Commission will engage in appropriate consultation prior to determining whether to issue a future NPRM regarding "covered SEFs."

II. THE FINAL RULES

A. Categories of Risk Analysis and Oversight -- §§ 37.1401(a), 38.1051(a), and 49.24(b).

1. Proposed Rule.

As noted above, the NPRM proposed clarification of what is already required of all DCMs, SEFs, and SDRs regarding the categories which their programs of risk analysis and oversight must address, by further defining the six categories addressed by the current rules.[40] It also added and defined another category, enterprise risk management and governance, doing so to clarify a requirement already implicit in the statutory mandate to maintain a program of system safeguards risk analysis and oversight.[41] As set out in the NPRM, all seven categories and their definitions are grounded in generally accepted best practices.[42]

2. Comments Received.

The Commission received three comments on this topic. Two commenters, CME and DDR, concurred with the NPRM's addition of the category of enterprise risk analysis and governance to the list of categories that programs of risk analysis and oversight must address, and suggested clarifications in this respect. CME stated that it recognizes the importance of effective Board oversight, and asked the Commission to confirm that such oversight may appropriately be delegated to Board level committees. CME also asked the Commission to confirm that the final rule will allow regulated entities flexibility of organizational design concerning how their programs of risk analysis and oversight

[40] 80 CFR 80139, 80147 (Dec. 23, 2015).

[41] Id. at 80143.

[42] Id.

address the enterprise risk management and governance category, and will not require that an entity's enterprise risk management function conduct all components of this category. DDR agreed with the Commission that active supervision of system safeguards by both senior management and the Board of Directors promotes more efficient, effective, and reliable risk management, and will better position regulated entities to strengthen the integrity, resiliency, and availability of their automated systems. Noting its agreement that regulated entities should give their boards access to the appropriate system safeguards and cyber resiliency information so as to enable effective oversight, DDR suggested that the final rules should acknowledge that there are multiple ways a regulated entity can ensure that its board is appropriately informed. One commenter, MGEX, questioned why this NPRM proposed adding the category of enterprise risk management and governance, while the Commission's parallel Notice of Proposed Rulemaking addressed to DCOs did not, citing this as an inconsistency between the two NPRMs.[43]

MGEX commented that the NPRM proposed a requirement for all DCMs, SEFs, and SDRs to have a program of risk analysis and oversight, without defining such a program. MGEX also stated that the lists of topics specified in the NPRM as included in each category to be addressed in the required program of risk analysis and oversight were overly prescriptive, citing as an example the list of topics the NPRM specified as included in the category of information security. MGEX suggested that the specified categories should be principles-based and should look to evolving best practices.

[43] See 80 FR 80139, 80113 (Dec. 23, 2015).

3. Final Rule.

The Commission has considered and evaluated the comments concerning addition of the category of enterprise risk analysis and governance to the list of categories which must be addressed by the program of system safeguards-related risk analysis and oversight which the CEA requires all DCMs, SEFs, and SDRs to establish and maintain. For the reasons set forth below, the Commission is adopting the list of categories as proposed.

The Commission continues to believe that addition of the category of enterprise risk analysis and governance is appropriate because this clarifies a requirement already implicit in the statutory mandate to maintain a program of system safeguards risk analysis and oversight.[44] The Commission confirms that the addition of this category does not require that the listed elements of this category be conducted through a particular organizational structure or by particular DCM, SEF, or SDR staff; rather, the final rule provides flexibility in this regard.

The Commission agrees with the comments acknowledging the importance of effective Board of Directors oversight of system safeguards, which the Commission believes is essential to establishing and maintaining the top-down, organization-wide culture of adherence to cybersecurity principles that is required for resilience in today's cybersecurity threat environment. In addition, the Commission agrees with CME's comment that Board of Directors oversight of system safeguards may appropriately be delegated to a Board-level committee or committees, and with DDR's comment that there are a variety of ways in which a DCM, SEF, or SDR can ensure that its Board is

[44] 80 FR 80139, 80143 (Dec. 23, 2015).

sufficiently and appropriately informed to enable it to provide appropriate system safeguards and cybersecurity oversight. In the Commission's view, providing the Board with information sufficient to enable it to provide active, appropriate, knowledgeable, and effective oversight of system safeguards and cybersecurity is the key in this regard.

The Commission has also considered and evaluated MGEX's comment asserting that the NPRM proposed establishment of a requirement for DCMs, SEFs, and SDRs to have a program of system safeguards risk analysis and oversight, without defining such a program, and its comment concerning the lists of topics specified in the NPRM as included in each category to be addressed in the required program of risk analysis and oversight. The requirement for regulatees to have a program of system safeguards risk analysis and oversight was mandated by Congress in the CEA itself, and thus is required by law.[45] The NPRM's references to it did not propose creation of a new requirement in this regard. The Commission's current system safeguards regulations define the program of risk analysis and oversight by specifying the categories of risk analysis and oversight which the program must address. As noted above and in the NPRM, the category of enterprise risk management and governance is implicit and inherent in the statutory requirement itself, and supported by generally accepted standards and best practices.[46]

The Commission agrees with MGEX that the required categories of risk analysis and oversight should be principles-based, but disagrees that the NPRM lists of topics included in each category consist of static lists of controls. As set out in detail in the NPRM, each of the aspects cited in the NPRM for the various categories that the required

[45] CEA § 5(d)(20)(A), 17 USC § 7(d)(20).

[46] 80 FR 80139, 80143 (Dec. 23, 2015).

program of risk analysis and oversight must address is rooted in generally accepted standards and best practices.[47] Because the Commission's current system safeguards rules and guidance provide that DCMs, SEFs, and SDRs should follow generally accepted best practices and standards regarding system safeguards, these entities' programs of risk analysis and oversight should already be addressing each of the aspects included in the NPRM for each risk analysis and oversight category. As the NPRM explicitly states, the aspects specified in the NPRM for each category do not provide all-inclusive or static lists; rather, they highlight important aspects of the categories that are already recognized as best practices.[48] An important benefit of the adherence-to-best-practices approach taken in the Commission's current system safeguards rules, the NPRM generally, and the NPRM provisions addressing the categories in particular, is precisely that such best practices can evolve over time as the cybersecurity field evolves. In addition, the Commission continues to believe, as it stated in the NPRM, that risk analysis and oversight programs that address each of the aspects listed in the NPRM for the risk analysis and oversight categories are essential to maintaining effective system safeguards in today's cybersecurity threat environment.[49]

B. Requirement to Follow Generally Accepted Standards and Best Practices – §§ 37.1401(b), 38.1051(b), and 49.24(c).

1. Proposed Rule.

The NPRM retained the substance of the Commission's current system safeguards rule provision calling for DCMs, SEFs, and SDRs to adhere to generally accepted

[47] Id.

[48] Id.

[49] Id. at 80145.

standards and best practices in their required programs of system safeguards risk analysis and oversight. The only change proposed in the NPRM was language adjustment to clarify that such adherence is mandatory for all DCMs, SEFs, and SDRs.[50]

2. Comments Received.

Several commenters, including CME, Nadex, DDR, Tradeweb, and WMBAA, agreed with the Commission that an entity's program of risk analysis and oversight should follow generally accepted standards and best practices. CME requested that the Commission confirm that generally accepted best practices not explicitly cited in the NPRM may also be used in this regard. CME also asked the Commission to confirm that the intent of this provision is that a regulated entity should take generally accepted best practices into account as it designs a program of risk analysis and oversight tailored to its risks and its appropriate analysis of those risks, rather than to codify particular best practices.

3. Final Rule.

The Commission has considered and evaluated the comments concerning the requirement that a DCM's, SEF's, or SDR's required program of risk analysis and oversight should follow generally accepted standards and best practices. For the reasons set forth below, the Commission is adopting this provision as proposed.

As CME asked the Commission to confirm, the best practices cited in the NPRM do not constitute an exclusive or codified list.[51] DCMs, SEFs, and SDRs should take generally accepted best practices and standards into account as they conduct appropriate

[50] Id. at 80146.

[51] Id.

and current analysis of individual risks and conducts appropriate and effective oversight with respect to such risks. A program of risk analysis and oversight should consider all generally accepted sources of best practices in addressing the particular risks and circumstances of the entity in question in an effective and appropriate way. In the Commission's view, the requirement to follow generally accepted standards and best practices is one of the most important requirements of the Commission's system safeguards rules. Best practices evolve over time in conjunction with the changing cybersecurity threat environment. The agility that a best practices approach therefore provides is crucial to effective resilience with respect to cybersecurity and system safeguards. In addition, ongoing development of best practices benefits from private sector expertise and input, as well as from public sector contributions. Such private sector expertise and input is important to effective cybersecurity. The Commission also observes that requiring financial sector entities to follow best practices with respect to system safeguards and cybersecurity is an effective key to harmonizing the oversight of cybersecurity conducted by different financial regulators. Some financial regulators, such as the FFIEC agencies, are themselves sources of generally accepted best practices. Regulatory oversight of cybersecurity generally follows best practices, most sources of which are largely consonant with each other.

C. Business Continuity-Disaster Recovery Plan -- §§ 37.1401(c), 38.1051(c), and 49.24(d).

1. Proposed Rule.

The Commission's current rules concerning the business continuity-disaster recovery ("BC-DR") plans of DCMs, SEFs, and SDRs require that these entities maintain BC-DR plans and resources, emergency procedures, and backup facilities sufficient to enable timely recovery and resumption of their operations and fulfillment of their responsibilities and obligations as registrants, and specify recovery time. The NPRM proposed further alignment of these provisions with generally accepted standards and best practices by adding a requirement for DCMs, SEFs, and SDRs to update their BC-DR plans and emergency procedures at a frequency determined by an appropriate risk analysis, but at a minimum no less frequently than annually.[52]

2. Comments Received.

CME stated that it agreed with the Commission's proposal to require updating of BC-DR plans and emergency procedures at least annually and more frequently if necessitated by other circumstances.

3. Final Rule.

The Commission has considered and evaluated the comment concerning the frequency of updates to BC-DR plans and emergency procedures, with which it agrees. As noted above, updating such plans at a frequency determined by risk analysis but no less frequently than annually is supported by generally accepted standards and best practices. The Commission is adopting this provision as proposed.

[52] Id. at 80147.

D. Books and Records Requirements -- §§ 37.1401(g), 38.1051(g), and 49.24(i).

1. Proposed Rule.

As noted above, the Commission's current system safeguards rules for all DCMs, SEFs, and SDRs contain a provision addressing required production of system safeguards-related documents to the Commission on request.[53] The NPRM proposed amending these document production provisions to further clarify requirements for system safeguards-related document production.[54] Specifically, the NPRM proposed requiring each DCM, SEF, or SDR to provide to the Commission, promptly on the request of Commission staff: current copies of its BC-DR plans and emergency procedures; all assessments of its operational risks or system safeguards-related controls; all reports concerning system safeguards testing and assessment; and all other books and records requested in connection with Commission oversight of system safeguards.[55]

2. Comments Received.

Two commenters, CME and WMBAA, recognized the Commission's established authority to require production of records, but asked the Commission to continue to work with DCMs, SEFs, and SDRs to find ways that highly sensitive system safeguards-related materials can be made available to Commission staff in ways that maximize protection of their confidentiality. WMBAA suggested that this could be accomplished in appropriate cases by having CFTC staff review highly sensitive information at a registrant's location or in a non-electronic, non-reproducible format.

---

[53] 17 CFR 38.1051(g) and (h) (for DCMs); 17 CFR 37.1401(f) and (g) (for SEFs); 17 CFR 49.24(i) and (j) (for SDRs).

[54] 80 FR 80139, 80147 (Dec. 23, 2015).

[55] Id.

ICE, suggested that, with respect to parent firms that own both CFTC-regulated and non-CFTC-regulated entities, the Commission should avoid requiring production of documents discussing risks at the firm-wide level, and limit its production requests to documents focused solely on the risks of CFTC-regulated entities. In contrast, WMBAA noted that a registrant's systems, such as SEF systems, are often a subset of a larger financial services company's systems, and share cybersecurity defenses, procedures, and testing with the parent entity as a whole, rather than standing alone with respect to cybersecurity. WMBAA suggested that it would be contrary to best practices for CFTC oversight to focus solely on the risks and cybersecurity protections of the CFTC-regulated entity's systems, without considering the related systems and protections of the parent entity.

3. Final Rule.

The Commission has considered and evaluated the comments concerning the books and records provisions of the NPRM. For the reasons set forth below, the Commission is adopting these provisions as proposed.

The established requirements of the Commission's regulations regarding production of books and records are essential to the Commission's ability to fulfill its oversight responsibilities. The Commission also recognizes that the cybersecurity and system safeguards information of DCMs, SEFs, and SDRs can be sensitive. As noted by commenters, Commission staff conducting cybersecurity oversight work regularly with regulated entities to find ways for sensitive cybersecurity information to be made available to the Commission while minimizing the risk of inappropriate disclosure.

The Commission has also considered and evaluated the comments concerning production of books and records that address the system safeguards risks and cybersecurity protections of parent companies. The Commission agrees with WMBAA's observation that the automated systems, programs of system safeguards-related risk analysis and oversight, cybersecurity defenses and testing, and BC-DR plans and resources of CFTC-regulated DCMs, SEFs, and SDRs owned by parent financial sector companies that also own entities not regulated by the Commission are frequently shared across the parent company. Indeed, this is presently the case with respect to the parent companies of all DCMs, SEFs, and SDRs regulated by the Commission which are subsidiaries of a parent company. The Commission disagrees with ICE's suggestion that production of books and records addressing parent-wide system safeguards risks and risk analysis and oversight programs should not be required. Production of all of the books and records specified in the NPRM books and records provision is already required by the Act and Commission regulations, notably by Commission regulation § 1.31.[56] Because DCMs, SEFs, and SDRs often share system safeguards and cybersecurity risks, system safeguards risk analysis and oversight programs, automated systems, business continuity-disaster recovery plans, and other system safeguards and cybersecurity resources with their parent companies, the suggested limitation would in many cases—including the case of ICE itself—cripple the oversight of system safeguards risks and risk analysis and oversight programs for which the CEA makes the Commission responsible, and thus would harm the public interest. The Commission will continue to exercise its authority to require production of all books and records relating to the system safeguards

[56] 80 FR 80139, 80147 (Dec. 23, 2015).

of DCMs, SEFs, and SDRs, including those relating to the system safeguards risks and risk analysis and oversight programs of parent companies where such risks or such programs are shared in whole or in part by a DCM, SEF, or SDR.

E. System Safeguards Testing -- §§ 37.1401(h), 38.1051(h), and 49.24(j).

The provisions of the NPRM addressing automated system testing by DCMs, SEFs, and SDRs retained the language of the Commission's current rules requiring these entities to conduct regular, periodic, objective testing and review of their automated systems to ensure their reliability, security, and adequate scalable capacity.[57] They also retained the language of the current rules requiring regular, periodic testing and review of the business continuity-disaster recovery capabilities of such entities. The NPRM proposed further clarification of the current rules by specifying that such testing and review must include vulnerability testing, penetration testing, controls testing, security incident response plan testing, and enterprise technology risk assessment, and defining certain terms related to such testing.[58]

1. Definitions -- §§ 37.1401(h)(1), 38.1051(h)(1), and 49.24(j)(1).

a. Proposed Rule.

For the purposes of the testing sections of the Commission's system safeguards rules, the NPRM defined the following terms relating to system safeguards testing and assessment by DCMs, SEFs, and SDRs: controls; controls testing; enterprise technology risk assessment; external penetration testing; internal penetration testing; key controls; security incident; security incident response plan; security incident response plan testing;

[57] Id. at 80147, 80148.

[58] Id.

and vulnerability testing. With respect to testing by DCMs, the NPRM also defined the following term: covered designated contract market.[59]

b. Comments Received.

Five commenters, CME, ICE, MGEX, DDR, and WMBAA, provided comments concerning some of the definitions proposed in the NPRM.

(1) External and internal penetration testing.

ICE recommended that the definitions of external and internal penetration testing specify that such testing should include scenario or capture-the-flag testing intended to compromise the system holistically via all available means including technical exploit, social engineering, and lateral traversal. ICE also suggested that the Commission clarify that penetration testing is not intended to include application-specific tests, and recommended that the final rule should avoid specifying parameters for internal penetration testing, in order to allow each regulated entity to determine its own testing methodology. Tradeweb suggested that external penetration testing should be defined to mean penetration testing conducted over the internet. WMBAA suggested that the final rule should not focus on testing from a SEF system's perimeter, but should focus on all the systems supporting the SEF's functionality, whether those of the SEF itself or of its parent company.

(2) Controls and key controls.

As part of its recommendation that the final rule eliminate all requirements for controls testing (addressed in the discussion of controls testing below), ICE

[59] Id. at 80148.

recommended that the final rule should remove the proposed definitions of controls and key controls.

(3) Covered designated contract market.

MGEX commented that the definitional distinction between covered and non-covered DCMs is a valuable concept that recognizes the lower systemic risk posed by smaller entities.[60] However, CME commented that the distinction is unnecessarily complex and imposes undue burdens, and suggested that the final rule adopt a uniform set of standards for all DCMs. CME also suggested that if the covered DCM concept were to be retained, the Commission should consider alternatives to annual DCM reporting of total annual trading volume, because the Commission currently receives volume reports pursuant to DCM Core Principle 8 and part 16 of the Commission's regulations.

(4) Security incident.

The NPRM defined "security incident" as a cyber security or physical security event that actually or potentially jeopardizes automated system operation, reliability, security, or capacity, or the availability, confidentiality, or integrity of data. No comments were received concerning the NPRM definition. However, the Commission received a comment from the Options Clearing Corporation ("OCC") concerning the identical definition included in the parallel Notice of Proposed Rulemaking issued by the

[60] MGEX commented that the Commission should use a similar definition to distinguish between larger and smaller derivatives clearing organizations ("DCOs"). MGEX also made these comments in its comment letter concerning the Commission's NPRM regarding system safeguards testing by DCOs, available at: http://comments.cftc.gov/ PublicComments/ViewComment.aspx?id=60651&SearchText=. Since testing by DCOs is not addressed by this final rule, but will be addressed in the final rule regarding DCO system safeguards testing, these comments are most appropriately addressed in the DCO system safeguards testing final rule, and are addressed there.

Commission on December 15, 2015, proposing to amend its system safeguards rules for DCOs.[61] OCC argued that including in the definition events that "potentially" jeopardize automated systems or data renders the definition vague, and could be interpreted to include most, if not all, cybersecurity events experienced by a DCO. OCC suggested amending the definition to replace "potentially jeopardizes" with "has a significant likelihood of jeopardizing."

Some comments also addressed terms that were used but not defined in the NPRM. Although the NPRM did not define the terms "recovery" or "resumption," DDR commented that, in its view, the NPRM distinguished between resumption of critical functions following a cyber incident on the one hand, and recovery in the sense of restoration of capabilities or services impaired due to a cyber event. Noting that this distinction is consistent with the definitions of these terms in the CMPI-IOSCO Guidance on Cyber Resilience for Financial Market Infrastructures – Consultative Report of November 24, 2015,[62] DDR stated that in this respect the NPRM appropriately recognized differences among financial market infrastructures with respect to varying requirements for recovery and resumption timeframes.

CME, ICE, and MGEX commented concerning the NPRM's use of the terms "independent contractor" and "independent professional." CME asserted that neither term is clearly defined in either the Commission's current rules or the NPRM. ICE called on the Commission to clarify in the final rule that entity employee groups such as the

[61] 80 FR 80113 (Dec. 23, 2015). The OCC comment letter is available at http://comments.cftc.gov/PublicComments/ViewComment.aspx?id=60650&SearchText=.

[62] CPMI-IOSCO, Guidance on Cyber Resilience for Financial Market Infrastructures – Consultative Report (Nov. 2015), at 26, available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD513.pdf.

internal audit function are considered to be independent professionals not responsible for the development of operation of the systems or capabilities tested or assessed in the area of system safeguards. While not commenting directly on these definitions, MGEX expressed the view that having independent testing performed is a key and costly feature proposed in the NPRM.

c. Final Rule.

The Commission has considered and evaluated the comments concerning the definitions proposed in the NPRM. For the reasons discussed below, the final rule will amend the definition of security incident, and otherwise retain the definitions as proposed.

(1) External and internal penetration testing.

The Commission agrees with ICE's suggestion that penetration testing that attempts to compromise an entity's systems holistically through means including technical exploit, social engineering, and lateral traversal is appropriate to today's cybersecurity threat environment. The Commission also agrees with ICE's recommendation that the final rule should avoid specifying particular internal penetration testing parameters in order to give DCMs, SEFs, and SDRs flexibility in determining their particular methodology for such testing, and believes that approach is also appropriate regarding external penetration testing. Best practices indicate that with respect to penetration testing, entities should regularly "update the list of attack techniques and exploitable vulnerabilities used in penetration testing based on an organizational assessment of risk or when significant new vulnerabilities or threats are

identified and reported."[63] Where penetration testing that attempts to compromise systems holistically through means including technical exploit, social engineering, and lateral traversal is called for by appropriate risk analysis, as it may be in most or even all cases, the final rule will require penetration testing using such means, by virtue of its requirement for all DCMs, SEFs, and SDRs to follow best practices, and its requirement for all DCMs, SEFs, and SDRs to make the scope of their cybersecurity testing broad enough to include all testing that their programs of risk analysis and current cybersecurity threat analysis indicate is necessary. The Commission notes that essential penetration testing methods and techniques may change over time, based on an entity's appropriate risk analysis, technological changes, and the evolving nature of cybersecurity threats. The Commission disagrees with Tradeweb's suggestion that external penetration testing should be defined as testing conducted over the internet. Best practices indicate that external penetration testing should be conducted from multiple vectors including remote access, virtual private network connections, and any separate environments or local area network segments, as well as the internet.[64] In addition, such testing should include not only internet based or network-layer based tests but also application-layer assessments. The Commission agrees with WMBAA's comment that penetration testing must include testing of all systems supporting a regulated entity's functionality or involved in the

[63] NIST SP 800-53A, Rev. 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations – Building Effective Assessment Plans, at E-1, http://nvlpubs.nist.gov/nistpubs/SpecialPublications /NIST.SP.800-53Ar4.pdf.

[64] See, e.g., Security Standards Council, Payment Card Industry Data Security Standards, Apr. 2016, v. 3.2 ("PCI DSS"), available at https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf, Information Supplement: Penetration Testing Guidance, at 5-8, available at https://www.pcisecuritystandards.org/documents/ Penetration_Testing_Guidance_March_2015.pdf; and Center for Internet Security, Critical Security Controls, at 68-69, available at https://www.cisecurity.org/critical-controls/.

entity's system safeguards, whether the systems belong to the entity itself or to the entity's parent company.

(2) Covered designated contract market.

The Commission has considered and evaluated the comments for and against the NPRM's definitional distinction between covered and non-covered DCMs. The Commission continues to believe that the NPRM's proposed requirements regarding the minimum frequencies at which various types of cybersecurity testing should be conducted and regarding the use of independent contractors to perform specified tests are important and appropriate in today's cybersecurity threat environment. As noted in the NPRM, these requirements aim to strengthen the objectivity and reliability of the testing and assessment information available to the Commission regarding system safeguards, and to ensure the effectiveness and timeliness of both cybersecurity testing and programs of risk analysis and oversight.[65] Additionally, the use of independent contractors for many types of testing is consonant with best practices. The Commission also continues to believe that application of these requirements to DCMs whose annual total trading volume is five percent or more of the annual total trading volume of all DCMs regulated by the Commission is appropriate. This approach reduces possible costs and burdens for smaller and less systemically critical DCMs, by giving them additional flexibility regarding their cybersecurity testing. The fact that smaller DCMs will still be required to conduct testing of all the types addressed in the final rule means that this approach will not impair the fundamental goals of the CEA and the Commission's system safeguards regulations. The NPRM also proposed offering such added flexibility to SEFs, which

[65] 80 FR 80139, 80148 (Dec. 23, 2015).

like non-covered DCMs are required to conduct all of the specified types of testing but not made subject to the minimum frequency and independent contractor requirements. The Commission continues to believe this to be appropriate as well, for the same reasons.[66]

The Commission declines CME's suggestion that it rely on DCM volume reports submitted pursuant to part 16 of the Commission's regulations. The Commission notes that while it receives daily trade information from DCMs pursuant to part 16, it does not receive total annual trading volume information from DCMs.[67] The Commission believes that DCM submission of annual trading volume requirement is essential for the Commission to accurately evaluate whether a particular DCM must comply with the frequency and independent contractor requirements as a covered DCM. The Commission believes that annual total trading volume information is readily available to DCMs, and that DCMs generally calculate their annual trading volume in the usual course of business. The Commission does not believe that looking up the amount of a DCM's annual total trading volume and reporting that amount to the Commission once a year, something that can be done by email in thirty minutes or less, can reasonably be said to impose an undue burden on a DCM.

(3) Security incident.

The Commission has considered and evaluated OCC's comment concerning the definition of "security incident" included in the Commission's parallel NPRM proposing amendment of its system safeguards rules for DCOs. The Commission is amending the

---

[66] Id.

[67] Core Principle 8 is inapplicable here, because it requires DCMs to publish daily volume information but does not require submission of that information to the Commission.

definition as the comment suggested, defining security incident as a cyber security or physical security event that "actually jeopardizes or has a significant likelihood of jeopardizing" automated systems or data. The definition included in the DCO NPRM is identical to the one included in the NPRM regarding DCMs, SEFs, and SDRs. The Commission issued the two NPRMs simultaneously and in parallel, and intended that the final rules issued in connection with both NPRMs should be closely aligned. Accordingly, the Commission believes the comment received is germane to both final rules. The Commission also notes that the amendment of this definition does not expand the definition's reach but rather narrows it somewhat, and therefore lightens any costs or burdens involved to at least some degree.

(4) Recovery and resumption.

With respect to DDR's comment regarding the terms "recovery" and "resumption," the Commission notes that the NPRM did not, and the final rule will not, define these terms or make any change to the language or the requirements of the Commission's current system safeguards rules for DCMs, SEFs, or SDRs regarding recovery and resumption of operations and fulfillment of responsibilities and obligations as a registered entity.

(5) Independent contractor and independent professional.

The Commission has considered and evaluated the various comments concerning the terms "independent contractor" and "independent professional" used in the NPRM.[68] The Commission notes that both terms are effectively defined in the Commission's current system safeguards rules for DCMs and SDRs and its current system safeguards

[68] 80 FR 80139, 80146 through 80161 (Dec. 23, 2015).

rules and guidance for SEFs.[69] These current provisions call for the system safeguards testing required of all DCMs, SEFs, and SDRs to be conducted by qualified, independent professionals, who:

> may be independent contractors or employees of the [DCM, SEF, or SDR], but should not be persons responsible for development or operation of the systems or capabilities being tested.[70]

Accordingly, for purposes of the current system safeguards rules, independent contractors are qualified system safeguards professionals who are not employees of the DCM, SEF, or SDR. The current rules use the terms independent contractor and employee as they are legally defined and generally used.[71] The Commission believes that the distinction between independent contractor and employee is well settled and understood, and does not need additional definition in the system safeguards rules.

With respect to system safeguards testing, the current rules provide that employees conducting required testing must be independent in that they are not employees responsible for development or operation of the systems or capabilities being tested. The Commission believes that this distinction between employees with sufficient independence to appropriately conduct required system safeguards testing and those who lack such independence is also sufficiently clear, and does not require additional definition. The NPRM used, and the final rule will retain, this language from the current system safeguards rules. Where this requirement is included, the testing in question must

---

[69] 17 CFR §§ 38.1051(h) (for DCMs); 37.1401 (g) and Appendix B to Part 37, Core Principle 14 of Section 5h of the Act—System Safeguards (C)(a)(2) (for SEFs); 49.24(j) (for SDRs).

[70] Id.

[71] See, e.g., Black's Law Dictionary, Tenth Ed. (Thomson Reuters, St. Paul, MN, 2014) ("Employee. Someone who works in the service of another person (the employer) under an express or implied contract of hire, under which the employer has the right to control the details of work performance.") ("Independent Contractor. Someone who is entrusted to undertake a specific project but who is left free to do the assigned work and to choose the method for accomplishing it.")

be conducted by employees who are independent, which means employees not responsible for developing or operating what is being tested.[72] Employees who are part of the internal audit function of a DCM, SEF, or SDR, are one example of employees having appropriate independence. Other employees who possess the specified degree of independence and have qualifications the DCM, SEF, or SDR believes are appropriate may also be suitable in such cases.

One clarification may be helpful with respect to testing required to be performed by independent contractors, as distinct from testing performed by persons performing the internal audit function. As noted above, the internal audit function is a required aspect of the enterprise risk management and governance category which must be included in the program of risk analysis and oversight that a DCM, SEF, or SDR must maintain. It is an integral part of, and a responsibility of, the regulated entity, whether carried out in-house or outsourced. The NPRM proposed required testing by independent contractors in part to give the Commission's system safeguards oversight a third source of system safeguards information on which to rely, in addition to the entity's employees and its internal audit function.[73] It also proposed independent contractor testing to give the regulated entity the benefit of a truly outside perspective concerning system safeguards, not colored by beginning from the institutional point of view, something that best practices say is important as noted earlier. Accordingly, testing performed by persons executing the internal audit function will not fulfill the requirement for testing by independent contractors, whether it is performed by employees executing the internal

[72] This requirement is included in the final rule provisions concerning most types of testing, but as discussed below is not included in the SIRP testing provision.

[73] 80 FR 80139, 80148 (Dec. 23, 2015).

audit function or by internal audit contractors to whom a DCM, SEF, or SDR outsources part or all of its internal audit function.

2. Vulnerability Testing -- §§ 37.1401(h)(2), 38.1051(h)(2), and 49.24(j)(2).

a. Proposed Rule.

The NPRM called for all DCMs, SEFs, and SDRs to conduct vulnerability testing of a scope sufficient to satisfy the requirements in the proposed rule.[74] It proposed requiring all such entities to conduct vulnerability testing at a frequency determined by an appropriate risk analysis, with a minimum frequency requirement of quarterly vulnerability testing for covered DCMs and SDRs.[75] The NPRM called for vulnerability testing to include automated vulnerability scanning, conducted on an authenticated basis where indicated by appropriate risk analysis, with compensating controls where scanning is conducted on an unauthenticated basis. The NPRM called for covered DCMs and SDRs to engage independent contractors to conduct two of the minimum quarterly vulnerability tests required of them each year.[76] It provided that all other vulnerability testing by covered DCMs and SDRs, and all vulnerability testing by non-covered DCMs and SEFs, should be conducted either by independent contractors or by employees not responsible for development or operation of the systems or capabilities being tested.[77]

[74] 80 FR 80139, 80148 through 80151 (Dec. 23, 2015).

[75] Id. at 80149, 80150.

[76] Id. at 80150.

[77] Id. at 80150, 80151.

b. Comments Received.

(1) Requirement for vulnerability testing.

Several commenters, including CME, ICE, and Nadex, agreed that the NPRM's call for vulnerability testing was appropriate, because such testing is critical to identification and remediation of cybersecurity vulnerabilities. CME stated that vulnerability testing, of a scope aligned with risk analysis, should be embedded in an organization's systems development life cycle, in order to promote a culture of awareness as early and close to the first line of defense as possible.

(2) Vulnerability testing frequency.

Commenters, including CME and ICE, supported the minimum quarterly vulnerability testing frequency requirement for covered DCMs and SDRs. CME noted that at least quarterly testing is likely to be an appropriate frequency for most organizations where critical assets are concerned. Regarding the requirement to test as often as indicated by appropriate risk analysis, CME agreed that vulnerability testing frequency should be aligned with appropriate risk analysis. MGEX called for the final rule to leave the frequency of vulnerability testing to be determined by regulatees. ICE argued that regulatees should not be subject to a formal risk assessment to potentially determine a higher vulnerability testing frequency. Nadex asked the Commission to confirm that the level of detail in the risk assessment used to determine appropriate vulnerability testing frequency is that called for by generally accepted standards and best practices.

(3) Automated scanning and authenticated scanning.

Commenters raised no issue with the NPRM requirement for vulnerability testing to include automated vulnerability scanning. ICE called for removal of the requirement for automated scanning to include authenticated scanning, arguing that this requirement would increase the cost and time of a scan, increase risk through creation of an operating system login on a new system, and have limited utility in the context of financial system infrastructure.

(4) Vulnerability testing by independent contractors.

A number of commenters argued that the use of independent contractors for vulnerability testing could undesirably increase risks. CME suggested that outsider access to systems can broaden both operations risk and the risk of disclosure of sensitive information, and noted that there is a limited supply of independent contractors with appropriate qualifications for vulnerability testing. ICE commented that vulnerability scanners can be hazardous to systems, can cause issues during deployment, and require a high level of care to avoid live system jeopardy, including both intimate network knowledge and change control interaction. In short, ICE stated, third-party vulnerability scanning would be costly and potentially dangerous without adding value. DDR stated that vulnerability testing by independent contractors would introduce unnecessary risk to critical infrastructure and heighten the risk of systems outages. These commenters therefore requested that the final rule eliminate the independent contractor requirement for vulnerability testing, and permit such testing to be conducted by entity employees not responsible for development or operation of the systems or capabilities tested. CME suggested that allowing such employees to conduct vulnerability testing has been proven

effective, allows testing by those with the greatest knowledge and experience concerning the systems tested, and has the benefit of promoting an organizational culture of cybersecurity awareness. DDR recommended that SDR employees conduct vulnerability testing, and that independent contractors review testing procedures to confirm that they are effective and consonant with industry standards.

c. Final Rule.

The Commission has considered and evaluated the comments concerning vulnerability testing. For the reasons set out below, the final rule will call for vulnerability testing and include the proposed vulnerability testing frequency requirements, but will not require that automated vulnerability scanning include authenticated scanning, and will not require the use of independent contractors as proposed.

(1) Requirement for vulnerability testing.

The Commission agrees with commenters that vulnerability testing is critical to identification and remediation of cybersecurity vulnerabilities. It is an essential component of an effective program of risk analysis and oversight, and an essential means of fulfilling the testing requirements of the Commission's current system safeguards rules.

(2) Vulnerability testing frequency.

The Commission agrees with the comments supporting the minimum quarterly vulnerability testing requirement for covered DCMs and SDRs, and agrees that, in today's cybersecurity environment, most organizations should conduct such testing at least quarterly. The Commission also agrees that, beyond the minimum frequency

proposed for covered DCMs and SDRs, all DCMs, SEFs, and SDRs should conduct vulnerability testing as frequently as indicated by appropriate risk analysis. The Commission disagrees with the suggestion that the frequency of vulnerability testing should simply be left to these entities themselves. It is essential for such testing to be conducted as frequently as indicated by analysis of a particular entity's risks, which is likely in most cases to call for testing at least quarterly. The risk analysis referred to in the NPRM in this connection is the appropriate risk analysis which each DCM, SEF, and SDR must conduct and maintain as an integral part of the program of risk analysis and oversight that the CEA requires. ICE apparently misunderstood the NPRM as calling for a separate, formal risk analysis made for the specific purpose of determining vulnerability testing frequency. That is not required; what is required is vulnerability testing as often as indicated by the ongoing, appropriate risk analysis inherent in a regulatee's required program of risk analysis and oversight. As provided in the current system safeguards rules and in the NPRM, the program of risk analysis required of a DCM, SEF, or SDR, and the risk analyses inherent in that program, are indeed to be conducted in light of generally accepted standards and best practices.[78]

(3) Automated scanning and authenticated scanning.

No commenters disagreed with the proposed requirement for vulnerability testing to include automated vulnerability scanning. In light of ICE's suggestion that the proposed requirement for automated scanning to include authenticated scanning could increase costs, burdens, and risks while having limited utility for DCMs, SEFs, and SDRs, the Commission has decided to remove the authenticated scanning requirement

[78] 80 FR 80139, 80149, 80150 (Dec. 23, 2015).

from the final rule. Instead, the final rule provides that automated vulnerability scanning must follow best practices. The Commission notes that, to the extent that best practices require or come to require authenticated scanning, such scanning would be mandatory pursuant to the requirement to follow best practices, and would be addressed in system safeguards examinations.

(4) Vulnerability testing by independent contractors.

The Commission has carefully considered the multiple comments suggesting that use of independent contractors for vulnerability testing could undesirably increase risks, raise hazards for automated systems, and increase costs and dangers without adding value. The Commission has also noted the comment that vulnerability testing conducted by employees not responsible for development or operation of the systems or capabilities tested has been proven effective, provides expertise valuable in vulnerability testing, and promotes an organizational culture of cybersecurity awareness. For these reasons, and in order to reduce costs and burdens to the extent practicable while still achieving the purposes of the CEA and of the NPRM, the final rule does not include the proposed requirement for covered DCMs and SDRs to have some vulnerability testing conducted by independent contractors. Instead, the final rule permits all DCMs, SEFs, and SDRs to conduct all required vulnerability testing by using either independent contractors or entity employees not responsible for development or operation of the systems or capabilities being tested. The Commission acknowledges the value of DDR's recommendation that independent contractors evaluate the effectiveness of the regulatee's vulnerability testing procedures and their consistency with best practices. While the final rule's vulnerability testing provisions will not incorporate such a requirement, the Commission observes that

such independent validation of vulnerability testing procedures should likely be included as part of a regulatee's controls testing program.

3. External Penetration Testing -- §§ 37.1401(h)(3), 38.1051(h)(3), and 49.24(j)(3).

a. Proposed Rule.

The NPRM called for all DCMs, SEFs, and SDRs to conduct external penetration testing of a scope sufficient to satisfy the requirements in the proposed rule.[79] It proposed requiring all such entities to conduct external penetration testing at frequency determined by an appropriate risk analysis, with a minimum frequency requirement of annual external penetration testing for covered DCMs and SDRs.[80] The NPRM called for covered DCMs and SDRs to engage independent contractors to conduct the annual external penetration test required of them.[81] It provided that all other external penetration testing by covered DCMs and SDRs, and all external penetration testing by non-covered DCMs and SEFs, should be conducted either by independent contractors or by employees not responsible for development or operation of the systems or capabilities being tested.[82]

b. Comments Received.

(1) Requirement for external penetration testing.

Commenters raised no issue with the NPRM's call for external penetration testing. CME noted that penetration testing is a significant component of the program to identify and minimize sources of operational risk required of all DCMs, SEFs, and SDRs.

[79] 80 FR 80139, 80152 (Dec. 23, 2015).

[80] Id. at 80152, 80153.

[81] Id. at 80153.

[82] Id. at 80152, 80153.

CME also approved the flexibility concerning penetration test design provided in the NPRM. Nadex noted its agreement with the NPRM's penetration testing requirement.

(2) External penetration testing frequency.

Commenters also raised no issue with the requirement for all DCMs, SEFs, and SDRs to conduct external penetration testing at a frequency determined by appropriate risk analysis. CME noted that many risk based factors should inform the frequency of such testing. Several commenters also supported the annual minimum frequency requirement for external penetration testing by covered DCMs and SDRs. CME stated that annual external penetration testing generally will be appropriate, ICE stated that it agrees with the annual requirement, and Nadex agreed with the NPRM's penetration testing requirements. MGEX called for the final rule to leave the frequency of external penetration testing to be determined by regulatees. ICE argued that regulatees should not be subject to a formal risk assessment to potentially determine a higher penetration testing frequency.

(3) External penetration testing by independent contractors.

Most commenters raised no issue with the requirement for covered DCMs and SDRs to have the required annual external penetration test conducted by independent contractors. DDR commented generally that an SDR should have flexibility regarding whether to have testing conducted by independent contractors or employees not responsible for development or operation of the systems or capabilities tested, based on the risks of that SDR.

c. Final Rule.

The Commission has considered and evaluated the comments concerning external penetration testing. For the reasons discussed below, the final rule will include the NPRM provisions regarding such testing as proposed.

(1) Requirement for external penetration testing.

The Commission agrees with commenters that external penetration testing is a significant and essential component of an effective program of system safeguards risk analysis and oversight. Such testing is an essential means of fulfilling the testing requirement in the Commission's current system safeguards rules.

(2) External penetration testing frequency.

The Commission agrees with the comment that many risk based factors should inform the frequency of external penetration testing, and notes that this is true for all DCMs, SEFs, and SDRs. The Commission also agrees with the comments supporting the minimum frequency requirement of annual external penetration testing by covered DCMs and SDRs. As noted in the NPRM, this requirement is supported by generally accepted standards and best practices, which make it clear that such testing at least annually is essential to adequate system safeguards in today's cybersecurity environment. For this reason, the Commission disagrees with the suggestion that the frequency of such testing by covered DCMs and SDRs should be left to determination by those entities themselves. The proposal's minimum requirement was for a single annual test; although, as noted in the NPRM, adequate risk analysis could well require more frequent testing in light of the risks faced by a particular regulatee.[83] A separate, formal risk analysis made for the

[83] Id. at 80152.

specific purpose of determining external penetration testing frequency is not required. Rather, external penetration testing is required as often as indicated by the ongoing, appropriate risk analysis inherent in a regulatee's statutorily-required program of risk analysis and oversight, conducted in light of generally accepted standards and best practices.

(3) External penetration testing by independent contractors.

In determining the final rule's provisions regarding external penetration testing by independent contractors, the Commission has noted that, as set forth above, most commenters raised no issue with this requirement for covered DCMs and SDRs. As noted in the NPRM, generally accepted standards and best practices make it clear that independent testing by third party service providers is an essential component of an adequate testing regime, and that this is notably the case with respect to penetration testing.[84] The Commission believes that the independent viewpoint and approach provided by independent contractors, who can conduct a penetration test from the perspective of an outside adversary uncolored by insider assumptions or blind spots, will benefit covered DCM and SDR programs of risk analysis and oversight. Independent contractor penetration testing will strengthen Commission oversight of system safeguards, by providing an important, credible third source of information in addition to what is available from covered DCM or SDR staff and from the internal audit function of those entities. In light of these considerations, the Commission disagrees with the comments suggesting elimination of the requirement for the minimum annual external penetration test of a covered DCM or SDR to be conducted by independent contractors.

[84] Id. at 80153.

4. Internal Penetration Testing -- §§ 37.1401(h)(4), 38.1051(h)(4), and 49.24(j)(4).

a. Proposed Rule.

The NPRM called for all DCMs, SEFs, and SDRs to conduct internal penetration testing of a scope sufficient to satisfy the requirements in the proposed rule.[85] It proposed requiring all such entities to conduct external penetration testing at a frequency determined by an appropriate risk analysis, with a minimum frequency requirement of annual internal penetration testing for covered DCMs and SDRs.[86] The NPRM provided that all internal penetration testing by DCMs, SEFs, or SDRs should be conducted either by independent contractors or by employees not responsible for development or operation of the systems or capabilities being tested.[87]

b. Comments Received.

(1) Requirement for internal penetration testing.

Commenters raised no issue with the NPRM's call for internal penetration testing. As noted above concerning external penetration testing, CME noted that penetration testing generally is a significant component of the program to identify and minimize sources of operational risk required of all DCMs, SEFs, and SDRs, and approved the flexibility concerning penetration test design provided in the NPRM. Also as noted above, Nadex stated its agreement with the NPRM's penetration testing requirements.

(2) Internal penetration testing frequency.

Commenters also raised no issue with the requirement for all DCMs, SEFs, and SDRs to conduct internal penetration testing at a frequency determined by appropriate

[85] 80 FR 80139, 80152 (Dec. 23, 2015).

[86] Id. at 80152, 80153.

[87] Id.

risk analysis. As noted above, CME stated that many risk based factors should inform the frequency of penetration testing generally. With respect to the requirement for covered DCMs and SDRs to conduct internal penetration testing at least annually, ICE stated agreement with the proposal. Nadex agreed with the proposed penetration testing requirements generally. On the basis that that there is a scarcity of potential employees with the skill set required to conduct internal penetration testing without introducing risks into the production environment and other sensitive environments, CME suggested making annual internal penetration testing an objective rather than a requirement, so that covered DCMs and SDRs can prioritize truly effective testing over less skilled testing done merely to satisfy the annual requirement. As noted above, MGEX called for the final rule to leave the frequency of penetration testing to be determined by regulatees. ICE argued that regulatees should not be subject to a formal risk assessment to potentially determine a higher penetration testing frequency.

(3) Who should perform internal penetration testing.

Commenters raised no issue with the NPRM provision giving all DCMs, SEFs, and SDRs the choice of whether to have internal penetration testing performed by independent contractors or by employees not responsible for development or operation of the systems or capabilities tested.

c. Final Rule.

The Commission has considered and evaluated the comments concerning internal penetration testing. For the reasons discussed below, the final rule will include the NPRM's internal penetration testing provisions as proposed.[88]

[88] 80 FR 80139, 80152, 80153 (Dec. 23, 2015).

(1) Requirement for internal penetration testing.

The Commission agrees with commenters that external penetration testing is a significant and essential component of an effective program of system safeguards risk analysis and oversight. Such testing is an essential means of fulfilling the testing requirement in the Commission's current system safeguards rules.

(2) Internal penetration testing frequency.

The Commission agrees with the comment that many risk based factors should inform the frequency of internal penetration testing, and notes that this is true for all DCMs, SEFs, and SDRs. It also agrees with the comments supporting the minimum frequency requirement of annual internal penetration testing by covered DCMs and SDRs. As noted in the NPRM, this requirement, like the parallel requirement regarding external penetration testing, is supported by generally accepted standards and best practices, which make it clear that such testing at least annually is essential to adequate system safeguards in today's cybersecurity environment.[89] Accordingly, the Commission disagrees with the suggestions that annual internal penetration testing by covered DCMs and SDRs should be a mere objective, or that the frequency of such testing by covered DCMs and SDRs should be left to determination by those entities themselves. The Commission also notes, as it stated in the NPRM, that adequate risk analysis could well require more frequent testing in light of the risks faced by a particular regulatee.[90] A separate, formal risk analysis made for the specific purpose of determining internal penetration testing frequency is not required. Rather, internal penetration testing is

[89] Id.

[90] Id.

required as often as indicated by the ongoing, appropriate risk analysis inherent in a regulatee's required program of risk analysis and oversight, conducted in light of generally accepted standards and best practices.

(3) Who should perform internal penetration testing.

The Commission continues to believe, as provided in the NPRM, that it is appropriate to give all DCMs, SEFs, and SDRs the choice of whether to have internal penetration testing performed by independent contractors or by employees not responsible for development or operation of the systems or capabilities tested.[91] Commenters raised no issue with this provision.

5. Controls Testing -- §§ 37.1401(h)(5), 38.1051(h)(5), and 49.24(j)(5).

a. Proposed Rule.

The NPRM called for each DCM, SEF, and SDR to conduct controls testing of a scope sufficient to satisfy the scope requirements in the proposed rule, including testing of each control included in the entity's program of risk analysis and oversight.[92] It proposed each such entity to conduct controls testing at frequency determined by an appropriate risk analysis, with a minimum frequency requirement for covered DCMs and SDRs calling for testing of all controls every two years.[93] The NPRM provided that covered DCMs and SDRs could conduct such testing on a rolling basis over the minimum two-year period or over the minimum period determined by appropriate risk analysis, whichever is shorter.[94] The NPRM called for covered DCMs and SDRs to engage

[91] Id. at 80153.

[92] Id. at 80153, 80154.

[93] Id. at 80154.

[94] Id.

independent contractors to conduct testing of key controls no less frequently than every two years.[95] It provided that all other controls testing by covered DCMs and SDRs, and all controls testing by non-covered DCMs and SEFs, should be conducted either by independent contractors or by employees not responsible for development or operation of the systems or capabilities being tested.[96]

b. Comments Received.

(1) Requirement for controls testing.

CME and Nadex approved of the NPRM's call for controls testing. CME stated that the NPRM correctly identified controls testing as a crucial part of a program of risk analysis and oversight, and agreed with the categories which the current rules and the NPRM specify as included in such a program. CME also agreed with the NPRM's flexible approach to using best practices to inform the design and implementation of controls testing in light of risk analysis. ICE called for the final rule to eliminate the requirement for controls testing, arguing that many controls do not require testing, that few organizations have a static universe of controls, and that control weaknesses will come to light in vulnerability and penetration testing. Tradeweb asked the Commission to provide further guidance on how controls testing differs from vulnerability testing, whether Service Organization Controls ("SOC") 1 and 2 reports prepared in accordance with the American Institute of Certified Public Accountants' Statement on Standards for Attestation Engagements ("SSAE") Number 16 could be used for controls testing

[95] Id.

[96] Id. at 80154, 80155.

purposes, and whether penetrations tests could be used to fulfill controls testing requirements.

(2) Controls testing frequency.

Regarding the minimum controls testing frequency of every two years proposed for covered DCMs and SDRs, CME commented that some less critical controls do not warrant testing on a two-year cycle, and cited best practices permitting controls testing on a three-year cycle. CME suggested that the final rule should call for the minimum controls testing frequency for covered DCMs and SDRs to be determined by risk analysis (as the NPRM proposed for non-covered DCMs and SEFs), or alternatively that a minimum frequency cycle of three years would be a reasonable alternative to the NPRM's proposed two-year cycle. CME suggested that, while many organizations will implement a two-year schedule for at least the testing of key controls, either of CME's proposed alternatives would make controls testing more cost effective, and increase focus on the most critical controls.

(3) Who should perform controls testing.

CME commented that effective testing of key controls can be done by employees not responsible for development or operation of the controls tested, as well as by independent contractors, and that such independent employees' familiarity with the organization's controls can improve the efficiency and effectiveness of controls testing. Accordingly, CME suggested that, while independent contractor controls testing may be beneficial, the final rule should not exclude controls testing by independent employees, for example employees such as internal audit staff. DDR also commented that, where the NPRM proposed to require independent contractor testing, the final rule should give

flexibility to use either independent contractors or independent employees. ICE suggested that the final rule should not require key controls testing at all. In support, ICE argued that the concept of key controls is not universally adopted; that risk analysis relies on testing of all controls in concert; that a testing requirement directed at key controls could result in organizations documenting fewer controls; and that the key controls testing proposal would impose a large burden for little or no practical improvement in security. MGEX stated that the NPRM required testing of all controls on a rolling basis by independent contractors every two years.

c. Final Rule.

The Commission has considered and evaluated the comments concerning controls testing. For the reasons discussed below, the Commission is adopting the NPRM's requirement for all DCMs, SEFs, and SDRs to conduct testing of all their system safeguards-related controls, its requirement for such testing by all such entities to be conducted as often as indicated by appropriate risk analysis, and its requirement for independent contractor testing of the key controls of covered DCMs and SDRs. However, for the reasons discussed below concerning controls testing frequency, the Commission is modifying the proposed controls testing minimum frequency requirement for covered DCMs and SDRs, to call for testing of their key controls—including independent contractor testing of such controls—within a three-year rather than a two-year period.

(1) Requirement for controls testing.

The Commission agrees with commenters that controls testing is a crucial part of a program of risk analysis and oversight and that best practices should inform the design

and implementation of controls testing in light of risk analysis. In today's rapidly-changing cybersecurity threat environment, regular, ongoing controls testing that verifies over time the effectiveness of each system safeguards control used by a DCM, SEF, or SDR is essential to ensuring the continuing overall efficacy of the entity's system safeguards. The Commission disagrees with the suggestion that the final rule should not require any controls testing. As noted in the NPRM, generally accepted standards and best practices call for such testing.[97] Moreover, in conducting oversight of system safeguards, Commission staff have found a significant number of instances, at both larger and smaller entities, where (a) system malfunctions, market halts, and the success of cyber intrusions were caused by failures of both key and non-key controls; (b) such problems could have been prevented had the controls in question been tested; and (c) testing of the relevant controls had been entirely omitted or not done for substantial periods of time. The controls testing requirement set out in the NPRM is designed to remedy such situations, and ensure that controls testing by all DCMs, SEFs, and SDRs follows best practices. By design, the NPRM did not prescribe the design of the overall program of controls testing or the particular tests it may include. Various forms of testing, including vulnerability testing, penetration testing, SSAE16 SOC1 or SOC2 assessments, and others, may well contribute in varying degrees—subject to their particular natures and limitations—to an overall program for the testing of controls as called for by the NPRM. The Commission notes that the depth and coverage of a single assessment may not be sufficient to meet the final rule's testing scope requirements discussed below. It also notes that the proposed controls testing requirement gives

[97] 80 FR 80139, 80152 (Dec. 23, 2015).

DCMs, SEFs, and SDRs the flexibility to determine the appropriate combination of testing methods and techniques necessary to determine whether their controls are implemented correctly, operating as intended, and enabling them to meet the system safeguards requirements of the Commission's rules.

(2) Controls testing frequency.

The Commission has noted the best practices cited by CME supporting controls testing on a three-year cycle. After due consideration, the Commission agrees that a three-year rather than two-year minimum controls testing frequency requirement for covered DCMs and SDRs may reduce costs and burdens, while providing beneficial flexibility in overall controls testing program design and still ensuring that the fundamental purposes of the CEA and the Commission's system safeguards rules are achieved. The NPRM called for covered DCMs and SDRs, as well as non-covered DCMs and SEFs, to conduct controls testing as frequently as appropriate risk analysis requires.[98] The Commission notes that this fundamental frequency requirement could well require a controls testing cycle shorter than three years, as acknowledged in the comment on this point. In light of these considerations, the final rule requires all DCMs, SEFs, and SDRs to test the controls included in their programs of risk analysis and oversight as frequently as appropriate risk analysis requires. At a minimum, it will require covered DCMs and SDRs to conduct the required key controls testing—including key controls testing by independent contractors as discussed below—no less frequently than every three years. As proposed in the NPRM, it will permit covered DCMs and SDRS to conduct such testing on a rolling basis, but require this to be done over the

[98] 80 FR 80139, 80154 (Dec. 23, 2015).

course of the minimum period or the period determined by an appropriate risk analysis, whichever is shorter.

(3) Who should perform controls testing.

The Commission agrees with the comments noting that testing of key controls by both independent contractors and employees not responsible for development or operation of the controls tested can be valuable and effective. As noted in the NPRM, best practices recognize the value of, and recommend, both such approaches.[99] The Commission notes that the NPRM did not propose barring covered DCM or SDR employees from testing key controls; rather, it proposed that covered DCM and SDR testing of key controls include independent contractor testing of all such controls within the minimum period. As with penetration testing, the Commission believes that independent contractor testing of key controls will strengthen covered DCM and SDR programs of risk analysis and oversight, by providing a valuable outsider perspective concerning crucial safeguards uncolored by insider assumptions or blind spots. The Commission further believes that independent contractor testing of key controls will strengthen Commission oversight of system safeguards, by providing an important, credible third source of information concerning crucial safeguards in addition to what is available from covered DCM or SDR staff and from the internal audit function of those entities. As noted above, because best practices call for controls testing, the Commission disagrees with the comment suggesting that the final rule should not require testing of key controls by either independent contractors or employees. The NPRM did not require

[99] Id. at 80154, 80155.

independent contractor testing of all controls, but rather required independent contractor testing of the key controls of covered DCMs and SDRs.[100]

6. Security Incident Response Plan Testing -- §§ 37.1401(h)(6), 38.1051(h)(6), and 49.24(j)(6).

a. Proposed Rule.

The NPRM called for each DCM, SEF, and SDR to conduct security incident response plan ("SIRP") testing of a scope sufficient to satisfy the scope requirements in the proposed rule.[101] It called for each such entity's SIRP to include, without limitation, the entity's definition and classification of security events, its policies and procedures for reporting and communicating internally and externally concerning security incidents, and the hand-off and escalation points in its security incident response process.[102] It proposed permitting each such entity to coordinate its SIRP testing with its BC-DR plan or other testing required by the applicable system safeguards rules.[103] The NPRM proposed requiring all DCMs, SEFs, and SDRs to conduct SIRP testing at a frequency determined by an appropriate risk analysis, with a minimum frequency requirement of annual SIRP testing for covered DCMs and SDRs.[104] Finally, the NPRM called for all DCMs, SEFs, and SDRs to have SIRP testing conducted by either independent contractors or employees not responsible for development or operation of the systems or capabilities tested.[105]

---

[100] Id.

[101] Id. at 80155 through 80157.

[102] Id.

[103] Id. at 80157.

[104] Id.

[105] Id.

b. Comments Received.

(1) Requirement to maintain and test a SIRP.

Several commenters agreed with the NPRM's call for each DCM, SEF, and SDR to maintain and test a SIRP meeting the requirements in the proposal. CME called SIRPs an important tool for all entities in their efforts to be ready to face inevitable cyber attacks. CME noted its appreciation for the proposal's flexibility for entities to design their SIRP testing in light of their risk analysis, and for the proposal's approval of coordination of SIRP testing with other types of testing. ICE and Nadex also stated support for the NPRM's SIRP testing provision. However, while Tradeweb stated that having a SIRP is essential to the functioning of a SEF, it argued that the SIRP testing requirement should be reduced to annual review and approval of the SIRP by a SEF employee responsible for information security.

(2) SIRP testing frequency.

No commenters expressed disagreement with the proposed requirement for all DCMs, SEFs, and SDRs to conduct SIRP testing as often as indicated by appropriate risk analysis. Regarding the proposed requirement for covered DCMs and SDRs to test their SIRPs once a year at a minimum, CME commented that at least annual SIRP testing is appropriate in today's cybersecurity environment.

(3) Who should conduct SIRP testing.

No commenters expressed disagreement with the proposed general requirement giving DCMs, SEFs, and SDRs the choice of whether to have SIRP testing conducted by independent contractors or employees. However, CME suggested that the final rule should permit SIRP testing to be led by an independent employee who is not responsible

for development or operation of what is tested but who is responsible for design of the SIRP itself. CME stated that this would allow the entity to leverage its employees with expertise in crisis and risk management and in incident response and planning, for both planning and testing purposes, in a way that is optimal for the entity's system safeguards.

c. Final Rule.

The Commission has considered and evaluated the comments concerning SIRP testing. For the reasons discussed below, the Commission is adopting the proposed requirements for each DCM, SEF, and SDR to maintain a SIRP (as defined and described) and test it as often as indicated by appropriate risk analysis, and the proposed requirement for each covered DCM and SDR to conduct SIRP testing at least annually. It is modifying the proposed provisions regarding who may conduct SIRP testing, to permit testing to be led or conducted either by independent contractors or by any entity employee.

(1) Requirement to maintain and test a SIRP.

The Commission agrees with commenters that maintaining and testing a SIRP is important for effective system safeguards in today's cybersecurity environment. The Commission confirms that the proposed SIRP testing requirement is indeed intended to give DCMs, SEFs, and SDRs flexibility concerning the format and design of their SIRP testing, and concerning its coordination with other types of testing, so long as the entity's SIRP testing is consonant with appropriate risk analysis and enables fulfillment of the proposed scope requirements. The Commission disagrees with the suggestion that the requirement to test the SIRP should be reduced to mere annual review and approval of the SIRP by an employee responsible for information security. As noted in the NPRM,

best practices emphasize that SIRP testing is crucial to effective cyber incident response in today's cybersecurity environment.[106] Failure to practice the cyber incident response process can delay or paralyze timely response and cause severe consequences.

(2) SIRP testing frequency.

The Commission notes that no commenters disagreed with the requirement to conduct SIRP testing as often as indicated by appropriate risk analysis, and agrees with the comment that at least annual SIRP testing is appropriate for covered DCMs and SDRs in today's cybersecurity environment.

(3) Who should conduct SIRP testing.

The Commission has considered the suggestion that allowing SIRP testing to be led by an employee responsible for design of the SIRP itself could improve system safeguards in general and SIRP testing in particular. The Commission believes that this could provide useful benefits and flexibility to DCMs, SEFs, and SDRs, without impairing the purposes of the CEA and the Commission's regulations which SIRP testing is designed to advance. In addition, SIRP testing differs from the other types of testing specified in the final rule, in that what is tested is not automated systems but the security incident response plan itself, or in other words what people do if a security incident happens. Accordingly, the final rule calls for SIRP testing by all DCMs, SEFs, and SDRs to be conducted by either independent contractors or employees, without restricting which employees may lead or conduct the testing.

[106] 80 FR 80139, 80155 through 80156 (Dec. 23, 2015).

7. Enterprise Technology Risk Assessment -- §§ 37.1401(h)(7), 38.1051(h)(7), and 49.24(j)(7).

a. Proposed Rule.

The NPRM called for each DCM, SEF, and SDR to conduct enterprise technology risk assessment ("ETRA") of a scope sufficient to satisfy the scope requirements in the proposed rule.[107] It called for each DCM, SEF, and SDR to conduct an ETRA as often as required by appropriate risk analysis, and for covered DCMs and SDRs to do this at least annually.[108] It stated that all regulatees could conduct ETRAs by using independent contractors or employees not responsible for development or operation of the systems or capabilities being assessed.[109]

b. Comments Received.

(1) ETRA requirement.

CME agreed that regular risk assessments should drive ongoing efforts to address cyber risks. Nadex stated its general agreement with the proposed ETRA requirement. ICE argued that the ETRA requirement is already adequately addressed by current Commission rules, and called for omission of the ETRA requirement in the final rule. ICE also argued that the proposed ETRA requirement is not cyber-specific and does not focus on the confidentiality, availability, or integrity of data. Tradeweb agreed that assessment of technology risks is essential, but argued that the ETRA requirement is duplicative of the other proposed testing requirements.

[107] Id. at 80157 through 80159.

[108] Id. at 80158.

[109] Id. at 80158, 80159.

(2) ETRA frequency and scope.

CME suggested that ETRAs would benefit from incorporating the results of controls testing and other testing, and suggested that it would be beneficial and less costly to align the requirement for completing an ETRA with the applicable frequency requirement for controls testing. Nadex requested clarification of whether the ETRA could incorporate the results of other required testing as reported to management and the board of directors, or whether a full stand-alone assessment is required. Tradeweb suggested that an annual full assessment would be burdensome and costly, and suggested that, in lieu of repeated full assessments, annual review and approval of previous assessments should be sufficient.

(3) Who should conduct ETRAs.

No commenters expressed disagreement with the NPRM provision calling for ETRAs to be conducted by either independent contractors or employees not responsible for development or operation of the systems or capabilities assessed. ICE suggested that ETRAs should be carried out by enterprise risk program staff rather than information security staff.

c. Final Rule.

The Commission has considered and evaluated the comments concerning ETRAs. For the reasons discussed below, the Commission is adopting the proposed requirements, but is adding a provision in the final rule stating that a DCM, SEF, or SDR that has conducted an enterprise technology risk assessment as required may conduct subsequent assessments by updating the previous assessment.

(1) ETRA requirement.

The Commission agrees with the comment that regular risk assessments should drive ongoing efforts to address cyber risks. The Commission continues to believe that conducting regular ETRAs is essential to meeting the testing requirements of its current system safeguards rules and maintaining system safeguards resiliency in today's cybersecurity environment. Regular, ongoing identification, estimation, and prioritization of risks that could result from impairment of the confidentiality, integrity, or availability of data and information or the reliability, security, and capacity of automated systems is crucial to effective system safeguards. As noted in the NPRM, regular performance of ETRAs is a well-established best practice.[110] The proposed ETRA requirement is designed to provide an overarching vehicle through which a DCM, SEF, or SDR draws together and uses the results and lessons learned from each of the types of cybersecurity and system safeguards testing addressed in the proposed rule, in addition to other methods of risk identification, in order to identify and mitigate its system safeguards-related risks. ETRAs can also inform the design of the other types of testing. As such, the ETRA requirement it is not duplicative of the other testing requirements, but rather an enhancement of their value. The Commission also notes that, as discussed above, multiple NPRM provisions to be adopted in the final rule call for determinations made in light of the appropriate risk analysis that is required by the CEA. Accordingly, a regulatee's current ETRA summarizing in writing both its analysis of its system safeguards risks and the basis for that analysis and for the entity's system safeguards decisions will be a key tool for Commission determination of the adequacy of

[110] Id. at 80158.

the entity's compliance with system safeguards requirements. The Commission therefore disagrees with the suggestion that the final rule should omit the ETRA requirement.

(2) ETRA frequency and scope.

While the Commission agrees that the results of other types of testing can usefully inform ETRAs, the Commission believes that, as best practices provide, regularly updated ETRAs are crucial to the effectiveness of system safeguards in today's rapidly changing cybersecurity environment. The Commission therefore does not accept the suggestion that ETRAs should only be required as often as a complete cycle of controls testing is completed, not least because the final rule is adopting the suggestion to lengthen that cycle to three rather than two years. The Commission reiterates that the results of other required forms of system safeguards testing can and should be incorporated in ETRAs, and in turn should be informed and driven by ETRAs. Because ETRAs that provide current assessment of current risks are essential to effective programs of system safeguards risk analysis and oversight, as discussed above, the Commission disagrees with the suggestion that annual review and reapproval of previous assessments would be sufficient. However, the Commission believes that thorough updating of a previous assessment conducted in compliance with the ETRA requirements set out in the NPRM can be sufficient to fulfill the purposes of an appropriate ETRA, and can reduce costs and burdens without impairment of the purposes of the CEA and the system safeguards rules. Accordingly the final rule clarifies that such updating of a previous fully compliant ETRA, in light of current risks and circumstances, can fulfill the ETRA requirement. The Commission emphasizes that best practices require all DCMs, SEFs, and SDRs to conduct risk assessment and monitoring on an ongoing basis, as

frequently as the entity's risks and circumstances require. The final rule requirement for covered DCMs and SDRs to prepare a written assessment on at least an annual basis does not eliminate the need for a covered DCM or SDR to conduct risk assessment and monitoring on an ongoing basis, as best practices require. Rather, the minimum frequency requirement is intended to formalize the risk assessment process and ensure that it is documented at a minimum frequency.

(3) Who should conduct ETRAs.

The NPRM's call for ETRAs to be conducted by either independent contractors or employees not responsible for development or operation of the systems or capabilities assessed drew no objections from commenters. The Commission also notes that the NPRM did not prescribe whether enterprise risk program staff, information security staff, or both should conduct ETRAs, but deliberately left flexibility to DCMs, SEFs, and SDRs in this regard, so long as the employees conducting the ETRA have the independence specified.

F. Scope of Testing and Assessment -- §§ 37.1401(k), 38.1051(k), and 49.24(l).

1. Proposed Rule.

The NPRM called for the scope of all system safeguards testing and assessment to be broad enough to include all testing of automated systems and controls necessary to identify any vulnerability which, if triggered, could enable an intruder or unauthorized user to take any of a number of undesirable actions.[111] These actions were specified to include interfering with the regulatee's operations or fulfillment of its statutory and regulatory responsibilities; impairing or degrading the reliability, security, or capacity of

[111] 80 FR 80139, 80159 (Dec. 23, 2015).

the regulatee's automated systems; adding to, deleting, modifying, exfiltrating, or compromising the integrity of data; or taking any other unauthorized action affecting the regulatee's regulated activities or the hardware or software used in connection with them.[112]

2. Comments Received.

A number of commenters suggested that the scope provisions of the NPRM were overbroad, and that the proposed requirement to perform "all" testing necessary to identify "any" vulnerability was impossible to achieve in practice. CME argued that it is infeasible to conduct testing to identify "any" potential vulnerability, and called for the final rule to provide that testing scope should be risk-based, to enable focus on the most likely scenarios and highest value information assets. CME suggested that the NPRM's overbroad scope provision could impose outsized costs without yielding commensurate benefits. ICE stated that it is impossible to predict and test for all cyber attack scenarios. Nadex agreed with the general thrust of the proposed scope provision, but argued that the requirement to identify "any" vulnerability was too broad, and that it is unrealistic and likely impossible to guarantee testing that could provide 100 percent security against all vulnerabilities or unauthorized actions. WMBAA stated concern that the proposed scope provision would set a standard impracticable for regulatees to achieve, because no regulatee could guarantee that "any" vulnerability would be uncovered by testing, and because it is impracticable to test all potential avenues for penetrating regulatee systems. WMBAA questioned whether any penetration testing firm would be willing to certify that its testing procedures met such a standard. Nadex, CFE, Tradeweb, and WMBAA

[112] Id.

suggested that the NPRM scope provision could be read as imposing a strict liability standard under which any successful cyber attack would mean a violation of the testing scope provisions must have occurred. CME, Nadex, CFE, DDR, Tradeweb, and WMBAA requested that the Commission consider establishing "safe harbor" provisions under which an entity that has made good faith efforts to adhere to one or more designated cybersecurity frameworks or statements of cybersecurity best practices would be deemed to be in compliance with the system safeguards rules. Nadex called for the final rule scope provision to limit responsibility to a reasonableness standard. Nadex also asked the Commission to clarify that the current cybersecurity threat analysis a regulatee should consider in assessing potential cyber adversary capabilities to determine testing scope is limited to the organization's internal risk assessments.

3. Final Rule.

The Commission has considered and evaluated the comments concerning the testing scope provision of the NPRM.[113] For the reasons discussed below, the Commission is modifying the scope provision in the final rule to call for the scope of testing to be based on appropriate risk and threat analysis.

The Commission does not intend the scope provision of the testing rule to create any sort of strict liability standard with respect to system safeguards testing. On the contrary, the Commission recognizes that in today's cybersecurity environment no entity can be expected to be immune from cyber intrusions. As noted in the NPRM, one fundamental goal of the Commission's system safeguards and cybersecurity testing rules is enhancing regulatees' ability to detect, contain, respond to, and recover from cyber

[113] 80 FR 80139, 80159 (Dec. 23, 2015).

intrusion when they happen.[114] In conducting oversight of the system safeguards of DCMs, SEFs, and SDRs, the Commission looks and will continue to look to what a reasonable and prudent DCM, SEF, or SDR would do with respect to system safeguards in light of generally accepted standards and best practices, and in light of informed risk analysis appropriate to the circumstances and risks faced by the DCM, SEF or SDR in question. The Commission does not believe that the mere fact that a DCM, SEF, or SDR has suffered a cyber intrusion means that that entity has failed to comply with system safeguards rules. The Commission would be concerned when examination shows that a DCM, SEF, or SDR failed to follow the best practices that a reasonable entity in its circumstances and facing its risks should follow.

The Commission also recognizes that no program of cybersecurity testing can be expected to detect every possible vulnerability or avenue of intrusion. Here, too, the touchstone is what system safeguards testing a reasonable and prudent DCM, SEF, or SDR would conduct in light of generally accepted standards and best practices, and in light of informed risk analysis appropriate to the circumstances and risks faced by the DCM, SEF or SDR in question. The Commission evaluates, and will continue to evaluate, system safeguards testing in that light.

Given today's rapidly changing cyber threat environment and the resulting continuous evolution of generally accepted standards and best practices with respect to system safeguards, the Commission does not believe it would be appropriate to label compliance with any one source of best practices as written at a particular point in time as a "safe harbor" with respect to system safeguards compliance. The Commission believes

[114] Id. at 80156.

that the appropriate way to address the concerns underlying the comments seeking designation of such safe harbors is the standard discussed above: reasonable and prudent system safeguards testing in light of generally accepted standards and best practices, and in light of informed risk analysis appropriate to the circumstances and risks faced by the DCM, SEF or SDR in question.

The Commission disagrees with the comment asking confirmation that the current cybersecurity threat analysis a DCM, SEF, or SDR should consider in designing its system safeguards testing is limited to the organization's internal risk assessments. As noted in the NPRM, a DCM, SEF, or SDR acting as a reasonable and prudent regulatee would act in light of best practices and the current cybersecurity threat environment should obtain and consider threat analysis available from outside sources in addition to conducting its own threat analysis.

For those reasons, the Commission agrees with the comments suggesting that the scope provisions of the final rule should call for testing scope to be based on appropriate risk and threat analysis. In order to provide the clarity requested by commenters, the final rule calls for the scope of system safeguards testing to include the testing that the regulatee's program of risk analysis and oversight and its current cybersecurity threat analysis indicate is necessary to identify risks and vulnerabilities that could enable the deleterious actions by intruders or unauthorized users listed in the scope provisions of the proposed rules. The Commission agrees with the comments suggesting that this approach will avoid imposing undue burdens and costs, while supporting the purposes of the CEA and the Commission's system safeguards rule.

G. Internal Reporting and Review -- §§ 37.1401(l), 38.1051(l), and 49.24(m).

1. Proposed Rule.

The NPRM called for DCM, SEF, and SDR senior management and boards of directors to receive and review reports setting forth the results of the testing and assessment required by the system safeguards rules.[115] It also called for these entities to establish and follow procedures for remediation of issues identified through such review, and for evaluation of the effectiveness of testing and assessment protocols.[116]

2. Comments Received.

a. Board and Senior Management Oversight.

Several commenters agreed with the NPRM's call for oversight of system safeguards and cybersecurity by boards of directors and senior management. CME and MGEX recognized the importance of effective board oversight and the need to keep the board and senior management up to date in this regard. DDR said it agreed with the Commission that active board and senior management supervision of system safeguards promotes more efficient, effective, and reliable risk management. However, ICE argued that internal reporting and review of test results should be limited to reports to senior management, and that boards of directors should not be required to review even high-level, high-priority test findings, but instead should only be apprised of enterprise-level high risk issues when identified thresholds (unspecified by ICE) are crossed.

[115] 80 FR 80139, 80160 (Dec. 23, 2015).

[116] Id.

b. Level of Detail for Board and Senior Management Review.

Commenters requested clarification concerning what level of detail the NPRM called for boards and senior management to review in terms of test results. ICE, MGEX, and Nadex noted that test result reports can be voluminous, technical, and complex, and that requiring boards and senior management to review each such document could produce an undue burden without commensurate benefits. MGEX and Nadex therefore asked the Commission to clarify in the final rule that what is required is board and management review of appropriate summaries and compilations of test and assessment results. DDR suggested it should be the regulatee's responsibility to provide the board and senior management with the level of test result information appropriate for enabling their effective oversight of system safeguards. DDR asked the Commission to confirm in the final rule that there are multiple ways this can be done. Nadex also asked the Commission to clarify that board consideration of test results in the course of regularly scheduled meetings would be an acceptable way of fulfilling this requirement.

3. Final Rule.

The Commission has considered and evaluated the comments concerning the internal reporting and review provision of the NPRM.[117] For the reasons discussed below, the Commission is adopting the provision as proposed.

a. Board and Senior Management Oversight.

The Commission agrees with the comments recognizing the importance of effective board of directors and senior management of system safeguards, and the resulting need to keep the board and senior management informed appropriately

[117] 80 FR 80139, 80160 (Dec. 23, 2015).

concerning the results of cybersecurity testing and assessment. In today's cybersecurity threat environment, active board and senior management supervision of system safeguards is essential to the enterprise-wide, effective risk management that the CEA and Commission regulations require of DCMs, SEFs, and SDRs. Such active supervision would be impossible if board members and senior managers were not appropriately apprised of the results of cybersecurity testing and assessment, and thus lacked an essential level of knowledge of the organization's system safeguards risks. As noted in the NPRM, generally accepted standards and best practices emphasize the importance of board and senior management oversight of cybersecurity, and make it clear that the absence of proactive board and senior management involvement in cybersecurity can make regulatees more vulnerable to successful cyber attacks.[118] Accordingly, best practices call for directors to either have the appropriate level of experience and knowledge of information technology and related risks themselves or obtain the assistance of expert consultants in this regard. In the Commission's view, protection of the public interest and the economic security of the United States with respect to derivatives markets in today's cybersecurity threat environment demands no less. For these reasons, the Commission disagrees with the suggestion that boards of directors should not be involved in internal reporting and review of cybersecurity test results.

b. Level of Detail for Board and Senior Management Review.

The Commission also agrees with the comments suggesting that test result reports can be voluminous, technical, and complex, and that effective board of directors and senior management oversight of system safeguards does not require board or senior

[118] 80 FR 80139, 80160 (Dec. 23, 2015).

management review of every detail of each such report. The Commission further agrees with the comments suggesting that DCMs, SEFs, and SDRs should provide their boards and senior management with a level of test result information that enables their effective, knowledgeable oversight of cybersecurity and system safeguards in light of the risks faced by their organizations. While the internal reporting and review provision of the final rule requires that the board receive and review test results, it does not prevent an organization from including additional, clarifying documents, such as executive summaries or compilations, with the required reports. Board and senior management review of appropriate summaries and compilations of test and assessment results can be an effective and acceptable way of fulfilling the internal reporting and review requirement, provided that such summaries give board members and senior management sufficiently detailed information to enable them to conduct effective and informed oversight. The appropriate level of information should also enable boards and senior management to fulfill this provision's requirement for them to evaluate the overall effectiveness of testing and assessment protocols, and direct and oversee appropriate remediation of issues identified through their review of test results. As noted in the NPRM, best practices call for boards and senior management to review the overall effectiveness of the testing program.[119]

H. Remediation -- §§ 37.1401(m), 38.1051(m), and 49.24(n).

1. Proposed Rule.

The NPRM called for each DCM, SEF, and SDR to analyze the results of the testing and assessment required by the system safeguards rules in order to identify all

[119] 80 FR 80139, 80160 (Dec. 23, 2015).

vulnerabilities and deficiencies in its systems.[120] It proposed requiring each such entity to remediate those vulnerabilities and deficiencies to the extent necessary to enable the entity to meet the requirements of the system safeguards rules and of its statutory and regulatory responsibilities.[121] It called for such remediation to be timely in light of appropriate risk analysis with respect to the risks presented.

2. Comments Received.

Nadex and Tradeweb suggested that the proposed requirement to identify and remediate "all" vulnerabilities and deficiencies in a regulatee's systems was impossible to achieve in practice. Nadex observed that other discussion in the NPRM indicated Commission intent to require remediation of vulnerabilities and deficiencies identified in the testing results, and suggested amending the final rule to make this clear. Noting that remediation after a cyber attack often takes time, Tradeweb argued that regulatees should not be penalized for that fact, and requested Commission guidance on what constitutes timely remediation, perhaps including specification that remediation over nine to twelve months would be timely.

3. Final Rule.

The Commission has considered and evaluated the comments concerning the remediation provision of the NPRM. For the reasons discussed below, the Commission is modifying the remediation provision in the final rule require DCMs, SEFs, and SDRs to: (1) identify and document the vulnerabilities and deficiencies revealed by the testing called for in the system safeguards rules; and (2) conduct and document an appropriate

[120] 80 FR 80139, 80160 (Dec. 23, 2015).

[121] Id.

analysis of the risks presented, in order to determine and document whether to remediate or accept each such risk. The Commission is adopting the requirement for the entity to remediate such risks in a timely manner in light of appropriate risk analysis as proposed.

The Commission agrees with commenters that a requirement calling for a DCM, SEF, or SDR to remediate all vulnerabilities and deficiencies could be read as overbroad and impossible in practice. As suggested in a comment, the intent of the NPRM remediation provision was in fact to require remediation of the vulnerabilities and deficiencies disclosed through the regulatee's program of risk analysis and oversight, which includes testing of appropriate scope. In response to the comments received, the Commission is narrowing the remediation requirement to address remediation or acceptance of the vulnerabilities and deficiencies of which the entity is aware or through an appropriate program of risk analysis and oversight should be aware, rather than the remediation of all vulnerabilities and deficiencies. This revision is being made to reduce burdens and costs to the extent possible without impairing the purposes of the CEA and the Commission's system safeguards regulations. Best practices call for organizations to conduct appropriate risk analysis with respect to vulnerabilities and deficiencies disclosed by testing, in order to determine whether to remediate or accept the risks presented.[122] Documentation of such analysis and decisions is needed for both an effective program of risk analysis and effective Commission oversight of system safeguards. The NPRM proposal to require identification of vulnerabilities was intended to include their documentation. Effective remediation would be impossible without documentation of

[122] For clarity, the Commission notes that it sees the term "remediation" as including mitigation and avoidance of risks as discussed in some sources of best practices. See, e.g., NIST SP 800-39, at 41-43.

both the vulnerabilities in question and the remediation steps needed. Accordingly, the Commission believes regulatees would create such documentation in the normal course of business. However, because documentation was not explicitly required in the proposal, the Commission is treating the final rule documentation requirement as a possible, slight additional burden. The Commission notes, however, that in the context of the burden reduction resulting from requiring regulatees to identify and remediate the vulnerabilities of which they are or should be aware, rather than to identify "all" vulnerabilities as proposed in the NPRM, the overall effect of the final rule remediation provision represents a considerable reduction in burden and cost over what was proposed.

The Commission is aware that appropriate and effective remediation following a cyber attack often must proceed over a reasonable period of time, determined by the nature of the intrusion and the mitigation steps needed, and it takes this fact into account in determining whether remediation is timely. The Commission does not believe it is practicable to codify specific periods of time as constituting timely remediation, since what is timely and appropriate depends on the particular circumstances and risks involved in a given situation.

III. RELATED MATTERS

A. Regulatory Flexibility Act

The Regulatory Flexibility Act (''RFA'') requires federal agencies, in promulgating rules, to consider the impact of those rules on small entities.[123] The rules adopted herein will affect DCMs, SEFs, and SDRs. The Commission has previously

[123] 5 U.S.C. 601 et seq.

established certain definitions of ‘‘small entities’’ to be used by the Commission in evaluating the impact of its rules on small entities in accordance with the RFA.[124] The Commission previously determined that DCMs, SEFs, and SDRs are not small entities for the purpose of the RFA.[125] The Commission received no comments on the impact of the rules contained herein on small entities. Therefore, the Chairman, on behalf of the Commission and pursuant to 5 U.S.C. 605(b), certifies that the final rules will not have a significant economic impact on a substantial number of small entities.

B. Paperwork Reduction Act

1. Introduction.

The Paperwork Reduction Act of 1995 (‘‘PRA’’)[126] 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. The final rules contain recordkeeping and reporting requirements that are collections of information within the meaning of the PRA. In accordance with the requirements of the PRA, the Commission may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number.

As discussed below, the final rules contain provisions that qualify as collections of information, for which the Commission has already sought and obtained control numbers from OMB. The titles for these collections of information are “Part 38–Designated Contract Markets” (OMB Control Number 3038-0052), “Part 37–Swap

[124] See 47 FR 18618 through 18621 (Apr. 30, 1982).

[125] See 47 FR 18618, 18619 (Apr. 30, 1982) discussing DCMs; 78 FR 33548 (June 4, 2013) discussing SEFs; 76 FR 54575 (Sept. 1, 2011) discussing SDRs.

[126] 44 U.S.C. 3501 et seq.

Execution Facilities" (OMB Control Number 3038-0074), and "Part 49–Swap Data Repositories; Registration and Regulatory Requirements" (OMB Control Number 3038-0086). With the exception of § 38.1051(n) that requires all DCMs to submit annual trading volume information to the Commission, the final rules will not impose any new recordkeeping or reporting requirements that are not already accounted for in existing collections 3038-0052,[127] 3038-0074,[128] and 3038-0086.[129]

2. Clarifications of Collections 3038-0052, 3038-0074, and 3038-0086.

As stated in the NPRM, all DCMs, SEFs, and SDRs are already subject to system safeguard-related books and records obligations.[130] The final rules amend §§ 38.1051(g), 37.1041(g), and 49.24(i) to clarify the system safeguard-related books and records obligations for all DCMs, SEFs, and SDRs. The Commission is adopting these provisions as proposed. Specifically, §§ 38.1051(g), 37.1041(g), and 49.24(i) require all DCMs, SEFs, and SDRs to provide the Commission with the following system safeguards-related books and records promptly upon request of any Commission representative: (1) current copies of the BC-DR plans and other emergency procedures; (2) all assessments of the entity's operational risks or system safeguard-related controls; (3) all reports concerning system safeguards testing and assessment required by this chapter, whether performed by independent contractors or employees of the DCM, SEF, or SDR; and (4) all other books and records requested by Commission staff in connection

[127] See OMB Control No. 3038-0052, available at http://www.reginfo.gov/public/do/PRAOMBHistory?ombControlNumber=3038-0052.

[128] See OMB Control No. 3038-0074, available at http://www.reginfo.gov/public/do/PRAOMBHistory?ombControlNumber=3038-0074

[129] See OMB Control No. 3038-0086, available at http://www.reginfo.gov/public/do/PRAOMBHistory?ombControlNumber=3038-0086.

[130] 80 FR 80139, 80162 (Dec. 23, 2015).

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 entity's automated systems. The NPRM invited public comment on the accuracy of its estimate that no additional recordkeeping or information collection requirements or changes to the existing collection requirements would result from the proposed clarifying amendments.[131] The Commission did not receive any comments that addressed whether additional recordkeeping or information collection requirements or changes to existing collection requirements would result from the adoption of the proposed rules.[132] In light of the above, the Commission believes that §§ 38.1051(g), 37.1041(g), and 49.24(i) do not impact the burden estimates currently provided for in OMB Control Numbers 3038-0052, 3038-0074, and 3038-0086.

3. Revision to Collection 3038-0052.

The final DCM rules will require a new information collection which is covered by OMB Control No. 3038-0052. Commission regulation § 38.1051(n) requires each DCM to provide to the Commission its annual total trading volume for calendar year 2015 and each calendar year thereafter. This information is required for 2015 within 30 calendar days of the effective date of the final rules, and for 2016 and subsequent years by January 31 of the following calendar year.

The Commission requested comment concerning the accuracy of its estimate concerning the proposed reporting requirements in § 38.1051(n).[133] Although the

[131] Id.

[132] As discussed in the preamble, the Commission received comment letters from WMBAA, CME, and ICE concerning the books and records obligations generally.

[133] 80 FR 80139, 80163 (Dec. 23, 2015).

Commission did not receive any comment concerning the accuracy of its estimate, the Commission received a comment from CME that the Commission should consider alternatives to the reporting requirements in proposed § 38.1051(n) because the Commission currently receives daily trade reports regarding volume pursuant to DCM Core Principle 8 and part 16 of the Commission's regulations. The Commission notes that while it receives daily trade information from DCMs pursuant to part 16, it does not receive total annual trading volume from DCMs. Additionally, the Commission believes that Core Principle 8 is inapplicable because it requires DCMs to publish daily volume, but does not require submission of that information to the Commission. The Commission's rules do not currently require the submission of annual trading volume, which is essential for the Commission to accurately evaluate whether a particular DCM must comply with the enhanced system safeguard requirements. The Commission believes that DCMs generally calculate their annual trading volume in the usual course of business and any associated costs incurred by DCMs to comply with this provision will be minimal.

Currently, there are 15 registered DCMs that will be required to comply with the annual trading volume information. Consistent with its estimate in the NPRM, the Commission estimates that the information collection required associated with the final rule will impose an average of .5 hours annually per respondent.[134] The estimated annual burden for 3038-0052 was calculated as follows:

Estimated number of respondents: 15

Annual responses by each respondent: 1

[134] Id.

Total annual responses: 15

Estimated average hours per response: .5

Aggregate annual reporting burden: 7.5

The final rule requiring the submission of annual trading volume information to the Commission will result in an annual cost burden of approximately $24.80 per respondent.[135] The Commission based its calculation on an hourly wage of $49.59 for a Compliance Officer.[136]

Accordingly, the Commission intends to amend existing collection 3038-0052 to account for the submission of annual trading volume information to the Commission. The amendment will add an estimated annual burden of 7.5 hours to the existing collection, which currently includes an annual reporting burden of 8,670 hours. Therefore, the new annual reporting burden for collection 3038-0052 will be 8,677.5 hours.

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 discretionary actions before promulgating a regulation under the CEA or issuing certain orders.[137] Section 15(a) further specifies that the costs and benefits shall

[135] Id.

[136] In arriving at a wage rate for the hourly costs imposed, Commission staff used the National Industry-Specific Occupational Employment and Wage Estimates, published in May (2015 Report). The hourly rate for a Compliance Officer in the Securities and Commodity Exchanges section as published in the 2015 Report was $49.59 per hour. In the NPRM, the Commission's estimate of $22.015 per respondent was based on the hourly wage of $44.03 for a Compliance Officer in the 2014 Report. 80 FR 80139, 80163 (Dec. 23, 2015).

[137] 7 U.S.C. 19(a).

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. In adopting the final system safeguard rules for DCMs, SEFs, and SDRs, the Commission has considered the costs and benefits resulting from its discretionary determinations with respect to the section 15(a) factors.

To further the Commission's consideration of the costs and benefits imposed by its regulations, the Commission invited comments from the public on all aspects of the Consideration of Costs and Benefits section of the NPRM. The Commission specifically invited responses to a series of questions regarding costs and benefits, and specifically invited commenters to provide data or other information quantifying such costs and benefits. The Commission received one comment that provided quantitative information pertaining to the costs associated with certain proposed provisions.[138] CME estimated that the additional cost that it would incur over a two year period is over $7.2 million.[139] A number of other commenters did not provide specific cost estimates, but provided comments concerning the costs generally. The Commission is addressing both types of comments in the discussion that follows. As discussed more fully below, the Commission believes that the changes to the final regulations will reduce the overall costs of compliance as compared to the NPRM.

[138] CME provided cost estimates for the proposed independent contractor requirements, conducting ETRAs, and controls testing.

[139] CME noted that its cost estimate also includes costs associated with the Commission's parallel NPRM that addresses system safeguards for DCOs. Additionally, CME noted that its estimate "does not separate out the costs for clearing, trading, or data reporting."

As stated in the NRPM, Commission staff collected preliminary information 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 ("DMO Preliminary Survey").[140] Some of the cost estimates provided by the DCMs and SDRs included estimates at the parent company level of the DCM and SDR because the entities were unable to apportion the actual costs to a particular entity within their corporate structure.[141] In some cases, apportioning costs could be further complicated by sharing of system safeguards among DCMs, SEFs, SDRs, or DCOs. Therefore, in the data collected for the DMO Preliminary Survey, it was difficult in some cases to distinguish between the system safeguard-related costs of DCMs, SEFs, SDRs, and DCOs. This distinction was highlighted by CME in its comment letter by noting that its cost estimates do not separate out costs for clearing, trading, or data reporting. Given the lack of quantitative data provided in the comments, the Commission is relying on the data collected from the DMO Preliminary Survey concerning the costs for conducting vulnerability testing, external and internal penetration testing, controls testing, and enterprise technology risk assessments.[142]

[140] 80 FR 80139, 80165 (Dec. 23, 2015). The Commission notes that the DCMs and SDRs that provided the information for the DMO Preliminary Survey requested confidential treatment.

[141] It is not uncommon for entities within the same corporate structure to share automated systems and system safeguard programs.

[142] The estimates from the DMO Preliminary Survey provided in this section are presented as simple cost averages of the affected entities', without regard to the type of entity. By definition, averages are meant to serve only as a reference point; the Commission understands that due to the nature of the requirements in relation to the current practices at a covered DCM or an SDR, some entities may go above the average while others may stay below.

2. Baseline for Final Rules.

The Commission recognizes that any economic effects, including costs and benefits, should be evaluated with reference to a baseline that accounts for current regulatory requirements. As stated in the NPRM, the baseline for this cost and benefit consideration is the set of current requirements under the Act and the Commission's regulations for DCMs, SEFs, and SDRs.[143] The Act requires each DCM, SEF, and SDR to develop and maintain a program of system safeguards-related risk analysis and oversight to identify and minimize sources of operational risk.[144] Additionally, the Act mandates that each DCM, SEF, and SDR must develop and maintain automated systems that are reliable, secure, and have adequate scalable capacity, and must ensure system reliability, security, and capacity through appropriate controls and procedures.[145] The Commission's current system safeguards rules for DCMs, SEFs, and SDRs mandate that, in order to achieve these statutory requirements, each DCM, SEF, and SDR must conduct testing and review sufficient to ensure that its automated systems are reliable, secure, and have adequate scalable capacity.[146]

The final rules clarify the system safeguards and cybersecurity testing requirements for DCMs, SEFs, and SDRs, by specifying and defining five types of system safeguards testing that a DCM, SEF, or SDR necessarily must perform to fulfill the testing requirement. For the following reasons, the Commission believes that the final rules calling for each DCM, SEF, and SDR to conduct each of these types of testing

[143] 80 FR 80139, 80164 (Dec. 23, 2015).

[144] CEA § 5(d)(20) (for DCMs); CEA § 5h(f)(14) (for SEFs); CEA § 21(f)(4)(A) and 17 CFR 49.24(a) (for SDRs).

[145] Id.

[146] 17 CFR 38.1051(h) (for DCMs); 17 CFR 37.1401(g) (for SEFs); 17 CFR 49.24(j) (for SDRs).

and assessment will not impose any new costs on DCMs, SEFs, and SDRs. Each of the types of testing and assessment required under the final rules—vulnerability testing, penetration testing, controls testing, security incident response plan testing, and enterprise technology risk assessment—is a generally recognized best practice for system safeguards. Moreover, the Commission believes that it is essentially impossible for a DCM, SEF, or SDR to fulfill its current obligation to conduct testing sufficient to ensure the reliability, security, and capacity of its automated systems without conducting each type of testing addressed by the final rules. This has been true since before the testing requirements of the Act and the current regulations were adopted, and it would be true today even if the Commission were not adopting the final rules.[147] If compliance with the clarified testing requirements herein results in costs to DCMs, SEFs, and SDRs, the

[147] The Commission's current rules and guidance provide that a DCM's, SEF's, or SDR's entire program of risk analysis and oversight, which includes testing, should be based on generally accepted standards and best practices with respect to the development, operation, reliability, security, and capacity of automated systems. See Appendix A to Part 37, Core Principle 14 of Section 5h of the Act—System Safeguards (a) Guidance (1) Risk analysis and oversight program (for SEFs); 17 CFR 38.1051(h) (for DCMs); 17 CFR 49.24(j) (for SDRs). Each of the types of testing addressed in the final rules—vulnerability testing, penetration testing, controls testing, security incident response plan testing, and enterprise technology risk assessment—has been a generally recognized best practice for system safeguards since before the testing requirements of the Act and the current regulations were adopted. The current system safeguards provisions of the CEA and the Commission's regulations became effective in August 2012. Generally accepted best practices called for each type of testing specified in the final rule well before that date, as shown in the following examples. Regarding all five types of testing, see, e.g., NIST SP 800-53A, Rev. 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations ("NIST 800-53A Rev.1"), at E1, F67, F230, F148, and F226, June 2010, available at http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf. Regarding vulnerability testing, see, e.g., NIST SP 800-53A Rev. 1, at F67, June 2010, available at http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf; and NIST SP 800-115, Technical Guide to Information Security Testing and Assessment, at 5-2, September 2008, available at http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf. Regarding penetration testing, see, e.g., NIST Special Publication ("SP") 800-53A, Rev. 1, at E1, June 2010, available at: http://csc.nist.gov/ publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf; and NIST 800-115, at 4-4, September 2008, available at: http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf. Regarding controls testing, see, e.g., NIST 800-53A, Rev. 1, at 13 and Appendix F1, June 2010, available at http://csrc.nist.gov/publications/nistpubs/ 800-53A-rev1/sp800-53A-rev1-final.pdf. Regarding security incident response plan testing, see, e.g., NIST 800-53A, Rev. 1, at F148, June 2010, available at http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf. Regarding enterprise technology risk assessment, see, e.g., NIST 800-53A, Rev.1, at F226, June 2010, available at http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf.

Commission believes that those are costs associated with compliance with current testing requirements and not the final rules.[148]

The Commission believes that new costs will be imposed by the minimum testing frequency and independent contractor requirements for covered DCMs and SDRs included in the final rules. In addition, the final rules that make it mandatory for all DCMs (covered and non-covered), SEFs, and SDRs to follow best practices, ensure testing independence, and coordinate BC-DR plans will also impose new costs. As discussed more fully below in Section C.3.b., the language in the final rules make these currently recommended provisions mandatory and the Commission believes this modification will result in new costs relative to current practice. Finally, the Commission believes that the final rules requiring all DCMs (covered and non-covered), SEFs, and SDRs to update BC-DR plans and emergency procedures no less frequently than annually, and the requirement for all DCMs to report their total annual trading volume to the Commission each year will also impose new costs relative to the current requirements.

The Commission expects that the costs and benefits may vary somewhat among the covered DCMs and SDRs. For example, some covered DCMs and SDRs are larger or more complex than others, and the new requirements may impact covered DCMs and

[148] MGEX commented that it has defined and implemented a system that it believes conforms to industry best practices. MGEX further commented that unless each organization's structure is identical to the CFTC's rulemakings, there will be a cost of compliance. Throughout this section, the Commission has articulated areas where it believes the new rules will impose new costs relative to the current requirements. Accordingly, unless otherwise stated, the Commission believes that any additional costs incurred by DCMs, SEFs, and SDRs are attributable to the current requirements.

SDRs differently depending on their size and the complexity of their systems.[149] The Commission believes that it is not possible to precisely estimate the additional costs for covered DCMs and SDRs that may be incurred as a result of this rulemaking, as the actual costs will be dependent on the operations and staffing of the particular covered DCM and SDR, and to some degree, the manner how they choose to implement compliance with the new requirements.

While certain costs are amenable to quantification, other costs are not easily estimated, such as the costs to the public or market participants in the event of a cybersecurity incident at a DCM, SEF, or SDR. The public interest is served by these critical infrastructures performing their functions. The final regulations are intended to mitigate the frequency and severity of system security breaches or functional failures, and therefore, provide an important if unquantifiable benefit to the public interest.

The discussion of costs and benefits that follows begins with a summary of each final rule and a consideration of the corresponding costs and benefits and the associated comments. At the conclusion of this discussion, the Commission considers the costs and benefits of the rules collectively in light of the five factors set forth in section 15(a) of the CEA.

[149] Based on information obtained from the DMO Preliminary Survey and the Commission's system safeguard compliance program, the Commission understands that most large DCMs (that are likely to be covered DCMs) and SDRs currently conduct system safeguard testing at the minimum frequency for most of the tests required by the final rules. Additionally, the Commission understands that most large DCMs and SDRs currently engage independent contractors for the testing required by the final rules.

3. Summary of Final Rules and Discussion of Costs and Benefits.

a. Categories of Risk Analysis and Oversight: §§ 38.1051(a), 37.1401(a), and 49.24(b).

(1) Summary of Final Rules.

The final rules concerning the categories of risk analysis and oversight clarify what is already required of all DCMs, SEFs, and SDRs regarding the categories which their programs of risk analysis and oversight must address by further defining the six categories addressed by the current rules. The six categories are: (1) Information security; (2) Business-continuity disaster recovery planning and resources; (3) Capacity and performance planning; (4) Systems operations; (5) Systems development and quality assurance; and (6) Physical security and environmental controls. In addition, the final rules add and define enterprise risk management as a seventh category.

(2) Costs and Discussion of Comments.

MGEX stated that because the categories of risk analysis and oversight identified by the Commission in the DCM, SEF, and SDR NPRM differ from the Commission's parallel DCO NPRM, the lack of consistency increases the compliance burden of a combined DCM and DCO entity. The Commission acknowledges that its DCM, SEF, and SDR NPRM included the additional category of enterprise risk management and governance.[150]

MGEX also argued that because the two NPRMs differ on the component parts of a program of risk analysis and oversight, it is difficult to conclude that these programs are pre-existing requirements that do not have a cost of compliance. The Commission disagrees with MGEX. As noted in the DCO NPRM, DCO's face a wider array of risks

[150] 80 FR 80139, 80143 (Dec. 23, 2015).

than DCMs, and therefore enterprise risk management requirements for DCOs are not limited to the system safeguards context, but need to be addressed in a more comprehensive fashion and possibly in a future rulemaking.[151] The requirement for DCMs, SEFs, and SDRs to have a program of system safeguards risk analysis and oversight was mandated by Congress in the CEA itself, and thus is already required by law.[152] The Commission's current system safeguards regulations define the program of risk analysis and oversight by specifying the categories of risk analysis and oversight which the program must address. The category of enterprise risk management and governance is implicit and inherent in the statutory requirement itself, and supported by generally accepted standards and best practices.[153] The final rules make enterprise risk management and governance an explicitly listed category for the sake of clarity. If compliance with the clarifications regarding the categories of risk analysis and oversight results in additional costs, the Commission believes that those are costs associated with compliance with current requirements, not the final rules.

MGEX further argued that the specific and itemized content of some of the categories of risk analysis and oversight are overly prescriptive and should be principles based. MGEX noted information security controls as one example that is overly prescriptive. The Commission agrees with MGEX that the categories of risk analysis and oversight should be principles based, but disagrees with MGEX's assertion that the NPRM lists of topics included in each category consist of a static list of controls. As set

---

[151] Id. at 80123.

[152] CEA § 5(d)(20)(A), 17 USC § 7(d)(20).

[153] See, e.g., NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View (March 2011) ("NIST SP 800-39"), available at http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.

out in detail in the NPRM, each of the aspects of the various categories that the program of risk analysis and oversight must address is rooted in generally accepted standards and best practices.[154] Because the Commission's current system safeguards rules and guidance provide that DCMs, SEFs, and SDRs should follow generally accepted best practices and standards regarding system safeguards, these entities' programs of risk analysis and oversight should already be addressing each of the aspects included in the NPRM for each risk analysis and oversight category.[155]

CME requested that the Commission confirm that the final rule will allow regulated entities flexibility of organizational design concerning how their programs of risk analysis and oversight address enterprise risk management and governance, and will not require that an entity's enterprise risk management function conduct all components of this category. As discussed in the preamble, the Commission confirms that the addition of enterprise risk management and governance does not require that the listed elements of this category be conducted through a particular organizational structure; rather, the final rule provides flexibility in this regard.

(3) Benefits.

The primary benefit of the final rules is clarity to all DCMs, SDRs, and SEFs with regard to administering their programs of risk analysis and oversight. The final rules provide definitions for each category of risk analysis and oversight and highlight important aspects of each category that are recognized as best practices. An important

---

[154] 80 FR 80139, 80143 (Dec. 23, 2015).

[155] See § 38.1051(b) (for DCMs); Appendix A to Part 37, Core Principle 14 of Section 5h of the Act—System Safeguards (a) Guidance (1) Risk analysis and oversight program (for SEFs); § 49.24 (c) (for SDRs).

benefit of the adherence-to-best-practices approach taken in the Commission's final system safeguards rules is that best practices can evolve over time as the cybersecurity field evolves. In addition, the Commission believes that all seven categories of risk analysis and oversight are essential to maintaining effective system safeguards in today's cybersecurity threat environment.

b. Requirements to Follow Best Practices, Ensure Testing Independence, and Coordinate BC-DR Plans: §§ 38.1051(b), 37.1401(b), and § 49.24(c) (best practices); 38.1051(h)(2)(iii), (3)(iii), (4)(ii), (5)(iii), and (7)(ii), 37.1401(h)(2)(iii), (3)(ii), (4)(ii), (5)(ii), and (7)(ii), and 49.24(2)(iii), (4)(ii), and (7)(ii) (testing independence); 38.1051(i), 37.1401(i), and 49.24(k) (BC-DR plans).

(1) Summary of Final Rules.

The final rules make mandatory for DCMs, SEFs, and SDRs the provisions concerning best practices, testing independence, and coordination of BC-DR plans recommended but not made mandatory in the Commission's current rules.

(2) Costs.

The Commission did not receive any comments addressing the costs of these provisions. The Commission's current rules for DCMs and SDRs, and its guidance for SEFs, provide that such entities should follow best practices in addressing the categories which their programs of risk analysis and oversight are required to include.[156] The current rules and guidance also provide that such entities should ensure that their system safeguards testing, whether conducted by contractors or employees, is conducted by independent professionals (persons not responsible for development or operation of the

[156] See § 38.1051(b) (for DCMs); Appendix A to Part 37, Core Principle 14 of Section 5h of the Act—System Safeguards (a) Guidance (1) Risk analysis and oversight program (for SEFs); § 49.24 (c) (for SDRs).

systems or capabilities being tested).[157] They further provide that such entities should coordinate their BC-DR plans with the BC-DR plans of market participants and essential service providers.[158] Because the final rules will make these currently recommended provisions mandatory, it is anticipated that they will impose new costs relative to current practice.

(3) Benefits.

Making the provisions concerning following best practices, ensuring testing independence, and coordinating BC-DR plans mandatory will align the system safeguards rules for DCMs, SEFs, and SDRs with the Commission's system safeguards rules for DCOs, which already contain mandatory provisions in these respects. As stated in the preamble, the Commission believes that the requirement to follow generally accepted standards and best practices is one of the most important requirements of its system safeguards rules. Best practices can evolve over time, in light of the changing cybersecurity threat environment. The agility that a best practices approach provides is crucial to effective resilience with respect to cybersecurity and system safeguards. Further, the ongoing development and evolution of best practices benefits from private sector expertise and input, as well as from public sector contributions. Such private sector expertise and input is important to effective cybersecurity. The Commission also observes that requiring financial sector entities to follow best practices with respect to system safeguards and cybersecurity is an effective key to harmonizing the oversight of

[157] See § 38.1051(h) (for DCMs); Appendix A to Part 37, Core Principle 14 of Section 5h of the Act—System Safeguards (a) Guidance (2) Testing (for SEFs); § 49.24(j) (for SDRs).

[158] See § 38.1051(i) (for DCMs); Appendix A to Part 37, Core Principle 14 of Section 5h of the Act—System Safeguards (a) Guidance (3) Coordination (for SEFs); § 49.24(k) (for SDRs).

cybersecurity conducted by different financial regulators. The Commission also believes that clarity concerning what is required benefits DCMs, SEFs, and SDRs, and the public interest.

c. Updating of Business Continuity-Disaster Recovery Plans and Emergency Procedures: §§ 38.1051(c), 37.1401(c), and 49.24(d).

(1) Summary of Final Rules.

The final rules require a DCM, SEF, or SDR to update its BC-DR plan and emergency procedures at a frequency determined by an appropriate risk analysis, but at a minimum no less frequently than annually.

(2) Costs.

The Commission did not receive any comments addressing the costs of this aspect of the proposed rules. The Commission's current system safeguards rules provide that DCMs, SEFs, and SDRs must maintain BC-DR plans and emergency procedures, but do not specify a frequency in which such plans and procedures must be updated.[159] As a result of the minimum annual frequency requirement, the final rules impose new costs relative to the requirements of the current rules.[160] The entities will incur the additional recurring costs associated with investing in the resources and staff necessary to updating the BC-DR and emergency plans at least annually.

(3) Benefits.

The Commission notes that updating BC-DR plans and emergency procedures at least annually is a generally accepted best practice, as it follows NIST and other

[159] Commission regulations §§ 38.1051(c) (for DCMs), 37.1401(b) (for SEFs), and 49.24(d) (for SDRs); 17 CFR 38.1051(c); 17 CFR 37.1401(b); 17 CFR 49.24(d).

[160] The Commission understands from conducting its oversight of DCMs, SEFs, and SDRs that many of these entities currently update their respective BC-DR plans and emergency procedures at least annually.

standards. These standards highlight the importance of updating such plans and procedures at least annually to help enable the organization to better prepare for cyber security incidents. Specifically, the NIST standards provide that once an organization has developed a BC-DR plan, "the organization should implement the plan and review it at least annually to ensure the organization is following the roadmap for maturing the capability and fulfilling their [sic] goals for incident response."[161]

d. Required System Safeguards-Related Books and Records Obligations: §§ 38.1051(g), 37.1041(g), and 49.24(i).

(1) Summary of Final Rules.

The final rules require a DCM, SEF, or SDR, in accordance with Commission regulation § 1.31,[162] to provide the Commission with the following system safeguards-related books and records promptly upon request of any Commission representative: (1) current copies of the BC-DR plans and other emergency procedures; (2) all assessments of the entity's operational risks or system safeguards-related controls; (3) all reports concerning system safeguards testing and assessment required by this chapter, whether performed by independent contractors or employees of the DCM, SEF, or SDR; and (4) all other books and records requested by Commission staff in connection with Commission oversight of system safeguards pursuant to the Act or Commission

[161] NIST SP 800-53 Rev. 4, Physical and Environmental Protection (PE) control family, available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf; FFIEC, Operations IT Examination Handbook, at 15-18, available at http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_Operations.pdf.

[162] Commission regulation § 1.31(a)(1) specifically provides that "[a]ll books and records required to be kept by the Act 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. 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).

regulations, or in connection with Commission maintenance of a current profile of the entity's automated systems.

(2) Costs and Discussion of Comments.

The Commission believes that the final rules do not impose any new costs.[163] All DCMs, SEFs, and SDRs are already subject to system safeguard-related books and records requirements. The final rules clarify the system safeguard recordkeeping and reporting requirements for these registered entities. Because the final rules only clarify current requirements and because the production of system-safeguard records is already required by the current rules, the Commission believes that the final rules do not impose any additional costs on DCMs, SEFs, and SDRs.

Although the Commission did not receive any comments specifically addressing the costs of the books and records obligations, two commenters addressed whether, and in what circumstances, books and records obligations would reach the parent firm. ICE commented that with respect to parent firms that own both CFTC-regulated and non-CFTC-regulated entities, the Commission should avoid requiring production of documents discussing risks at the firm-wide level. To this end, ICE argued that the Commission should limit its production requests to documents focused solely on the risks of CFTC-regulated entities. However, WMBAA observed that the automated systems, programs of system safeguards-related risk analysis and oversight, cybersecurity defenses and testing, and BC-DR plans and resources of CFTC-regulated DCMs, SEFs, and SDRs owned by parent financial sector companies that also own entities not regulated by the Commission are frequently shared across the parent company. The Commission agrees

[163] See also PRA discussion above.

with WMBAA's comment, and notes that this is presently the case with respect to all DCMs, SEFs, and SDRs regulated by the Commission that are owned by the same parent company. Thus, the Commission disagrees with ICE's suggestion that production of books and records addressing parent-wide system safeguards risks and risk analysis and oversight programs should not be required. A system safeguards document that is a book and record of a DCM, SEF, or SDR is required to be produced as a book and record subject to the Commission's rules, regardless of whether the parent company decides to share resources among CFTC regulated and non-CFTC regulated entities. The production of all of the books and records specified in the NPRM books and records provisions is already required by the Act and Commission regulations.[164]

(3) Benefits.

The recordkeeping requirements for DCMs, SEFs, and SDRs allow the Commission to effectively monitor a DCM's, SEF's, or SDR's system safeguards program and compliance with the Act and the Commission's regulations. In addition, such requirements enable Commission staff to perform examinations of DCMs, SEFs, and SDRs, and identify practices that may be inconsistent with the Act and Commission regulations. Further, making all system safeguard-related documents available to the Commission upon request informs the Commission of areas of potential weaknesses, or persistent or recurring problems, across DCMs, SEFs, and SDRs.

[164] 80 FR 80139, 80147 (Dec. 23, 2015).

e. Definitions: §§ 38.1051(h)(1), 37.1041(h)(1), and 49.24(j)(1).

(1) Summary of Final Rules.

The final rules include definitions for the following terms: (1) controls; (2) controls testing; (3) enterprise technology risk assessment; (4) external penetration testing; (5) internal penetration testing; (6) key controls; (7) security incident; (8) security incident response plan; (9) security incident response plan testing; and (10) vulnerability testing. Additionally, § 38.105(h)(1) includes the definition for covered DCM.

(2) Costs and Benefits.

The definitions specified in the final rules provide context to the specific system safeguard tests and assessments that a DCM, SEF, or SDR is required to conduct on an ongoing basis. Accordingly, the costs and benefits of these terms are attributable to the substantive testing requirements and are discussed in the cost and benefit considerations related to the final rules describing the requirements for each test. However, the Commission notes that some comments addressed terms that were used but not defined in the NPRM and are relevant to the consideration of costs for the final rules. In particular, as discussed in the preamble, CME, ICE, and MGEX commented concerning the NPRM's use of the terms "independent contractor" and "independent professional." CME asserted that neither term is clearly defined in either the Commission's existing rules or the NPRM. ICE called on the Commission to clarify in the final rule that entity employee groups such as the internal audit function are considered to be independent professionals not responsible for the development of operation of the systems or capabilities tested or assessed in the area of system safeguards. ICE stated that not allowing internal auditors to conduct certain system safeguards or information security

testing could add substantial costs to the regulated entities. While not commenting directly on these definitions, MGEX expressed the view that having independent testing performed is a key and costly feature proposed in the NPRM.

The Commission's current system safeguards rules for DCMs and SDRs and its current system safeguards rules and guidance for SEFs provide that independent contractors are qualified system safeguards professionals who are not employees of the DCM, SEF, or SDR.[165] The current rules use the terms independent contractor and employee as they are legally defined and generally used.[166] The Commission believes that the distinction between independent contractor and employee is well settled and understood, and does not need additional definition in the system safeguards rules. With respect to system safeguards testing, the current rules provide that employees conducting required testing must be independent in that they are not employees responsible for development or operation of the systems or capabilities being tested. The Commission believes that this distinction between employees with sufficient independence to appropriately conduct required system safeguards testing and those who lack such independence is also sufficiently clear, and does not require additional definition. The NPRM used, and the final rule will retain, this language from the current system safeguards rules. Where this requirement is included, the testing in question must be conducted by employees who are independent, which means employees not responsible

[165] 17 CFR §§ 38.1051(h) (for DCMs); 37.1401 (g) and Appendix B to Part 37, Core Principle 14 of Section 5h of the Act—System Safeguards (C)(a)(2) (for SEFs); 49.24(j) (for SDRs).

[166] See, e.g., Black's Law Dictionary, Tenth Ed. (Thomson Reuters, St. Paul, MN, 2014) ("Employee. Someone who works in the service of another person (the employer) under an express or implied contract of hire, under which the employer has the right to control the details of work performance.") ("Independent Contractor. Someone who is entrusted to undertake a specific project but who is left free to do the assigned work and to choose the method for accomplishing it.")

for developing or operating what is being tested. Employees who are part of the internal audit function of a DCM, SEF, or SDR, are one example of employees having appropriate independence. Other employees who possess the specified degree of independence and have qualifications the DCM, SEF, or SDR believes are appropriate may also be suitable in such cases.

As discussed in the preamble, one clarification may be helpful with respect to testing required to be performed by independent contractors, as distinct from testing performed by persons performing the internal audit function. The internal audit function is a required aspect of the enterprise risk management governance category which must be included in the program of risk analysis and oversight that a DCM, SEF, or SDR must maintain. It is an integral part of, and a responsibility of, the regulated entity, whether carried out in-house or outsourced. The NPRM proposed required testing by independent contractors in part to give the Commission' system safeguards oversight a third source of system safeguards information on which to rely, in addition to the entity's employees and its internal audit function.[167] It also proposed independent contractor testing to give the regulated entity the benefit of a truly outside perspective concerning system safeguards, not colored by beginning from the institutional point of view. Accordingly, testing performed by persons executing internal audit function will not fulfill the requirement for testing by independent contractors, whether it is performed by employees executing the internal audit function or by internal audit contractors to whom a DCM, SEF, or SDR outsources part or all of its internal audit function.

[167] 80 FR 80139, 80148 (Dec. 23, 2015).

f. Vulnerability Testing: §§ 38.1051(h)(2), 37.1401(h)(2), and 49.24(j)(2).

(1) Summary of Final Rules.

The final rules define vulnerability testing as testing of a DCM's, SEF's, or SDR'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. Additionally, the final rules require a DCM, SEF, or SDR to conduct vulnerability testing that is sufficient to satisfy the testing scope requirements in new §§ 38.1051(k), 37.1401(k), and 49.24(l), at a frequency determined by an appropriate risk analysis. Moreover, such vulnerability testing shall include automated vulnerability scanning and follow best practices in this regard. At a minimum, covered DCMs and SDRs are required to conduct vulnerability testing no less frequently than quarterly. For all DCMs, SEFs, and SDRs, vulnerability testing may be conducted by either independent contractors or employees of the entity that are not responsible for development or operation of the systems or capabilities being tested.

(2) Costs and Discussion of Comments.

(a) Vulnerability Testing Requirement for All DCMs, SEFs, and SDRs.

As stated in the NPRM and above in the Baseline discussion, the Act requires each DCM, SEF, and SDR to develop and maintain a program of system safeguards-related risk analysis and oversight to identify and minimize sources of operational risk.[168] The Act mandates that in this connection each DCM, SEF, and SDR must develop and maintain automated systems that are reliable, secure, and have adequate scalable

[168] 80 FR 80139, 80164, 80167 (Dec. 23, 2015). CEA § 5(d)(20) (for DCMs); CEA § 5h(f)(14) (for SEFs); CEA § 21(f)(4)(A) and 17 CFR 49.24(a) (for SDRs).

capacity, and must ensure system reliability, security, and capacity through appropriate controls and procedures.[169]

The Commission's current system safeguards rules for DCMs, SEFs, and SDRs mandate that, in order to achieve these statutory requirements, each DCM, SEF, and SDR must conduct testing and review sufficient to ensure that its automated systems are reliable, secure, and have adequate scalable capacity.[170] The Commission believes, as the generally accepted standards and best practices noted in the NPRM make clear, that it is essentially impossible for a DCM, SEF, or SDR to fulfill its current obligation to conduct testing sufficient to ensure the reliability, security, and capacity of its automated systems without conducting vulnerability testing.[171] If compliance with the current testing requirements as clarified by the final rules results in costs to a DCM, SEF, or SDR beyond those it already incurs in this connection, the Commission believes that such additional costs are attributable to compliance with the current rules and not to the final rules. Accordingly, the Commission believes that clarifying the rules will not impose any new costs for DCMs, SEFs, and SDRs.

(b) Authenticated Scanning Requirement for All DCMs, SEFs, and SDRs.

The NPRM called for vulnerability testing to include automated vulnerability scanning, conducted on an authenticated basis where indicated by appropriate risk analysis, with compensating controls where scanning is conducted on an unauthenticated

---

[169] Id.

[170] Commission regulations §§ 38.1051(h) (for DCMs), 37.1401(g) (for SEFs), and 49.24(j) (for SDRs). 17 CFR 38.1051(h); 17 CFR 37.1401(g); and 17 CFR 49.24(j).

[171] 80 FR 80139, 80164 (Dec. 23, 2015). See, e.g., NIST SP 800-53A Rev. 1, at F67, June 2010, available at http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf; and NIST SP 800-115, Technical Guide to Information Security Testing and Assessment, at 5-2, September 2008, available at http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

basis.[172] No commenters disagreed with the proposed requirement for vulnerability testing to include automated vulnerability scanning. ICE argued that the Commission should remove the authenticated vulnerability scanning requirement from vulnerability testing because such scanning increases the quantity of findings, potentially diluting and obscuring important results. Additionally, ICE stated that introducing authentication increases the cost and time of a scan and increases risk by requiring an operating system login to be created and maintained on a new system. In light of the possibility that the proposed requirement for automated scanning to include authenticated scanning could increase costs, burdens, and risks while having limited utility for DCMs, SEFs, and SDRs, the Commission is removing the authenticated scanning requirement from the final rules. Instead, the final rules provide that automated vulnerability scanning shall follow best practices.[173] The Commission believes that removal of the authenticated scanning requirement will reduce the costs of compliance where best practices do not require authenticated scanning.

(c) Vulnerability Testing Frequency Requirement for Covered DCMs and SDRs.

The final rules require covered DCMs and SDRs to conduct vulnerability testing no less frequently than quarterly.[174] The Commission's current rules require DCMs and SDRs to conduct regular, periodic, objective testing of their automated systems.[175]

---

[172] Id. at 80150.

[173] To the extent that best practices require or come to require authenticated scanning, such scanning would be mandatory pursuant to the requirement to follow best practices, and would be addressed in system safeguards examinations.

[174] Based on the information collected in the DMO Preliminary Survey, the Commission understands that most large DCMs and SDRs currently conduct vulnerability testing at least quarterly.

[175] See Commission regulations §§ 38.1051(h) (for DCMs) and 49.24(j) (for SDRs); 17 CFR 38.1051(h); 17 CFR 49.24(j).

Accordingly, the final rules will impose new costs relative to the requirements of the current rules.[176] MGEX stated that the frequency of conducting vulnerability testing should be determined by the regulatees and avoid prescriptive, static requirements.[177] ICE argued that regulatees should not be subject to a formal risk assessment to potentially determine a higher vulnerability testing frequency. The Commission notes that the minimum frequency requirement is supported by generally accepted standards and best practices.[178] Therefore, the Commission disagrees with the suggestion that the frequency of such testing should be left to the entities themselves. Accordingly, the Commission also notes that the final rule requires all DCMs, SEFs, and SDRs to conduct such testing as frequently as indicated by appropriate risk analysis.

(d) Independent Contractor Requirement for Covered DCMs and SDRs.

The NPRM called for covered DCMs and SDRs to engage independent contractors to conduct two of the quarterly vulnerability tests each year.[179] As explained in the preamble, a number of commenters argued that the use of independent contractors

---

[176] As stated in the NPRM, the Commission's current system safeguards rules provide that all DCMs must conduct testing to ensure the reliability, security, and capacity of their automated systems, and thus, to conduct vulnerability testing, external and internal penetration testing, controls testing, enterprise technology risk assessments, and to have and test security incident response plans in a way governed by appropriate risk analysis. The proposed rules avoided applying the addition minimum frequency requirements to non-covered DCMs, in order to give smaller DCMs with fewer resources additional flexibility regarding the testing they must conduct. 80 FR 80168 (Dec. 23, 2015). For purposes of the final rules, the Commission continues to believe that such a reduced burden for smaller DCMs is appropriate.

[177] MGEX also commented that a smaller entity, such as MGEX, that is a combined DCM and DCO would not be able to take advantage of the reasonable carve-out for non-covered DCMs, because it would have to meet the highest common denominator of the DCM and DCO rulemakings. As stated in the Commission's parallel DCO rulemaking, the Commission has worked to harmonize the regulations applicable to DCOs and DCMs and the regulations track each other very closely. To the extent that an entity operating as a non-covered DCM incurs additional costs as a result of operating a DCO that must comply with the minimum frequency and independent contractor requirements, such costs are attributable to the final DCO regulations.

[178] PCI DSS, Requirement 11.2 Regularly test security systems and processes, at 51, available at https://www.pcisecuritystandards.org/documents/navigating_dss_v20.pdf.

[179] Id. at 80150.

for vulnerability testing could undesirably increase risks. The Commission agrees with the commenters and the final rules do not include the requirement for covered DCMs and SDRs to have some vulnerability testing conducted by independent contractors. Instead, the final rules provide these entities with the flexibility to engage either independent contractors or use entity employees who are not responsible for the development or operation of the systems or capabilities being tested. The Commission believes that this will reduce costs and burdens for all covered DCMs and SDRs.[180]

(e) Cost Estimates for Covered DCMs and SDRs.

The Commission did not receive comments addressing the total costs for conducting vulnerability testing. As discussed above in the costs section concerning the minimum frequency requirement, the final rules will impose new costs on covered DCMs and SDRs. The data collected from the DMO Preliminary Survey, suggests that on average, a covered DCM or SDR currently spends approximately $3,495,000 annually on vulnerability testing. As stated in the NPRM, the Commission 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.[181] Additionally, although the Commission believes that all covered DCMs and SDRs have policies and procedures in place for vulnerability testing, the Commission acknowledges that affected entities may need to dedicate time to reviewing and revising their current policies and procedures to ensure that they are sufficient in the context of the final rules.

[180] CME commented that the NPRM's independent contractor requirements that apply to vulnerability testing will result in an additional cost of $1.1 million every two years.

[181] Id. at 80168.

The Commission believes that any costs incurred by the entities as result of such review will be minor.

(3) Benefits.

Vulnerability testing identifies, ranks, and reports vulnerabilities that, if exploited, may result in an intentional or unintentional compromise of a system.[182] The complex analysis and plan preparation that a DCM, SEF, or SDR undertakes to complete vulnerability testing, including designing and implementing changes to existing plans, are likely to contribute to a better understanding by management of the challenges the entity might face in a cyber threat scenario. In turn, the entity will be better prepared to address those challenges. Improved preparation helps reduce the possibility of market disruptions. Regularly conducting vulnerability tests enables a DCM, SEF, or SDR to mitigate the impact that a cyber threat to, or a disruption of, the entity's operations would have on market participants, and more broadly, the stability of the U.S. financial markets. Accordingly, the Commission believes that such testing strengthens a DCM's, SEF's, and SDR's automated systems, thereby protecting market participants and swaps data reporting parties from a disruption in services.

With respect to the minimum frequency requirement for covered DCMs and SDRs, the Commission believes that such entities have a significant incentive to conduct vulnerability testing at least quarterly in order to identify the latest threats to the organization and reduce the likelihood that attackers could exploit vulnerabilities. Best

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

practices also support the requirement that vulnerability testing be conducted no less frequently than quarterly. For example, PCI DSS standards provide that entities should run internal and external network vulnerability scans "at least quarterly," as well as after any significant network changes, new system component installations, firewall modifications, or product upgrades.[183] Moreover, the Commission believes that the minimum frequency requirement provides additional clarity to covered DCMs and SDRs concerning what is required in this respect. As noted above in the costs section for this provision, the final rules also provide flexibility for DCMs, SEFs, and SDRs to have vulnerability testing conducted by either independent contractors or entity employees who are not responsible for development or operation of the systems or capabilities being tested.

g. External Penetration Testing: §§ 38.1051(h)(3), 37.1401(h)(3), and 49.24(j)(3).

(1) Summary of Final Rules.

The final rules define external penetration testing as attempts to penetrate a DCM's, SEF's or SDR's automated systems from outside the systems' boundaries to identify and exploit vulnerabilities. Additionally, the final rules require a DCM, SEF, or SDR to conduct external penetration testing that is sufficient to satisfy the scope requirements in new §§ 38.1051(k), 37.1401(k), and 49.24(l), at a frequency determined by an appropriate risk analysis. At a minimum, covered DCMs and SDRs are required to conduct external penetration testing no less frequently than annually. Covered DCMs and SDRs also are required to engage independent contractors to perform the required

[183] PCI DSS, Requirement 11.2 Regularly test security systems and processes, at 51, available at https://www.pcisecuritystandards.org/documents/navigating_dss_v20.pdf.

annual external penetration test, although the entity could have other external penetration testing conducted by employees who are not responsible for development or operation of the systems or capabilities being tested.

(2) Costs and Discussion of Comments.

(a) External Penetration Testing for All DCMs, SEFs, and SDRs.

As stated in the NPRM and above in the Baseline discussion, the Act requires each DCM, SEF, and SDR to develop and maintain a program of system safeguards-related risk analysis and oversight to identify and minimize sources of operational risk.[184] The Act mandates that in this connection each DCM, SEF, and SDR must develop and maintain automated systems that are reliable, secure, and have adequate scalable capacity, and must ensure system reliability, security, and capacity through appropriate controls and procedures.[185]

The Commission's current system safeguards rules for DCMs, SEFs, and SDRs mandate that, in order to achieve these statutory requirements, each DCM, SEF, and SDR must conduct testing and review sufficient to ensure that its automated systems are reliable, secure, and have adequate scalable capacity.[186] The Commission believes, as the generally accepted standards and best practices noted in the NPRM make clear, that it is essentially impossible for a DCM, SEF, or SDR to fulfill its current obligation to conduct testing sufficient to ensure the reliability, security, and capacity of its automated systems

[184] 80 FR 80139, 80164, 80169 (Dec. 23, 2015). CEA § 5(d)(20) (for DCMs); CEA § 5h(f)(14) (for SEFs); CEA § 21(f)(4)(A) and 17 CFR 49.24(a) (for SDRs).

[185] Id.

[186] Commission regulations §§ 38.1051(h) (for DCMs), 37.1401(g) (for SEFs), and 49.24(j) (for SDRs). 17 CFR 38.1051(h); 17 CFR 37.1401(g); and 17 CFR 49.24(j).

without conducting external penetration testing.[187] If compliance with the current testing requirements as clarified by the final rules results in costs to a DCM, SEF, or SDR beyond those it already incurs in this connection, the Commission believes that such additional costs are attributable to compliance with the current rules and not to the final rules. Accordingly, the Commission believes that clarifying the rules will not impose any new costs for DCMs, SEFs, and SDRs.

(b) External Penetration Testing Frequency Requirement for Covered DCMs and SDRs.

The final rules require covered DCMs and SDRs to conduct external penetration testing no less frequently than annually. The Commission's current rules require DCMs and SDRs to conduct regular, periodic, objective testing of their automated systems.[188] Because the current rules do not specify the frequency of such testing, the final rules will impose new costs relative to the requirements of the current rules.[189] MGEX commented that the frequency of conducting external penetration testing should be left up to the organizations themselves. The Commission notes that external penetration testing is supported by generally accepted standards and best practices, which make it clear that testing at least annually is essential to adequate system safeguards in today's cybersecurity environment.[190] Therefore, the Commission disagrees with the suggestion

---

[187] 80 FR 80139, 80164 (Dec. 23, 2015). See, e.g., NIST Special Publication ("SP") 800-53A, Rev. 1, at E1, June 2010, available at: http://csc.nist.gov/ publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf; and NIST 800-115, at 4-4, September 2008, available at: http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf.

[188] See Commission regulations §§ 38.1051(h) (for DCMs) and 49.24(j) (for SDRs); 17 CFR 38.1051(h); 17 CFR 49.24(j).

[189] Based on the information collected in the DMO Preliminary Survey, the Commission understands that most large DCMs and SDRs currently conduct external penetration testing at the minimum frequency specified in the final rule.

[190] NIST, SP 800-115, Technical Guide to Information Security Testing and Assessment, Section 5.2.2, at 5-5, available at http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf.

that the frequency should be left to the determination of the entities themselves. Accordingly, the Commission also notes that the final rule requires all DCMs, SEFs, and SDRs to conduct such testing as frequently as indicated by appropriate risk analysis.

(c) Independent Contractor Requirement for Covered DCMs and SDRs.

The final rules also require that the annual external penetration test conducted by a covered DCM or SDR be conducted by an independent contractor. Current Commission regulations §§ 38.1051(h) and 49.24(j) provide that testing of automated systems should be conducted by qualified, independent professionals.[191] The qualified independent professionals may be independent contractors or employees of a DCM or SDR as long as they are not responsible for development or operation of the systems or capabilities being tested. Therefore, the final rules will impose new costs relative to the requirements of the current rules.[192]

DDR commented generally that an SDR should have flexibility regarding whether to have testing conducted by independent contractors or employees not responsible for the development or operation of the systems or capabilities being tested, based on the risks of that SDR. The Commission disagrees with DDR's comment. As discussed more fully in the preamble and noted below in the benefits section related to this provision, the Commission believes that the independent viewpoint and approach provided by independent contractors, who can conduct a penetration test from the perspective of an outside adversary uncolored by insider assumptions or blind spots, will benefit covered

[191] Id.

[192] Based on the information collected in the DMO Preliminary Survey, the Commission understands that most large DCMs and SDRs currently engage independent contractors to conduct external penetration testing.

DCM and SDR programs of risk analysis and oversight. The Commission also notes that best practices support using independent contractors.[193]

(d) Cost Estimates for Covered DCMs and SDRs.

The Commission did not receive any comments addressing the total costs for conducting external penetration testing. CME, however, estimated that the independent contractor requirements in the Proposal, which apply to external penetration testing, will result in an additional cost of $1.1 million every two years. The data collected from the DMO Preliminary Survey suggests that on average a covered DCM or SDR spends approximately $244,625 annually on external penetration testing. The Commission recognizes that the actual costs may vary widely as a result of many factors, including the size of the organization, the complexity of the automated systems, and the scope of the test. Where a covered DCM or SDR does not currently use an independent contractor to conduct the external penetration test, the Commission expects that such entities may incur some additional minor costs as a result of the need to establish and implement internal policies and procedures that are reasonably designed to address the workflow associated with the test. For example, the Commission expects that such policies and procedures may include communication and cooperation between the entity and independent contractor, communication and cooperation between the entity's legal, business, technology, and compliance departments, appropriate authorization to remediate vulnerabilities identified by the independent contractor, implementation of the measures to address such vulnerabilities, and verification that these measures are

[193] Council on CyberSecurity, CSC 20-1, available at http://www.counciloncybersecurity.org/critical-controls/.

effective and appropriate. Covered DCMs and SDRs that currently do not use independent contractors for the external penetration test may also need to dedicate time to reviewing and revising their current policies and procedures to ensure that they are sufficient in the context of the new requirements. The Commission believes that any costs incurred by the entities as result of such review will be minor.

(3) Benefits.

External penetration testing benefits DCMs, SEFs, and SDRs by identifying the extent to which their systems can be compromised before an attack is identified.[194] Such testing is conducted from outside a DCM's, SEF's, or SDR's security perimeter to help reveal vulnerabilities that could be exploited by an external attacker. The Commission believes that external penetration testing strengthens DCM, SEF, and SDR systems, thereby protecting the entity and market participants from a disruption in services. A disruption in services at any of these entities could potentially disrupt the functioning of the broader financial markets.

The requirement for annual external penetration testing at covered DCMs and SDRs to be performed by an independent contractor is intended to ensure that these entities' system safeguards programs of risk analysis and oversight include the benefits provided when independent contractors perform such testing. The Commission believes that independent contractor testing has particular value with respect to external penetration testing because the test is conducted from the viewpoint of an outsider and

[194] FFIEC, Information Security IT Examination Handbook, at 81, available at http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_InformationSecurity.pdf.

against the current tactics, techniques, and threat vectors of current threat actors as revealed by current threat intelligence.

h. Internal Penetration Testing: §§ 38.1051(h)(4), 37.1401(h)(4), and 49.24(j)(4).

(1) Summary of Final Rules.

The final rules define internal penetration testing as attempts to penetrate a DCM's, SEF's, or SDR's automated systems from inside the systems' boundaries to identify and exploit vulnerabilities. Additionally, the final rules require a DCM, SEF, or SDR to conduct internal penetration testing that is sufficient to satisfy the scope requirements in new §§ 38.1051(k), 37.1401(k), and 49.24(l), at a frequency determined by an appropriate risk analysis. At a minimum, covered DCMs and SDRs are required to conduct the internal penetration testing no less frequently than annually. All DCM, SEFs, or SDRs may engage independent contractors to conduct the test, or the entity may use employees of the entity who are not responsible for development or operation of the systems or capabilities being tested.

(2) Costs and Discussion of Comments.

(a) Internal Penetration Testing for All DCMs, SEFs, and SDRs.

As stated in the NPRM and above in the Baseline discussion, the Act requires each DCM, SEF, and SDR to develop and maintain a program of system safeguards-related risk analysis and oversight to identify and minimize sources of operational risk.[195] The Act mandates that in this connection each DCM, SEF, and SDR must develop and maintain automated systems that are reliable, secure, and have adequate scalable

[195] 80 FR 80139, 80164, 80170 (Dec. 23, 2015). CEA § 5(d)(20) (for DCMs); CEA § 5h(f)(14) (for SEFs); CEA § 21(f)(4)(A) and 17 CFR 49.24(a) (for SDRs).

capacity, and must ensure system reliability, security, and capacity through appropriate controls and procedures.[196]

The Commission's current system safeguards rules for DCMs, SEFs, and SDRs mandate that, in order to achieve these statutory requirements, each DCM, SEF, and SDR must conduct testing and review sufficient to ensure that its automated systems are reliable, secure, and have adequate scalable capacity.[197] The Commission believes, as the generally accepted standards and best practices noted in the NPRM make clear, that it is essentially impossible for a DCM, SEF, or SDR to fulfill its current obligation to conduct testing sufficient to ensure the reliability, security, and capacity of its automated systems without conducting internal penetration testing.[198] If compliance with the current testing requirements as clarified by the final rules results in costs to a DCM, SEF, or SDR beyond those it already incurs in this connection, the Commission believes that such additional costs are attributable to compliance with the current rules and not to the final rules. Accordingly, the Commission believes that clarifying the rules will not impose any new costs for DCMs, SEFs, and SDRs.

(b) Internal Penetration Testing by Independent Contractors or Employees of the DCM, SEF, or SDR.

The Commission continues to believe, as provided in the NPRM, that it is appropriate to give all DCMs, SEFs, and SDRs the flexibility of whether to have internal

---

[196] Id.

[197] Commission regulations §§ 38.1051(h) (for DCMs), 37.1401(g) (for SEFs), and 49.24(j) (for SDRs). 17 CFR 38.1051(h); 17 CFR 37.1401(g); and 17 CFR 49.24(j).

[198] 80 FR 80139, 80164 (Dec. 23, 2015). See, e.g., NIST Special Publication ("SP") 800-53A, Rev. 1, at E1, June 2010, available at: http://csc.nist.gov/ publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf; and NIST 800-115, at 4-4, September 2008, available at: http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf.

penetration testing performed by independent contractors or by employees not responsible for development or operation of the systems or capabilities tested.[199]

(c) Internal Penetration Testing Frequency Requirement for Covered DCMs and SDRs.

The final rules require covered DCMs and SDRs to conduct internal penetration testing no less frequently than annually. The Commission's current rules require DCMs and SDRs to conduct regular, periodic, objective testing of their automated systems.[200] Because the current rules do not specify the frequency of such testing, the final rules will impose new costs.[201] CME commented that there is a scarcity of potential employees with the skill set required to conduct internal penetration testing without introducing risks into the production environment and other sensitive environments. For this reason, CME suggested making annual internal penetration testing an objective rather than a requirement, so that covered DCMs and SDRs can prioritize truly effective testing over less skilled testing done merely to check the annual requirement box. MGEX called for the final rule to leave the frequency of penetration testing to be determined by regulatees. The Commission notes that the minimum annual frequency requirement is supported by generally accepted standards and best practices, which make it clear that such testing at least annually is essential to adequate system safeguards in today's cybersecurity environment.[202] Thus, the Commission disagrees with the suggestions that annual

---

[199] Id. at 80153.

[200] See Commission regulations §§ 38.1051(h) (for DCMs) and 49.24(j) (for SDRs); 17 CFR 38.1051(h); 17 CFR 49.24(j).

[201] Based on the information from the DMO Preliminary Survey, the Commission understands that most large DCMs and SDRs currently conduct internal penetration testing at the minimum frequency specified in the final rule.

[202] PCI DSS standards, at 96 through97, available at https://www.pcisecuritystandards.org/security_standards/index.php.

internal penetration should be a mere objective, or that the frequency of such testing by covered DCMs and SDRs should be left to determination by those entities themselves. The Commission also notes that the final rule requires all DCMs, SEFs, and SDRs to conduct such testing as frequently as indicated by appropriate risk analysis.

(d) Cost Estimates for Covered DCMs and SDRs.

The Commission did not receive comments addressing the total costs for conducting internal penetration testing. However, based on the data from the DMO Preliminary Survey, the Commission estimates that the current average cost for a covered DCM or SDR conducting internal penetration testing is approximately $410,625 annually. The Commission recognizes that the actual costs may vary significantly 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 Commission also recognizes that large DCMs and SDRs may undertake an evaluation, on an initial and ongoing basis, regarding internal policies and procedures for internal penetration testing that may need to be revised. The Commission believes that these costs will be minor.

(3) Benefits.

By attempting to penetrate a DCM's, SEF's or SDR's automated systems from inside the systems' boundaries, internal penetration tests allow the respective entities to assess system vulnerabilities from attackers that penetrate their perimeter defenses and from trusted insiders, such as former employees and contractors. In addition to being an industry best practice, the Commission believes that annual internal penetration testing is important because such potential attacks by trusted insiders generally pose a unique and substantial threat due to their more sophisticated understanding of a DCM's, SEF's, or

SDR's systems. Moreover, "[a]n advanced persistent attack may involve an outsider gaining a progressively greater foothold in a firm's environment, effectively becoming an insider in the process. For this reason, it is important to perform penetration testing against both external and internal interfaces and systems."[203]

As discussed above in the costs section for this provision, the final rules address the required minimum frequency for covered DCMs and SDRs to perform internal penetration testing. Best practices support both external and internal penetration testing on at least an annual basis. NIST calls for at least annual penetration testing of an organization's network and systems.[204] The FFIEC calls for penetration testing of high risk systems at least annually, and for quarterly testing and verification of the efficacy of firewall and access control defenses.[205] Data security standards for the payment card industry provide that entities should perform both external and internal penetration testing "at least annually," as well as after any significant network changes, new system component installations, firewall modifications, or product upgrades.[206] The Commission believes the specified frequency levels will increase the likelihood that the affected entities will be adequately protected against the level of cybersecurity threat now affecting the financial sector.

---

[203] FINRA, Report on Cybersecurity Practices (February 2015), at 22, available at https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf.

[204] NIST, SP 800-115, Technical Guide to Information Security Testing and Assessment, Section 5.2.2, at 5-5, available at http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf.

[205] FFIEC, Information Security IT Examination Handbook, at 82, available at http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_InformationSecurity.pdf.

[206] PCI DSS, Requirements 11.3.1 and 11.3.2., available at https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf.

i. Controls Testing: §§ 38.1051(h)(5), 37.1401(h)(5), and 49.24(j)(5).

(1) Summary of Final Rules.

The final rules define controls testing as an assessment of the DCM's, SEF's, or SDR's market controls to determine whether such controls are implemented correctly, are operating as intended, and are enabling the entity to meet the system safeguard requirements established by the respective chapters. Additionally, the final rules require a DCM, SEF, or an SDR to conduct controls testing that is sufficient to satisfy the scope requirements in new §§ 38.1051(k), 37.1401(k), and 49.24(l), at a frequency determined by an appropriate risk analysis. Covered DCMs and SDRs are required to test the key controls in the entity's risk analysis and oversight no less frequently than every three years. Such testing may be conducted on a rolling basis over the course of the minimum three-year period or over a minimum period determined by an appropriate risk analysis, whichever is shorter. Covered DCMs and SDRs also are required to engage independent contractors to test and assess their key controls no less frequently than every three years. The entities may conduct any other controls testing by using either independent contractors or employees of the DCM or SDR who are not responsible for development or operation of the systems or capabilities being tested.

(2) Costs and Discussion of Comments.

(a) Controls Testing for All DCMs, SEFs, and SDRs.

As stated in the NPRM and above in the Baseline discussion, the Act requires each DCM, SEF, and SDR to develop and maintain a program of system safeguards-

related risk analysis and oversight to identify and minimize sources of operational risk.[207] The Act mandates that in this connection each DCM, SEF, and SDR must develop and maintain automated systems that are reliable, secure, and have adequate scalable capacity, and must ensure system reliability, security, and capacity through appropriate controls and procedures.[208]

The Commission's current system safeguards rules for DCMs, SEFs, and SDRs mandate that, in order to achieve these statutory requirements, each DCM, SEF, and SDR must conduct testing and review sufficient to ensure that its automated systems are reliable, secure, and have adequate scalable capacity.[209] The Commission believes, as the generally accepted standards and best practices noted in the NPRM make clear, that it is essentially impossible for a DCM, SEF, or SDR to fulfill its current obligation to conduct testing sufficient to ensure the reliability, security, and capacity of its automated systems without conducting controls testing.[210] If compliance with the current testing requirements as clarified by the final rules results in costs to a DCM, SEF, or SDR beyond those it already incurs in this connection, the Commission believes that such additional costs are attributable to compliance with the current rules and not to the final rules. Accordingly, the Commission believes that clarifying the rules will not impose any new costs for DCMs, SEFs, and SDRs.

---

[207] 80 FR 80139, 80164, 80172 (Dec. 23, 2015). CEA § 5(d)(20) (for DCMs); CEA § 5h(f)(14) (for SEFs); CEA § 21(f)(4)(A) and 17 CFR 49.24(a) (for SDRs).

[208] Id.

[209] Commission regulations §§ 38.1051(h) (for DCMs), 37.1401(g) (for SEFs), and 49.24(j) (for SDRs). 17 CFR 38.1051(h); 17 CFR 37.1401(g); and 17 CFR 49.24(j).

[210] 80 FR 80139, 80172 (Dec. 23, 2015). See, e.g., NIST 800-53A, Rev. 1, at 13 and Appendix F1, June 2010, available at http://csrc.nist.gov/publications/nistpubs/ 800-53A-rev1/sp800-53A-rev1-final.pdf.

(b) Controls Testing Frequency Requirement for Covered DCMs and SDRs.

The final rules require a covered DCM or SDR to test each key control included in its program of system safeguards-related risk analysis and oversight no less frequently than every three years rather than the two-year cycle proposed in the NPRM. The Commission's current rules require DCMs and SDRs to conduct regular, periodic, objective testing of their automated systems.[211] Therefore, the final rules will impose new costs relative to the requirements of the current rules.[212] CME commented that some less critical controls do not warrant testing on a two-year cycle, and cited best practices permitting controls testing on a three-year cycle. CME suggested that the final rule should call for the minimum controls testing frequency for covered DCMs and SDRs to be determined by risk analysis (as the NPRM proposed for non-covered DCMs and SEFs), or alternatively that a minimum frequency cycle of three years would be a reasonable alternative to the NPRM's proposed two-year cycle. CME also suggested that, while many organizations will implement a two-year schedule for at least the testing of key controls, either of CME's proposed alternatives would make controls testing more cost effective, and increase focus on the most critical controls. The Commission agrees that a three-year rather than two-year minimum controls testing frequency requirement for covered DCMs and SDRs may reduce costs and burdens, while providing beneficial flexibility in overall controls testing program design and still ensuring that the

---

[211] See Commission regulations §§ 38.1051(h) (for DCMs) and 49.24(j) (for SDRs); 17 CFR 38.1051(h); 17 CFR 49.24(j).

[212] Based on the information collected in the DMO Preliminary Survey, the Commission understands that at least some of the large DCMs and SDRs currently conduct key controls testing at the frequency level specified in the final rule.

fundamental purposes of the CEA and the Commission's system safeguards rules are achieved.

(c) Independent Contractor Requirement for Covered DCMs and SDRs.

The final rules also require a DCM or SDR to engage an independent contractor to test and assess the key controls no less frequently than every three years. Current Commission regulations §§ 38.1051(h) and 49.24(j) provide that testing of automated systems should be conducted by qualified, independent professionals. The qualified independent professionals may be independent contractors or employees of a DCM or SDR as long as they are not responsible for development or operation of the systems or capabilities being tested. Accordingly, the final rules will impose new costs relative to the requirements of the current rules.[213] CME commented that, while independent contractor controls testing may be beneficial, the final rule should not exclude controls testing by independent employees, such as internal audit staff. DDR also commented that, where the NPRM proposed to require independent contractor testing, the final rule should give flexibility to use either independent contractors or independent employees. ICE suggested that the final rule should not require key controls testing, by independent contractors or otherwise, because it imposes a large burden for little or no practical improvement in security. The Commission notes that generally accepted standards and best practices call for key controls testing by independent contractors.[214] Therefore, the Commission disagrees with comments suggesting that the final rule should not require

[213] Based on the information collected in the DMO Preliminary Survey, the Commission understands that most large DCMs and SDRs currently engage independent contractors to conduct key controls testing.

[214] NIST SP 800-53A Rev. 4, at 17-18, available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf.

testing of key controls by independent contractors. Independent contractor testing of key controls will strengthen Commission oversight of system safeguards by providing an important, credible third source of information concerning crucial safeguards in addition to what is available from covered DCM or SDR staff and from the internal audit function of those entities. While the Commission recognizes that covered DCMs and SDRs will incur additional costs to engage independent contractors, the Commission believes that extending the minimum testing frequency for such testing by independent contractors from two to three years will reduce costs and burdens.

(d) Cost Estimates for Covered DCMs and SDRs.

Based on the information from the DMO Preliminary Survey, the Commission estimates that the average cost for a covered DCM or SDR to conduct controls testing is approximately $2,724,000 annually.[215] As discussed above in the costs section concerning the minimum frequency and independent contractor requirements, the final rules will impose new costs on covered DCMs and SDRs. CME estimated that conducting controls testing in the manner proposed by the Commission will result in an additional cost of $5.6 million over a two-year period. However, the Commission believes that the modification of the minimum frequency requirement from two to three years will reduce costs and burdens. Consistent with all of the system safeguard-related tests required in the final rules, the Commission 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. With respect to a covered

[215] One of the Cybersecurity Roundtable participants noted that with respect to the costs for a properly scoped program of controls testing there is no single answer to this question because it depends on the number of an organization's applications and the amount of money spent across the industry varies greatly. See CFTC Roundtable, at 258-59.

DCM or SDR that does not currently use an independent contractor to conduct key controls testing, the Commission expects that these entities may incur some minor costs as a result of the need to establish and implement internal policies and procedures that are reasonably designed to address the workflow associated with the test. For example, the Commission expects that such policies and procedures may include the communication and cooperation between the entity and independent contractor; communication and cooperation between the entity's legal, business, technology, and compliance departments; appropriate authorization to remediate deficiencies identified by the independent contractor; implementation of the measures to address such deficiencies; and verification that these measures are effective and appropriate. While the Commission believes that all covered DCMs and SDRs have policies and procedures in place for controls testing conducted by internal staff, the Commission acknowledges that the affected entities may dedicate time in reviewing and revising their current policies and procedures to ensure that they are sufficient in the context of the new requirements. The Commission believes that any costs incurred by the entities as result of such review will be minor.

(3) Benefits.

Controls testing is essential in determining risk to an organization's operations and assets, to individuals, to other organizations, and to the nation resulting from the use of the organization's systems.[216] In other words, controls testing is vital because it allows

[216] NIST SP 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.

firms to be nimble in preventing, detecting, or recovering from an attack.[217] The Commission believes that the complex analysis and plan preparation that DCMs, SEFs, and SDRs undertake with respect to controls testing, including designing and implementing changes to existing plans, likely contributes to a better understanding by management of the challenges the entity would face in a cyber threat scenario. Consequently, these entities should be better prepared to meet these challenges. This improved preparation also would help reduce the possibility of market disruptions and financial losses to market participants. Moreover, regularly conducting controls testing enables DCMs, SEFs, and SDRs to mitigate the impact that a cyber threat to, or a disruption of, operations would have on market participants, and more broadly, the stability of the U.S. financial markets. Accordingly, the Commission believes that such testing strengthens DCMs, SEFs, and SDRs automated systems, thereby protecting market participants and swaps data reporting parties from a disruption in services.

As noted above in the costs section for this provision, the final rules require a covered DCM or SDR to test each key control included in its program of system safeguards-related risk analysis oversight no less frequently than every three years. The Commission believes that it is essential for each key control to be tested at least this often in order to confirm the continuing adequacy of the entity's system safeguards in today's cybersecurity threat environment. Additionally, the frequency requirement would benefit the affected entities by providing additional clarity concerning what is required of them in this respect. The final rules also permit such testing to be conducted on a rolling basis over the course of the three-year period or over a minimum period determined by an

[217] CFTC Roundtable, at 43-44.

appropriate risk analysis, whichever is shorter. The rolling basis provision is designed to provide a covered DCM or SDR flexibility in conducting the key controls testing during the required minimum frequency period. This flexibility is intended to reduce burdens to the extent possible while still ensuring the needed minimum testing frequency. The Commission also notes that testing on a rolling basis is consistent with industry best practices.[218]

Additionally, the final rules require a covered DCM or SDR to engage independent contractors to test and assess each of the entity's key controls no less frequently than every three years. Independent testing of key controls is consistent with best practices. Significantly, the NIST Standards note the important benefits of independent testing and call for controls testing to include assessment by independent assessors, free from actual or perceived conflicts of interest, in order to validate the completeness, accuracy, integrity, and reliability of test results.[219] Accordingly, in light of best practices and the current cyber threat level to the financial sector, the Commission believes that the covered DCM and SDR independent contractor testing requirement for key controls would provide these substantial benefits.

j. Security Incident Response Plan Testing: §§ 38.1051(h)(6), 37.1401(h)(6), and 49.24(j)(6).

(1) Summary of Final Rules.

The final rules define security incident response testing as testing of a DCM's, SEF's, or SDR's security incident plan to determine the plan's effectiveness, identifying

[218] NIST SP 800-53A Rev. 4, at 17-18, available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf.

[219] Id.

its potential weaknesses or deficiencies, enabling regular plan updating and improvement, and maintaining organizational preparedness and resiliency with respect to security incidents. In addition, the methods of conducting security incident response plan testing may include checklist completion, walk-through or table-top exercises, simulations, and comprehensive exercises. The final rules require covered DCMs and SDRs to conduct such testing at a frequency determined by an appropriate risk analysis, but at a minimum no less frequently than annually. All DCMs, SEFs, and SDRs may conduct such testing by engaging either independent contractors or employees of the entity.

(2) Costs and Discussion of Comments.

(a) Requirement to Maintain and Test a Security Incident Response Plan for All DCMs, SEFs, and SDRs.

As stated in the NPRM and above in the Baseline discussion, the Act requires each DCM, SEF, and SDR to develop and maintain a program of system safeguards-related risk analysis and oversight to identify and minimize sources of operational risk.[220] The Act mandates that in this connection each DCM, SEF, and SDR must develop and maintain automated systems that are reliable, secure, and have adequate scalable capacity, and must ensure system reliability, security, and capacity through appropriate controls and procedures.[221]

The Commission's current system safeguards rules for DCMs, SEFs, and SDRs mandate that, in order to achieve these statutory requirements, each DCM, SEF, and SDR must conduct testing and review sufficient to ensure that its automated systems are

[220] 80 FR 80139, 80164, 80174 (Dec. 23, 2015). CEA § 5(d)(20) (for DCMs); CEA § 5h(f)(14) (for SEFs); CEA § 21(f)(4)(A) and 17 CFR 49.24(a) (for SDRs).

[221] Id.

reliable, secure, and have adequate scalable capacity.[222] The Commission believes, as the generally accepted standards and best practices noted in the NPRM make clear, that it is essentially impossible for a DCM, SEF, or SDR to fulfill its current obligation to conduct testing sufficient to ensure the reliability, security, and capacity of its automated systems without conducting security incident response plan testing.[223] If compliance with the current testing requirements as clarified by the final rules results in costs to a DCM, SEF, or SDR beyond those it already incurs in this connection, the Commission believes that such additional costs are attributable to compliance with the current rules and not to the final rules. Accordingly, the Commission believes that clarifying the rules will not impose any new costs for DCMs, SEFs, and SDRs.

As noted in the preamble, Tradeweb agreed that having a security incident response plan is essential to the functioning of a SEF, but suggested that the plan need only be reviewed annually and approved by an individual at the SEF in charge of information security. Tradeweb commented that requiring repeated testing of such plans is burdensome and unduly costly. The Commission disagrees with the suggestion that the requirement to test the security incident response plan should be reduced to mere annual review and approval of the plan by an employee responsible for information security. Best practices emphasize that security incident response plan testing is crucial to effective cyber incident response in today's cybersecurity environment.[224] The Commission notes

---

[222] Commission regulations §§ 38.1051(h) (for DCMs), 37.1401(g) (for SEFs), and 49.24(j) (for SDRs). 17 CFR 38.1051(h); 17 CFR 37.1401(g); and 17 CFR 49.24(j).

[223] 80 FR 80139, 80174 (Dec. 23, 2015). See, e.g., NIST 800-53A, Rev. 1, at F148, June 2010, available at http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf.

[224] NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, at 2-4 (citing NIST SP 800-53, Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations).

that failure to practice the cyber incident response process can delay or paralyze timely response and cause severe consequences. While the Commission recognizes that security incident response testing will impose costs, these costs are attributable to the current requirements.

(b) Security Incident Response Plan Testing by Independent Contractors or Employees of the DCM, SEF, or SDR.

The NPRM called for all DCMs, SEFs, and SDRs to have security incident response plan testing by either independent contractors or employees not responsible for development or operation of the systems or capabilities tested.[225] CME suggested that the Commission permit an independent employee responsible for incident response both design an organization's security incident response plan and be responsible for testing the plan. CME stated that this would allow an entity to leverage its employees with expertise in crisis and risk management and in incident response and planning, for both planning and testing purposes, in a way that is optimal for the entity's system safeguards. The Commission has considered CME's suggestion and believes that this could provide useful benefits and flexibility to all DCMs, SEFs, and SDRs, without impairing the purposes of the CEA and the Commission's regulations which security incident response plan testing is designed to advance. Accordingly, the final rules require security incident response plan testing by all DCMs, SEFs, and SDRs to be conducted by either independent contractors or entity employees, without restricting which employees may lead or conduct the testing.

[225] Id. at 80157.

(c) Security Incident Response Plan Testing Frequency Requirement for Covered DCMs and SDRs.

The final rules require covered DCMs and SDRs to conduct security incident response plan testing at least annually. The Commission's current rules require DCMs and SDRs to conduct regular, periodic, objective testing of their automated systems.[226] Accordingly, the final rules will impose new costs relative to the requirements of the current rules. The Commission notes that annual security incident response plan testing is consistent with industry best practices.[227]

(d) Cost Estimates for Covered DCMs and SDRs.

The Commission did not receive any comments addressing the costs of conducting security incident response plan testing for covered DCMs and SDRs. To the extent that the final rules impose additional costs on covered DCMs and SDRs, the Commission believes that such costs may vary widely as result of numerous factors, including the size of the organization, the complexity of its automated systems, and the scope of the test.[228] Additional costs incurred by the affected entities could include time in reviewing and revising current policies and procedures, initially and on an ongoing basis, concerning security incident response testing to ensure that they are sufficient in the context of the new requirements. In such cases, the Commission believes that any costs would be minimal.

---

[226] See Commission regulations §§ 38.1051(h) (for DCMs) and 49.24(j) (for SDRs); 17 CFR 38.1051(h); 17 CFR 49.24(j).

[227] NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, at 2-4 (citing NIST SP 800-53, Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations).

[228] Based on the Commission's experience in administering the system safeguard compliance program, the Commission believes that many large DCMs and SDRs currently conduct security incident response plan testing at the minimum frequency specified in the final rule.

(3) Benefits.

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

The final rules provide clarity to covered DCMs and SDRs concerning the minimum testing frequency for security incident response plans. The Commission believes that the frequency requirement would increase the likelihood that these entities could mitigate the duration and impact in the event of a security incident by making them better prepared for such an incident. Therefore, a covered DCM or SDR may also be better positioned to reduce any potential impacts to its automated system operation, reliability, security, or capacity; or the availability, confidentiality, or integrity of its futures and swaps data.

k. Enterprise Technology Risk Assessment: §§ 38.1051(h)(7), 37.1401(h)(7), and 49.24(j)(7).

(1) Summary of Final Rules.

The final rules define enterprise technology risk assessment as an assessment that includes an analysis of threats and vulnerabilities in the context of mitigating controls. In addition, the assessment identifies, estimates, and prioritizes risks to the entity's operations or assets, or to market participants, individuals, or other entities, resulting from impairment of the confidentiality, integrity, and availability of data and information

or the reliability, security, or capacity of automated systems. The final rules require covered DCMs and SDRs to conduct an ETRA at a frequency determined by an appropriate risk analysis, but at a minimum no less frequently than annually. The final rules provide that all DCMs, SEFs, and SDRs may conduct ETRAs by using independent contractors, or employees of the entity who are not responsible for development or operation of the systems or capabilities being assessed.

(2) Costs and Discussion of Comments.

(a) ETRAs for All DCMs, SEFs, and SDRs.

As stated in the NPRM and above in the Baseline discussion, the Act requires each DCM, SEF, and SDR to develop and maintain a program of system safeguards-related risk analysis and oversight to identify and minimize sources of operational risk.[229] The Act mandates that in this connection each DCM, SEF, and SDR must develop and maintain automated systems that are reliable, secure, and have adequate scalable capacity, and must ensure system reliability, security, and capacity through appropriate controls and procedures.[230]

The Commission's current system safeguards rules for DCMs, SEFs, and SDRs mandate that, in order to achieve these statutory requirements, each DCM, SEF, and SDR must conduct testing and review sufficient to ensure that its automated systems are reliable, secure, and have adequate scalable capacity.[231] The Commission believes, as the generally accepted standards and best practices noted in the NPRM make clear, that it is

[229] 80 FR 80139, 80164, 80175 (Dec. 23, 2015). CEA § 5(d)(20) (for DCMs); CEA § 5h(f)(14) (for SEFs); CEA § 21(f)(4)(A) and 17 CFR 49.24(a) (for SDRs).

[230] Id.

[231] Commission regulations §§ 38.1051(h) (for DCMs), 37.1401(g) (for SEFs), and 49.24(j) (for SDRs). 17 CFR 38.1051(h); 17 CFR 37.1401(g); and 17 CFR 49.24(j).

essentially impossible for a DCM, SEF, or SDR to fulfill its current obligation to conduct testing sufficient to ensure the reliability, security, and capacity of its automated systems without conducting ETRAs.[232] If compliance with the current testing requirements as clarified by the final rules results in costs to a DCM, SEF, or SDR beyond those it already incurs in this connection, the Commission believes that such additional costs are attributable to compliance with the current rules and not to the final rules. Accordingly, the Commission believes that clarifying the rules will not impose any new costs for DCMs, SEFs, and SDRs.

(b) ETRAs by Independent Contractors or Employees of the DCM, SEF, or SDR.

The Commission did not receive any comments addressing the costs of the proposed rules which called for ETRAs to be conducted by either independent contractors or employees not responsible for development or operation of the systems or capabilities. The Commission is adopting the proposed requirements and all DCMs, SEFs, and SDRs will have the same flexibility in the final rules.

(c) ETRA Frequency Requirement for Covered DCMs and SDRs.

The final rules require covered DCMs and SDRs to conduct ETRAs at least annually. The Commission's current rules require DCMs and SDRs to conduct regular, periodic, objective testing of their automated systems.[233] Therefore, the final rules will impose new costs relative to the requirements of the current rules.[234] CME suggested

---

[232] 80 FR 80139, 80175 (Dec. 23, 2015). See, e.g., NIST 800-53A, Rev.1, at F226, June 2010, available at http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf.

[233] See Commission regulations §§ 38.1051(h) (for DCMs) and 49.24(j) (for SDRs); 17 CFR 38.1051(h); 17 CFR 49.24(j).

[234] Based on the information from the DMO Preliminary Survey, the Commission understands that most large DCMs and SDRs currently conduct ETRAs at the minimum frequency specified in the final rule.

that ETRAs would benefit from incorporating the results of controls testing and other testing, and suggested that it would be beneficial and less costly to align the requirement for completing an ETRA with the applicable frequency requirement for controls testing. Tradeweb suggested that an annual full assessment would be burdensome and costly, and suggested that, in lieu of repeated full assessments, annual review and approval of previous assessments should be sufficient. The Commission believes that, as best practices provide, regularly updated ETRAs are crucial to the effectiveness of system safeguards in today's rapidly changing cybersecurity environment.[235] The Commission does not accept the suggestion that ETRAs should only be required as often as a complete cycle of controls testing is completed, not least because the final rule is adopting the suggestion to lengthen that cycle to three rather than two years. Because ETRAs that provide current assessment of current risks are essential to effective programs of system safeguards risk analysis and oversight, the Commission disagrees with the suggestion that annual review and re-approval of previous assessments would be sufficient. However, the Commission believes that thorough updating of a previous assessment conducted in compliance with the ETRA requirements set out in the NPRM can be sufficient to fulfill the purposes of an appropriate ETRA, and can reduce costs and burdens without impairment of the purposes of the CEA and the system safeguards rules. Accordingly, the final rules clarify that such updating of a previous fully compliant ETRA, in light of current risks and circumstances, can fulfill the ETRA requirement.

[235] FINRA, Report on Cybersecurity Practices (February 2015), at 14, available at https://www.finra.org/sites/ default/ files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf.

(d) Cost Estimates for Covered DCMs and SDRs.

CME estimated that the Commission's proposed ETRA requirement would result in an additional cost of $500,000 every two years. Based on the information from the DMO Preliminary Survey, the current average cost for covered DCMs and SDRs conducting the assessment is approximately $1,347,950 annually. However, the Commission notes that actual costs may vary widely among the affected entities due to the size of the organization, the complexity of the automated systems, and the scope of the assessment. The Commission recognizes that the affected entities may undertake an evaluation, on an initial and ongoing basis, regarding internal policies and procedures that may need to be revised. If such an evaluation is required, the Commission believes that any incremental costs will be minor.

(3) Benefits.

The Commission believes that ETRAs are an essential component of a comprehensive system safeguard program. ETRAs can be viewed as a strategic approach through which DCMs, SEFs, and SDRs identify risks and align their systems goals accordingly. The Commission believes that these requirements are necessary to support a strong risk management framework, thereby helping to protect DCMs, SEFs, SDRs, and market participants, and helping to mitigate the risk of market disruptions.

The final rules provide clarity to covered DCMs and SDRs concerning the minimum assessment frequency. Best practices support annual or more frequent assessment of technology and cybersecurity risk. For example, FINRA states that firms conducting appropriate risk assessment do so either annually or on an ongoing basis

throughout the year, in either case culminating in an annual risk assessment report.[236] The Commission believes that the frequency requirement would better position covered DCMs and SDRs to identify, estimate, and prioritize the risks facing them in today's cybersecurity threat environment.

l. Scope for Testing and Assessment: §§ 38.1051(k), 37.1401(k), and 49.24(l).

(1) Summary of Final Rules.

The final rules provide that the scope for all system safeguards testing and assessment must be broad enough to include the testing of automated systems and controls that the entity'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, augment, 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.

(2) Costs and Benefits and Discussion of Comments.

The Commission believes that the costs and benefits associated with the scope for testing and assessment are generally attributable to the substantive testing requirements; therefore they are generally discussed in the cost and benefit considerations related to the

[236] FINRA, Report on Cybersecurity Practices (February 2015), at 14, available at https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf.

rules describing the requirements for each test or assessment. However, as discussed in the preamble, a number of commenters suggested that the scope provisions of the NPRM were overbroad, and that the proposed requirement to perform "all" testing necessary to identify "any" vulnerability was impossible to achieve in practice. CME suggested that the NPRM's overbroad scope provision could impose outsized costs without yielding commensurate benefits. In order to provide the clarity requested by commenters, the final rules call for the scope of system safeguards testing to be based on appropriate risk and threat analysis. In other words, it should include the testing that the regulatee's program of risk analysis and oversight and its current cybersecurity threat analysis indicate is necessary to identify risks and vulnerabilities that could enable the deleterious actions by intruders or unauthorized users listed in the scope provisions of the proposed rules. The Commission agrees with the comments suggesting that this approach avoids imposing undue burdens and costs, while supporting the purposes of the CEA and the Commission's system safeguards rules.

m. Internal Reporting and Review: Sections 38.1051(l), 37.1401(l), and 49.24(m).

(1) Summary of Final Rules.

The final rules require the senior management and the Board of Directors of the DCM, SEF, or SDR to receive and review reports setting forth the results of all testing and assessment required by the respective sections. In addition, the final rules require the DCM, SEF, or SDR to establish and follow appropriate procedures for the remediation of issues identified through such review, as provided in sections 38.1051(m), 37.1401(m), and 49.24(n) (Remediation), and for evaluation of the effectiveness of testing and assessment protocols.

(2) Costs and Discussion of Comments.

The final rules clarify the testing requirements by specifying and defining certain aspects of DCM, SEF, and SDR risk analysis and oversight programs that are necessary to fulfillment of the testing requirements and achievement of their purposes. As stated in the NPRM, this clarification includes review of system safeguard testing and assessments by senior management and the DCM's, SEF's, or SDR's Board of Directors, which is recognized as best practice for system safeguards.[237] The Commission believes, as the generally accepted standards and best practices noted in the NPRM make clear, that it is essentially impossible for a DCM, SEF, or SDR to fulfill its current obligation to conduct testing sufficient to ensure the reliability, security, and capacity of its automated systems without performing appropriate internal reporting and review of test results.[238] If compliance with the current testing requirements as clarified by the final rules results in costs to a DCM, SEF, or SDR beyond those it already incurs, the Commission believes that such additional costs would be attributable to compliance with the current regulations and not to the final rules. Accordingly, the Commission believes that clarifying the rules will not impose any new costs for DCMs, SEFs, and SDRs.

ICE, MGEX, and Nadex commented that test result reports can be voluminous, technical, and complex, and that requiring boards and senior management to review each such document could produce an undue burden without commensurate benefits. As discussed in the preamble, the Commission notes that effective board of directors and senior management oversight of system safeguards does not require board or senior

[237] 80 FR 80139, 80176 (Dec. 23, 2015).

[238] See, e.g., NIST SP 800-115, Technical Guide to Information Security Testing and Assessment, at 6-10 – 6-12, September 2008, available at http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf.

management review of every detail of each such report. Board and senior management review of appropriate summaries and compilations of test and assessment results can be an effective and acceptable way of fulfilling the internal reporting and review requirement, provided that such summaries give board members and senior management sufficiently detailed information to enable them to conduct effective and informed oversight. The appropriate level of information should also enable boards and senior management to evaluate the overall effectiveness of testing and assessment protocols, and direct and oversee appropriate remediation of issues identified through their review of test results.

(3) Benefits.

The Commission believes that internal reporting and review are an essential component of a comprehensive and effective system safeguard program. While senior management and the DCM's, SEF's, or SDR's board of directors will have to devote resources to reviewing testing and assessment reports, active supervision by senior management and the board of directors promotes responsibility and accountability by affording them greater opportunity to evaluate the effectiveness of the testing and assessment protocols. Moreover, the attention by the board of directors and senior management should help to promote a focus on such reviews and issues, and enhance communication and coordination regarding such reviews and issues among the business, technology, legal, and compliance personnel of the DCM, SEF, and SDR. Active supervision by senior management and the board of directors also promotes a more efficient, effective, and reliable DCM and SDR risk management and operating structure.

Consequently, DCMs, SEFs, and SDRs should be better positioned to strengthen the integrity, resiliency, and availability of their automated systems.

n. Remediation: §§ 38.1051(m), 37.1401(m), and 49.24(n).

(1) Summary of Final Rules.

The final rules require DCMs, SEFs, and SDRs to identify and document the vulnerabilities and deficiencies in the entity's systems revealed by the testing and assessment in the respective sections. The entity shall conduct and document an appropriate risk analysis of the risks presented by such vulnerabilities and deficiencies, to determine and document whether to remediate or accept each risk. When an entity determines to remediate a vulnerability or deficiency, it must remediate in a timely manner given the nature and magnitude of the associated risk. The Commission did not receive any comments regarding the costs and benefits of the proposed rules.

(2) Costs and Discussion of Comments.

The final rules clarify the testing requirements by specifying and defining certain aspects of DCM, SEF, and SDR risk analysis and oversight programs that are necessary to fulfillment of the testing requirements and achievement of their purposes. This clarification includes remediation. As stated in the NPRM, remediation of vulnerabilities and deficiencies revealed by cybersecurity testing is a best practice and a fundamental purpose of such testing.[239] The Commission believes, as the generally accepted standards and best practices noted in the NPRM make clear, that it is essentially impossible for a DCM, SEF, or SDR to fulfill its current obligation to conduct testing sufficient to ensure the reliability, security, and capacity of its automated systems without performing

[239] 80 FR 80139, 80167 (Dec. 23, 2015).

remediation.[240] If compliance with the current testing requirements as clarified by the final rules results in costs to a DCM, SEF, or SDR beyond those it already incurs, the Commission believes that such additional costs would be attributable to compliance with the current regulations and not to the final rules. Accordingly, the Commission believes that clarifying the rules will not impose any new costs for DCMs, SEFs, and SDRs. However, as discussed below, the Commission is amending two aspects in the final rules where it believes the net effect will reduce the overall costs and burdens relative to the proposed rules.

Nadex and Tradeweb suggested that the proposed requirement to identify and remediate "all" vulnerabilities and deficiencies in a regulatee's systems was impossible to achieve in practice. Nadex observed that other discussion in the NPRM indicated Commission intent to require remediation of vulnerabilities and deficiencies identified in the testing results, and suggested amending the final rule to make this clear. Noting that remediation after a cyber attack often takes time, Tradeweb argued that regulatees should not be penalized for that fact, and requested Commission guidance on what constitutes timely remediation, perhaps including specification that remediation over nine to twelve months would be timely. As discussed in the preamble, the Commission agrees with commenters that a requirement calling for a DCM, SEF, or SDR to remediate all vulnerabilities and deficiencies could be read as overbroad and impossible in practice. Accordingly, the Commission is narrowing the remediation requirement to address remediation or acceptance of the vulnerabilities and deficiencies of which an entity is aware or through an appropriate program of risk analysis and oversight should be aware,

[240] See, e.g., NIST SP 800-115, Technical Guide to Information Security Testing and Assessment, at 6-10 – 6-12, September 2008, available at http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf.

rather than the remediation of all vulnerabilities and deficiencies. This revision is being made to reduce burdens and costs to the extent possible without impairing the purposes of the CEA and the Commission's system safeguards regulations.

The aspect of the final rules that could impose a slight additional cost relative to the proposed rules is the explicit requirement that all DCMs, SEFs, and SDRs 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 its decision concerning whether to remediate or accept each risk and the remediation steps chosen. As stated in the preamble, the NPRM proposal to require identification of vulnerabilities was intended to include their documentation. Effective remediation would be impossible without documentation of both the vulnerabilities in question and the remediation steps needed. However, because documentation was not explicitly required in the proposal, the Commission is treating the documentation requirement in the final rules as a possible slight additional cost. The Commission notes, however, that the narrowing of remediation requirement in the final rules represents a considerable reduction in burdens and costs and will more than offset the burdens and costs associated with the documentation requirement.

(3) Benefits.

The Commission believes that effective remediation is a critical component of a comprehensive and effective system safeguard program. Moreover, remediation may reduce the frequency and severity of systems disruptions and breaches. In addition, remediation helps to ensure that DCMs, SEFs, and SDRs dedicate appropriate resources to address system safeguard-related deficiencies in a timely fashion. Remediation also

places an emphasis on mitigating harm to market participants while promoting market integrity. Without a requirement for timely remediation, the impact of vulnerabilities or deficiencies identified by the testing or assessment could persist and have a detrimental effect on the futures and swaps markets generally as well as market participants.

o. Required Production of Annual Trading Volume: § 38.1051(n).

(1) Summary of Final Rule.

The final rule requires each DCM to provide its annual total trading volume to the Commission for calendar year 2015 and each calendar year thereafter. This information is required for 2015 within 30 calendar days of the effective date of the final version of this rule, and required for 2016 and subsequent years by January 31 of the following calendar year.

(2) Costs and Discussion of Comments.

As discussed in the PRA section, the Commission did not receive any comments concerning the accuracy of its estimate that each DCM would spend approximately $22.00 annually to comply with the proposed requirement. However, CME stated that the Commission should consider alternatives to the reporting requirements in proposed § 38.1051(n) because the Commission currently receives daily trade reports regarding volume pursuant to DCM Core Principle 8 and part 16 of the Commission's regulations. The Commission notes that while it receives daily trade information from DCMs pursuant to part 16, it does not receive total annual trading volume from DCMs. Additionally, the Commission believes that Core Principle 8 is inapplicable because it requires DCMs to publish daily volume, but does not require submission of that information to the Commission. The submission of annual trading volume is essential for

the Commission to accurately evaluate whether a particular DCM must comply with the enhanced system safeguard requirements. The Commission believes that all DCMs generally calculate their annual trading volume in the usual course of business and many of the DCMs already publish this information on their web site. The Commission also believes that each DCM would spend approximately half an hour to prepare and file the trading volume information with Commission at a cost of approximately $24.80 annually.[241]

(3) Benefits.

The Commission believes that it is necessary to require all DCMs to provide the Commission with annual trading volume information. Otherwise, the Commission would be unable to accurately evaluate whether a particular DCM would be subject to the enhanced covered DCM requirements. As stated in the final rule, the Commission will provide each DCM with its percentage of the combined annual trading volume of all DCMs regulated by the Commission for the preceding calendar year within 60 calendar days of the effective date of the final rule, and for subsequent years by February 28. Therefore, all DCMs will receive certainty from the Commission regarding whether they must comply with the provisions applicable to covered DCMs. This requirement will support more accurate application of the final rules.

[241] 80 FR 80139, 80177 (Dec. 23, 2015). In arriving at a wage rate for the hourly costs imposed, Commission staff used the National Industry-Specific Occupational Employment and Wage Estimates, published in May (2015 Report). The hourly rate for a Compliance Officer in the Securities and Commodity Exchanges as published in the 2015 Report was $49.59 per hour. In the NPRM, the Commission's estimate of $22.00 per respondent was based on the hourly wage of $44.03 for a Compliance Officer in the 2014 Report. 80 FR 80139, 80163 (Dec. 23, 2015).

4. Section 15(a) Factors.

a. Protection of Market Participants and the Public.

The Commission believes that the final rules will benefit the futures and swaps markets by promoting more robust automated systems and therefore fewer disruptions and market-wide closures, systems compliance issues, and systems intrusions. Fewer disruptions mean that investors will be able to trade more predictably, reducing the likelihood of investors facing difficulty in, for example, liquidating positions. Because automated systems play a central and critical role in today's electronic financial market environment, oversight of DCMs, SEFs, and SDRs with respect to automated systems is an essential part of effective oversight of both futures and swaps markets. In addition, providing the Commission with reports concerning system safeguards testing and assessments required by the rules will facilitate the Commission's oversight of futures and swaps 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 automated systems are available, reliable, secure, have adequate scalable capacity, and are effectively overseen. As a result, the Commission also expects fewer interruptions to the systems that directly support the respective entities, including matching engines, regulatory and surveillance systems, and the dissemination of market data, which should help ensure compliance with the relevant statutory and regulatory obligations. Moreover, market participants will benefit from systems that are secure and able to protect their anonymity with respect to positions in the marketplace and other aspects of their personally-identifiable information.

b. Efficiency, Competitiveness, and Financial Integrity of the Markets.

A DCM or SEF that has system safeguard policies and procedures in place, including the timely remediation of vulnerabilities and deficiencies in light of appropriate risk analysis, will promote overall market confidence and could lead to greater market efficiency, competitiveness, and perceptions of financial integrity. Safeguarding the reliability, security, and capacity of DCM, SEF, and SDR computer systems is essential to mitigation of systemic risk for the nation's financial sector as a whole. A comprehensive testing program capable of identifying operational risks will enhance the efficiency, and financial integrity of the markets by increasing the likelihood that trading remains uninterrupted and transactional data and positions are not lost.[242] A DCM or SEF with such a program also promotes confidence in the markets, and encourages liquidity and stability. Moreover, the ability of a DCM or SEF to recover and resume trading promptly in the event of a disruption of their operations, or an SDR to recover and resume its swap data recordkeeping and reporting function, is highly important to the U.S. economy and ensuring the resiliency of the automated systems is a critical part of the Commission's mission. Because SDRs hold data needed by financial regulators from multiple jurisdictions, safeguarding such systems will also be essential to mitigation of systemic risk world-wide. Notice to the Commission concerning the results of system safeguard tests performed by DCMs, SEFs, and SDRs will assist the Commission's oversight and its ability to assess systemic risk levels. It would present unacceptable risks to the U.S. financial system if futures and swaps markets that comprise critical

[242] During the CFTC Roundtable, one of the participants noted that "if data is disclosed about activity in the markets, that is a survivable event from a resiliency perspective, but if we don't know who owns what and what their positions are, then there are no markets." CFTC Roundtable, at 71.

components of the world financial system, and SDRs that hold data concerning swaps, were to become unavailable for an extended period of time for any reason, and adequate system safeguards are essential to the mitigation of such risks.

c. Price Discovery.

Any interruption in trading on a DCM or SEF can distort the price discovery process by preventing prices from adjusting to new information. Similarly, any interruption in the operations of an SDR will reduce the transparency of swap prices, thereby making it more difficult for traders to observe prices, and leading to the potential for higher trading costs. Interruptions in SDR operations also hamper the Commission's ability to examine potential price discrepancies and other trading inconsistencies in the swaps market. Therefore, reliable functioning computer systems and networks are essential in protecting the price discovery process. The Commission believes that the final rules will reduce the incidence and severity of automated system security breaches and functional failures. In addition, the Commission views the final rules as likely to facilitate the price discovery process by mitigating the risk of operational market interruptions from disjoining forces of supply and demand. The presence of thorough system safeguards testing signals to the market that a DCM or SEF is a financially sound place to trade, thus attracting greater liquidity which leads to more accurate price discovery.

d. Sound Risk Management Practices.

The final rules will benefit the risk management practices of both the regulated entities and the participants who use the facilities of those entities. Participants who use DCMs or SEFs to manage commercial price risks should benefit from markets that

behave in an orderly and controlled fashion. If prices move in an uncontrolled fashion due to a cybersecurity incident, those who manage risk may be forced to exit the market as a result of unwarranted margin calls or deterioration of their capital. In addition, those who want to enter the market to manage risk may only be able to do so at prices that do not reflect the actual supply and demand fundamentals due to the effects of a cybersecurity incident. Relatedly, participants may have greater confidence in their ability to unwind positions because market disruptions would be less common. With respect to SDRs, the Commission believes that the ability of participants in the swaps market to report swap transactions to an SDR likewise serve to allow participants to better observe swap prices, hence lowering trading costs. Fewer interruptions of SDR operations also serve to improve regulators' ability to monitor risk management practices through better knowledge of open positions and SDR services related to various trade, collateral, and risk management practices. The Commission notes regulator access (both domestic and foreign) to the data held by an SDR is essential for regulators to be able to monitor the swap market and certain participants relating to systemic risk.

5. Antitrust Considerations.

Section 15(b) of the CEA requires the Commission to take into consideration the public interest to be protected by the antitrust laws and endeavor to take the least anticompetitive means of achieving the objectives of the CEA in issuing any order or adopting any Commission rule or regulation. The Commission does not anticipate that the amendments adopted herein would promote or result in anticompetitive consequences or behavior.

IV. COMPLIANCE DATES

A. Comments Received.

For final rules issued by the Commission and published in the Federal Register, the Commission has discretion to set both the date on which a final rule becomes effective following its publication (the "effective date") and the date on which it will begin enforcement of regulatory provisions (the "compliance date").[243] In setting forth effective dates and compliance dates, the Commission considers the nature and particular provisions of the rule in question, comments received, available enforcement resources, and the goals and purposes of the CEA and the rule.

The Commission received comments concerning when full compliance with the provisions of the system safeguards testing requirements rule should be enforced for designated contract markets, swap data repositories, and swap execution facilities. Tradeweb suggested that the Commission specify an adequate implementation period of 9 to 12 months for the final rule, to allow regulatees sufficient time to prepare and implement additional policies and procedures needed to comply with the rule. CFE commented that the Commission should provide an implementation period sufficient to allow regulatees to review the final rules, compare them with their current testing and current risk analysis and oversight programs, and implement any changes needed. CFE noted that when the Securities and Exchange Commission ("SEC") adopted its comparable Regulation Systems Compliance and Integrity ("Regulation SCI"), that regulation became effective 60 days after Federal Register publication, and the SEC

[243] See Heckler v. Chaney, 470 U.S. 821 (1985).

adopted a compliance date of nine months after the effective date. CFE urged the Commission to take the same approach.

The Commission has considered these comments, agrees with them, and has determined to provide an effective date and compliance dates for system safeguards testing effectively incorporating commenters' suggestions, as set forth below.

The Commission notes that various aspects of the final rule require compliance within a specified period of time, such as performance of certain types of testing quarterly or annually. A starting point is needed for measurement of such periods. Because cybersecurity testing is crucial to resilience in today's cybersecurity threat environment, the Commission believes that prudence and protection of the public interest require starting the "clock" for measuring the periods within which the various types of testing required by the final rule must be conducted as soon as possible, by setting the earliest possible effective date for the rule. Starting the clock in this way does not mean that instant compliance is required; rather, the effective date provides the starting point for measuring the implementation period provided between the effective date and the compliance date on which a given provision of the rule is enforceable. Within this implementation period, a regulated entity can review the rule's requirements, compare them with current testing and risk analysis and oversight practices, implement any needed changes, and come into compliance with the rule.

For these reasons, the Commission has determined to set the effective date of this final rule as the date of its publication in the Federal Register, and to set the compliance dates applicable to the various provisions of the final rule as set forth below.

1. For vulnerability testing, the compliance date shall be 180 calendar days after the effective date. DCMs, SEFs, and SDRs must be conducting vulnerability testing that complies with this final rule by that compliance date.

2. For both external and internal penetration testing, the compliance date shall be one year after the effective date. DCMs, SEFs, and SDRs must conduct and complete penetration testing that complies with this final rule by that compliance date. Covered DCMs and SDRs must engage an independent contractor to conduct and complete penetration testing that complies with this final rule by that compliance date.

3. For controls testing, the compliance date shall be one year after the effective date. DCMs, SEFs, and SDRs must be conducting controls testing that complies with this final rule by that compliance date. Covered DCMs and SDRs must engage an independent contractor to conduct and complete testing of all key controls within three years of the effective date.

4. For SIRP testing, the compliance date shall be 180 days after the effective date. DCMs, SEFs, and SDRs must have a SIRP and complete testing of the SIRP by that compliance date.

5. For enterprise technology risk assessment, the compliance date shall be one year after the effective date. DCMs, SEFs, and SDRs must complete an ETRA that complies with this final rule by that compliance date.

6. For required updating of BC-DR plans and emergency procedures, the compliance date shall be one year after the effective date. DCMs, SEFs, and SDRs must complete an update of their BC-DR plans and emergency procedures by that compliance date.

7. For required production by DCMs of their annual total trading volume, the compliance date shall be 30 calendar days after the effective date.

8. For system safeguards books and records requirements, the compliance date shall be the effective date.

9. For all other aspects of the final rule, the compliance date shall be one year after the effective date. DCMs, SEFs, and SDRs must be in full compliance with the final rule by that compliance date.

List of subjects in 17 CFR Parts 37, 38, and 49

System Safeguards Testing Requirements

For the reasons set forth in the preamble, the Commodity Futures Trading Commission is amending part 37, part 38, and part 49 as follows:

Part 37, Section 37.1401

Authority: 7 U.S.C. 1a, 2, 5, 6, 6c, 7, 7a-2, 7b-3, and 12a, as amended by Titles VII and VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376 (2010).

Amend Part 37, Subpart O—System Safeguards, § 37.1401, by removing current § 37.1401(a) and adding new § 37.1401(a); adding new § 37.1401(b); removing current § 37.1401(b) and adding new § 37.1401(c); redesignating current §§ 37.1401(c) through (e) as §§ 37.1401(d) through (f); removing current § (f) and adding new § 37.1401(g); removing current § 37.1401(g) and adding new § 37.1401(h); adding new § 37.1401(i); redesignating current §37.1401(h) as §37.1401(j); adding new §§ 37.1401(k) through (m); and removing and reserving Guidance for Core Principle 14 of Section 5h of the

Act—System Safeguards in Appendix B to Part 37—Guidance on, and Acceptable Practices in, Compliance with Core Principles; to read as follows:

(a) A swap execution facility's program of risk analysis and oversight with respect to its operations and automated systems shall address each of the following categories of risk analysis and oversight:

(1) Enterprise risk management and governance. This category includes, but is not limited to: assessment, mitigation, and monitoring of security and technology risk; security and technology capital planning and investment; board of directors and management oversight of technology and security; information technology audit and controls assessments; remediation of deficiencies; and any other elements of enterprise risk management and governance included in generally accepted best practices.

(2) Information security. This category includes, but is 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.

(3) Business continuity-disaster recovery planning and resources. This category includes, but is not limited to: regular, periodic testing and review of business continuity-disaster recovery capabilities, the controls and capabilities described in paragraph (c), (d),

(j), and (k) of this section; and any other elements of business continuity-disaster recovery planning and resources included in generally accepted best practices.

(4) Capacity and performance planning. This category includes, but is not limited to: controls for monitoring the swap execution facility'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.

(5) Systems operations. This category includes, but is 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.

(6) Systems development and quality assurance. This category includes, but is 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.

(7) Physical security and environmental controls. This category includes, but is 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.

(b) In addressing the categories of risk analysis and oversight required under paragraph (a) of this section, a swap execution facility shall follow generally accepted standards and best practices with respect to the development, operation, reliability, security, and capacity of automated systems.

(c) A swap execution facility shall maintain a business continuity-disaster recovery plan and business continuity-disaster recovery resources, emergency procedures, and backup facilities sufficient to enable timely recovery and resumption of its operations and resumption of its ongoing fulfillment of its responsibilities and obligations as a swap execution facility following any disruption of its operations. Such responsibilities and obligations include, without limitation: order processing and trade matching; transmission of matched orders to a designated clearing organization for clearing, where appropriate; price reporting; market surveillance; and maintenance of a comprehensive audit trail. A swap execution facility's business continuity-disaster recovery plan and resources generally should enable resumption of trading and clearing of swaps executed on or pursuant to the rules of the swap execution facility during the next business day following the disruption. Swap execution facilities determined by the Commission to be critical financial markets are subject to more stringent requirements in this regard, set forth in § 40.9 of this chapter. A swap execution facility shall update its business continuity-disaster recovery plan and emergency procedures at a frequency determined by an appropriate risk analysis, but at a minimum no less frequently than annually.

* * * * *

(g) As part of a swap execution facility's obligation to produce books and records in accordance with Commission regulation § 1.31, Core Principle 10 (Recordkeeping and

Reporting), and §§ 37.1000 and 37.1001 of this part, a swap execution facility shall provide to the Commission the following system safeguards-related books and records, promptly upon the request of any Commission representative:

(i) Current copies of its business continuity-disaster recovery plans and other emergency procedures;

(ii) All assessments of its operational risks or system safeguards-related controls;

(iii) All reports concerning system safeguards testing and assessment required by this chapter, whether performed by independent contractors or by employees of the swap execution facility; and

(iv) All other books and records requested by Commission staff 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 swap execution facility's automated systems.

(v) Nothing in this § 37.1401(g) shall be interpreted as reducing or limiting in any way a swap execution facility's obligation to comply with Core Principle 10 (Recordkeeping and Reporting) or with §§ 1.31, 37.1000, or 37.1001 of the Commission's regulations.

(h) A swap execution facility shall conduct regular, periodic, objective testing and review of its automated systems to ensure that they are reliable, secure, and have adequate scalable capacity. It shall also conduct regular, periodic testing and review of its business continuity-disaster recovery capabilities. Such testing and review shall include, without limitation, all of the types of testing set forth in this paragraph (h).

(1) Definitions. As used in section 37.1401(h) of this part:

Controls means the safeguards or countermeasures employed by the swap execution facility in order to protect the reliability, security, or capacity of its automated systems or the confidentiality, integrity, and availability of its data and information, and in order to enable the swap execution facility to fulfill its statutory and regulatory responsibilities.

Controls testing means assessment of the swap execution facility's controls to determine whether such controls are implemented correctly, are operating as intended, and are enabling the swap execution facility 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 swap execution facility operations or assets, or to market participants, individuals, or other entities, resulting from impairment of the confidentiality, integrity, and availability of data and information or the reliability, security, or capacity of automated systems.

External penetration testing means attempts to penetrate the swap execution facility'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 the swap execution facility'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.

Security incident means a cyber security 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 swap execution facility'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 swap execution facility'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 swap execution facility'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.

(2) Vulnerability testing. A swap execution facility shall conduct vulnerability testing of a scope sufficient to satisfy the requirements set forth in section 37.1401(k) of this part.`

(i) A swap execution facility shall conduct such vulnerability testing at a frequency determined by an appropriate risk analysis.

(ii) Such vulnerability testing shall include automated vulnerability scanning, which shall follow generally accepted best practices.

(iii) A swap execution facility shall conduct vulnerability testing by engaging independent contractors or by using employees of the swap execution facility who are not responsible for development or operation of the systems or capabilities being tested.

(3) External penetration testing. A swap execution facility shall conduct external penetration testing of a scope sufficient to satisfy the requirements set forth in section 37.1401(k) of this part.

(i) A swap execution facility shall conduct such external penetration testing at a frequency determined by an appropriate risk analysis.

(ii) A swap execution facility shall conduct external penetration testing by engaging independent contractors or by using employees of the swap execution facility who are not responsible for development or operation of the systems or capabilities being tested.

(4) Internal penetration testing. A swap execution facility shall conduct internal penetration testing of a scope sufficient to satisfy the requirements set forth in section 37.1401(k) of this part.

(i) A swap execution facility shall conduct such internal penetration testing at a frequency determined by an appropriate risk analysis.

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

(5) Controls testing. A swap execution facility shall conduct controls testing of a scope sufficient to satisfy the requirements set forth in section 37.1401(k) of this part.

(i) A swap execution facility 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. Such testing may be conducted on a rolling basis.

(ii) A swap execution facility shall conduct controls testing by engaging independent contractors or by using employees of the swap execution facility who are not responsible for development or operation of the systems or capabilities being tested.

(6) Security incident response plan testing. A swap execution facility shall conduct security incident response plan testing sufficient to satisfy the requirements set forth in section 37.1401(k) of this part.

(i) A swap execution facility shall conduct such security incident response plan testing at a frequency determined by an appropriate risk analysis.

(ii) A swap execution facility's security incident response plan shall include, without limitation, the swap execution facility'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) A swap execution facility 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) A swap execution facility may conduct security incident response plan testing by engaging independent contractors or by using employees of the swap execution facility.

(7) Enterprise technology risk assessment. A swap execution facility shall conduct enterprise technology risk assessment of a scope sufficient to satisfy the requirements set forth in section 37.1401(k) of this part.

(i) A swap execution facility shall conduct enterprise technology risk assessment at a frequency determined by an appropriate risk analysis. A swap execution facility that has conducted an enterprise technology risk assessment that complies with this section may conduct subsequent assessments by updating the previous assessment.

(ii) A swap execution facility may conduct enterprise technology risk assessments by using independent contractors or employees of the swap execution

facility who are not responsible for development or operation of the systems or capabilities being assessed.

(i) To the extent practicable, a swap execution facility shall:

(i) Coordinate its business continuity-disaster recovery plan with those of the market participants it depends upon to provide liquidity, in a manner adequate to enable effective resumption of activity in its markets following a disruption causing activation of the swap execution facility's business continuity-disaster recovery plan;

(ii) Initiate and coordinate periodic, synchronized testing of its business continuity-disaster recovery plan with those of the market participants it depends upon to provide liquidity; and

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

* * * * *

(k) Scope of testing and assessment. The scope for all system safeguards testing and assessment required by this part shall be broad enough to include the testing of automated systems and controls that the swap execution facility'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 swap execution facility's operations or with fulfillment of its statutory and regulatory responsibilities;

(ii) Impair or degrade the reliability, security, or adequate scalable capacity of the swap execution facility's automated systems;

(iii) Add to, delete, modify, exfiltrate, or compromise the integrity of any data related to the swap execution facility's regulated activities; or

(iv) Undertake any other unauthorized action affecting the swap execution facility's regulated activities or the hardware or software used in connection with those activities.

(l) Internal reporting and review. Both the senior management and the Board of Directors of a swap execution facility shall receive and review reports setting forth the results of the testing and assessment required by this section. A swap execution facility shall establish and follow appropriate procedures for the remediation of issues identified through such review, as provided in section 37.1401(m) of this part, and for evaluation of the effectiveness of testing and assessment protocols.

(m) Remediation. A swap execution facility shall identify and document the vulnerabilities and deficiencies in its systems revealed by the testing and assessment required by this section. The swap execution facility shall conduct and document an appropriate analysis of the risks presented by such vulnerabilities and deficiencies, to determine and document whether to remediate or accept the associated risk. When the swap execution facility determines to remediate a vulnerability or deficiency, it must remediate in a timely manner given the nature and magnitude of the associated risk.

Part 38, Section 38.1051

Authority: 7 U.S.C. 1a, 2, 6, 6a, 6c, 6d, 6f, 6g, 6i, 6j, 6k, 6l, 6m, 6n, 7, 7a-s, 7b, 7b-1, 7b-3, 8, 9, 15, and 21, as amended by the Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376 (2010).

Amend Part 38, Subpart U—System Safeguards, § 38.1051, by removing current § 38.1051(a) and adding new § 38.1051(a); amending § 38.1051(b) by removing the word "should" and adding the word "shall" in its place; amending current § 38.1051(c) by adding a sentence at the end of the current section; removing current § 38.1051(g) and adding new § 38.1051(g); removing current § 38.1051(h) and adding new § 38.1051(h); and adding new §§ 38.1051(k), 38.1051(l), 38.1051(m), and 38.1051(n), to read as follows:

(a) A designated contract market's program of risk analysis and oversight with respect to its operations and automated systems shall address each of the following categories of risk analysis and oversight:

(1) Enterprise risk management and governance. This category includes, but is not limited to: assessment, mitigation, and monitoring of security and technology risk; security and technology capital planning and investment; board of directors and management oversight of technology and security; information technology audit and controls assessments; remediation of deficiencies; and any other elements of enterprise risk management and governance included in generally accepted best practices.

(2) Information security. This category includes, but is 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.

(3) Business continuity-disaster recovery planning and resources. This category includes, but is not limited to: regular, periodic testing and review of business continuity-disaster recovery capabilities, the controls and capabilities described in paragraph (c), (d), (j), and (k) of this section; and any other elements of business continuity-disaster recovery planning and resources included in generally accepted best practices.

(4) Capacity and performance planning. This category includes, but is not limited to: controls for monitoring the designated contract market'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.

(5) Systems operations. This category includes, but is 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.

(6) Systems development and quality assurance. This category includes, but is 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.

(7) Physical security and environmental controls. This category includes, but is 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.

(b) In addressing the categories of risk analysis and oversight required under paragraph (a) of this section, a designated contract market shall follow generally accepted standards and best practices with respect to the development, operation, reliability, security, and capacity of automated systems.

(c) A designated contract market shall maintain a business continuity-disaster recovery plan and business continuity-disaster recovery resources, emergency procedures, and backup facilities sufficient to enable timely recovery and resumption of its operations and resumption of its ongoing fulfillment of its responsibilities and obligations as a designated contract market following any disruption of its operations. Such responsibilities and obligations include, without limitation: order processing and trade matching; transmission of matched orders to a designated clearing organization for clearing; price reporting; market surveillance; and maintenance of a comprehensive audit trail. The designated contract market's business continuity-disaster recovery plan and resources generally should enable resumption of trading and clearing of the designated contract market's products during the next business day following the disruption. Designated contract markets determined by the Commission to be critical financial markets are subject to more stringent requirements in this regard, set forth in § 40.9 of this chapter. Electronic trading is an acceptable backup for open outcry trading in the event of a disruption. A designated contract market shall update its business continuity-

disaster recovery plan and emergency procedures at a frequency determined by an appropriate risk analysis, but at a minimum no less frequently than annually.

* * * * *

(g) As part of a designated contract market's obligation to produce books and records in accordance with Commission regulation § 1.31, Core Principle 18 (Recordkeeping), and §§ 38.950 and 38.951 of this part, a designated contract market shall provide to the Commission the following system safeguards-related books and records, promptly upon the request of any Commission representative:

(i) Current copies of its business continuity-disaster recovery plans and other emergency procedures;

(ii) All assessments of its operational risks or system safeguards-related controls;

(iii) All reports concerning system safeguards testing and assessment required by this chapter, whether performed by independent contractors or by employees of the designated contract market; and

(iv) All other books and records requested by Commission staff 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 designated contract market's automated systems.

(v) Nothing in this § 38.1051(g) shall be interpreted as reducing or limiting in any way a designated contract market's obligation to comply with Core Principle 18 (Recordkeeping) or with §§ 1.31, 38.950, or 38.951 of the Commission's regulations.

(h) A designated contract market shall conduct regular, periodic, objective testing and review of its automated systems to ensure that they are reliable, secure, and have

adequate scalable capacity. It shall also conduct regular, periodic testing and review of its business continuity-disaster recovery capabilities. Such testing and review shall include, without limitation, all of the types of testing set forth in this paragraph (h). A covered designated contract market, as defined in this section, shall be subject to the additional requirements regarding minimum testing frequency and independent contractor testing set forth in this paragraph (h).

(1) Definitions. As used in section 38.1051(h) of this part:

Controls means the safeguards or countermeasures employed by the designated contract market in order to protect the reliability, security, or capacity of its automated systems or the confidentiality, integrity, and availability of its data and information, and in order to enable the designated contract market to fulfill its statutory and regulatory responsibilities.

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

Covered designated contract market means a designated contract market whose annual total trading volume in calendar year 2015, or in any subsequent calendar year, is five percent (5%) or more of the combined annual total trading volume of all designated contract markets regulated by the Commission for the year in question, based on annual total trading volume information provided to the Commission by each designated contract market pursuant to the procedure set forth in this chapter. A covered designated contract market that has annual total trading volume of less than five percent (5%) of the

combined annual total trading volume of all designated contract markets regulated by the Commission for three consecutive calendar years ceases to be a covered designated contract market as of March 1 of the calendar year following such three consecutive calendar years.

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 designated contract market operations or assets, or to market participants, individuals, or other entities, resulting from impairment of the confidentiality, integrity, and availability of data and information or the reliability, security, or capacity of automated systems.

External penetration testing means attempts to penetrate the designated contract market'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 the designated contract market'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.

Security incident means a cyber security 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 designated contract market'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 designated contract market'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 designated contract market'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.

(2) Vulnerability testing. A designated contract market shall conduct vulnerability testing of a scope sufficient to satisfy the requirements set forth in section 38.1051(k) of this part.

(i) A designated contract market shall conduct such vulnerability testing at a frequency determined by an appropriate risk analysis. At a minimum, a covered designated contract market shall conduct such vulnerability testing no less frequently than quarterly.

(ii) Such vulnerability testing shall include automated vulnerability scanning, which shall follow generally accepted best practices.

(iii) A designated contract market shall conduct vulnerability testing by engaging independent contractors or by using employees of the designated contract market who are not responsible for development or operation of the systems or capabilities being tested.

(3) External penetration testing. A designated contract market shall conduct external penetration testing of a scope sufficient to satisfy the requirements set forth in section 38.1051(k) of this part.

(i) A designated contract market shall conduct such external penetration testing at a frequency determined by an appropriate risk analysis. At a minimum, a covered designated contract market shall conduct such external penetration testing no less frequently than annually.

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

(iii) A designated contract market which is not a covered designated contract market shall conduct external penetration testing by engaging independent contractors or by using employees of the designated contract market who are not responsible for development or operation of the systems or capabilities being tested.

(4) Internal penetration testing. A designated contract market shall conduct internal penetration testing of a scope sufficient to satisfy the requirements set forth in section 38.1051(k) of this part.

(i) A designated contract market shall conduct such internal penetration testing at a frequency determined by an appropriate risk analysis. At a minimum, a covered designated contract market shall conduct such internal penetration testing no less frequently than annually.

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

(5) Controls testing. A designated contract market shall conduct controls testing of a scope sufficient to satisfy the requirements set forth in section 38.1051(k) of this part.

(i) A designated contract market 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. Such testing may be conducted on a rolling basis. At a minimum, a covered designated contract market shall conduct testing of its key controls no less frequently than every three years. The covered designated contract market may conduct testing of its key controls on a rolling basis

over the course of three years or the period determined by such risk analysis, whichever is shorter.

(ii) A covered designated contract market shall engage independent contractors to test and assess the key controls included in its program of risk analysis and oversight no less frequently than every three years. The covered designated contract market may conduct any other controls testing required by this section by using independent contractors or employees of the covered designated contract market who are not responsible for development or operation of the systems or capabilities being tested.

(iii) A designated contract market which is not a covered designated contract market shall conduct controls testing by engaging independent contractors or by using employees of the designated contract market who are not responsible for development or operation of the systems or capabilities being tested.

(6) Security incident response plan testing. A designated contract market shall conduct security incident response plan testing sufficient to satisfy the requirements set forth in section 38.1051(k) of this part.

(i) A designated contract market shall conduct such security incident response plan testing at a frequency determined by an appropriate risk analysis. At a minimum, a covered designated contract market shall conduct such security incident response plan testing no less frequently than annually.

(ii) A designated contract market's security incident response plan shall include, without limitation, the designated contract market'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) A designated contract market 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) A designated contract market may conduct security incident response plan testing by engaging independent contractors or by using employees of the designated contract market.

(7) Enterprise technology risk assessment. A designated contract market shall conduct enterprise technology risk assessment of a scope sufficient to satisfy the requirements set forth in section 38.1051(k) of this part.

(i) A designated contract market shall conduct an enterprise technology risk assessment at a frequency determined by an appropriate risk analysis. At a minimum, a covered designated contract market shall conduct an enterprise technology risk assessment no less frequently than annually. A designated contract market that has conducted an enterprise technology risk assessment that complies with this section may conduct subsequent assessments by updating the previous assessment.

(ii) A designated contract market may conduct enterprise technology risk assessments by using independent contractors or employees of the designated contract market who are not responsible for development or operation of the systems or capabilities being assessed.

(i) To the extent practicable, a designated contract market shall:

* * * * *

(k) Scope of testing and assessment. The scope for all system safeguards testing and assessment required by this part shall be broad enough to include the testing of automated systems and controls that the designated contract market'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 designated contract market's operations or with fulfillment of its statutory and regulatory responsibilities;

(ii) Impair or degrade the reliability, security, or adequate scalable capacity of the designated contract market's automated systems;

(iii) Add to, delete, modify, exfiltrate, or compromise the integrity of any data related to the designated contract market's regulated activities; or

(iv) Undertake any other unauthorized action affecting the designated contract market's regulated activities or the hardware or software used in connection with those activities.

(l) Internal reporting and review. Both the senior management and the Board of Directors of a designated contract market shall receive and review reports setting forth the results of the testing and assessment required by this section. A designated contract market shall establish and follow appropriate procedures for the remediation of issues identified through such review, as provided in section 38.1051(m) of this part, and for evaluation of the effectiveness of testing and assessment protocols.

(m) Remediation. A designated contract market shall identify and document the vulnerabilities and deficiencies in its systems revealed by the testing and assessment

required by this section. The designated contract market shall conduct and document an appropriate analysis of the risks presented by such vulnerabilities and deficiencies, to determine and document whether to remediate or accept the associated risk. When the designated contract market determines to remediate a vulnerability or deficiency, it must remediate in a timely manner given the nature and magnitude of the associated risk.

(n) Required production of annual total trading volume.

(i) As used in this section 38.1051(n), annual total trading volume means the total number of all contracts traded on or pursuant to the rules of a designated contract market during a calendar year.

(ii) Each designated contract market shall provide to the Commission for calendar year 2015 and each calendar year thereafter its annual total trading volume, providing this information for 2015 within 30 calendar days of the effective date of the final version of this rule, and for 2016 and subsequent years by January 31 of the following calendar year. For calendar year 2015 and each calendar year thereafter, the Commission shall provide to each designated contract market the percentage of the combined annual total trading volume of all designated contract markets regulated by the Commission which is constituted by that designated contract market's annual total trading volume, providing this information for 2015 within 60 calendar days of the effective date of the final version of this rule, and for 2016 and subsequent years by February 28 of the following calendar year.

* * * * *

Part 49, Section 49.24

Authority: 7 U.S.C. 12a and 24a, as amended by Title VII of the Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376 (2010).

Amend Part 49, Section 49.24 System Safeguards, by removing current § 49.24(b) and adding new § 49.24(b); removing current 49.24(c) and adding new § 49.24(c); amending current § 49.24(d) by adding a sentence at the end of the current section; removing current § 49.24(i) and adding new § 49.24(i); removing current § 49.24(j) and adding new § 49.24(j); revising the introductory text of § 49.24(k); and adding new §§ 49.24(l), 49.24(m), and 49.24(n), to read as follows:

§ 49.24 System Safeguards.

* * * * *

(b) A swap data repository's program of risk analysis and oversight with respect to its operations and automated systems shall address each of the following categories of risk analysis and oversight:

(1) Enterprise risk management and governance. This category includes, but is not limited to: assessment, mitigation, and monitoring of security and technology risk; security and technology capital planning and investment; board of directors and management oversight of technology and security; information technology audit and controls assessments; remediation of deficiencies; and any other elements of enterprise risk management and governance included in generally accepted best practices.

(2) Information security. This category includes, but is 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.

(3) Business continuity-disaster recovery planning and resources. This category includes, but is not limited to: regular, periodic testing and review of business continuity-disaster recovery capabilities, the controls and capabilities described in paragraph (a), (d), (e), (f), and (k) of this section; and any other elements of business continuity-disaster recovery planning and resources included in generally accepted best practices.

(4) Capacity and performance planning. This category includes, but is not limited to: controls for monitoring the swap data repository'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.

(5) Systems operations. This category includes, but is 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.

(6) Systems development and quality assurance. This category includes, but is 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.

(7) Physical security and environmental controls. This category includes, but is 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.

(c) In addressing the categories of risk analysis and oversight required under paragraph (b) of this section, a swap data repository shall follow generally accepted standards and best practices with respect to the development, operation, reliability, security, and capacity of automated systems.

(d) A swap data repository shall maintain a business continuity-disaster recovery plan and business continuity-disaster recovery resources, emergency procedures, and backup facilities sufficient to enable timely recovery and resumption of its operations and resumption of its ongoing fulfillment of its duties and obligations as a swap data repository following any disruption of its operations. Such duties and obligations include, without limitation: the duties set forth in § 49.19, and maintenance of a comprehensive audit trail. The swap data repository's business continuity-disaster recovery plan and resources generally should enable resumption of the swap data repository's operations and resumption of ongoing fulfillment of the swap data repository's duties and obligations during the next business day following the disruption.

A swap data repository shall update its business continuity-disaster recovery plan and emergency procedures at a frequency determined by an appropriate risk analysis, but at a minimum no less frequently than annually.

* * * * *

(i) As part of a swap data repository's obligation to produce books and records in accordance with Commission regulations §§ 1.31, 45.2, and 49.12, a swap data repository shall provide to the Commission the following system safeguards-related books and records, promptly upon the request of any Commission representative:

(i) Current copies of its business continuity-disaster recovery plans and other emergency procedures;

(ii) All assessments of its operational risks or system safeguards-related controls;

(iii) All reports concerning system safeguards testing and assessment required by this chapter, whether performed by independent contractors or by employees of the swap data repository; and

(iv) All other books and records requested by Commission staff 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 swap data repository's automated systems.

(v) Nothing in this § 49.24(i) shall be interpreted as reducing or limiting in any way a swap data repository's obligation to comply with §§ 1.31, 45.2, or 49.12 of the Commission's regulations.

(j) A swap data repository shall conduct regular, periodic, objective testing and review of its automated systems to ensure that they are reliable, secure, and have adequate scalable

capacity. It shall also conduct regular, periodic testing and review of its business continuity-disaster recovery capabilities. Such testing and review shall include, without limitation, all of the types of testing set forth in this paragraph (j).

(1) Definitions. As used in section 49.24(j) of this part:

Controls means the safeguards or countermeasures employed by the swap data repository in order to protect the reliability, security, or capacity of its automated systems or the confidentiality, integrity, and availability of its data and information, and in order to enable the swap data repository to fulfill its statutory and regulatory duties and responsibilities.

Controls testing means assessment of the swap data repository's controls to determine whether such controls are implemented correctly, are operating as intended, and are enabling the swap data repository 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 swap data repository operations or assets, or to market participants, individuals, or other entities, resulting from impairment of the confidentiality, integrity, and availability of data and information or the reliability, security, or capacity of automated systems.

External penetration testing means attempts to penetrate the swap data repository'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 the swap data repository'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.

Security incident means a cyber security 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 swap data repository'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 swap data repository'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 swap data repository'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.

(2) Vulnerability testing. A swap data repository shall conduct vulnerability testing of a scope sufficient to satisfy the requirements set forth in section 49.24(l) of this part.

(i) A swap data repository 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 swap data repository shall conduct vulnerability testing by engaging independent contractors or by using employees of the swap data repository who are not responsible for development or operation of the systems or capabilities being tested.

(3) External penetration testing. A swap data repository shall conduct external penetration testing of a scope sufficient to satisfy the requirements set forth in section 49.24(l) of this part.

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

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

(4) Internal penetration testing. A swap data repository shall conduct internal penetration testing of a scope sufficient to satisfy the requirements set forth in section 49.24(l) of this part.

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

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

(5) Controls testing. A swap data repository shall conduct controls testing of a scope sufficient to satisfy the requirements set forth in section 49.24(l) of this part.

(i) A swap data repository 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. Such testing may be conducted on a rolling basis. A swap data repository shall conduct testing of its key controls no less frequently than every three years. The swap data repository may conduct testing of

its key controls on a rolling basis over the course of three years or the period determined by such risk analysis, whichever is shorter.

(ii) A swap data repository shall engage independent contractors to test and assess the key controls included in its program of risk analysis and oversight no less frequently than every three years. The swap data repository may conduct any other controls testing required by this section by using independent contractors or employees of the swap data repository who are not responsible for development or operation of the systems or capabilities being tested.

(6) Security incident response plan testing. A swap data repository shall conduct security incident response plan testing sufficient to satisfy the requirements set forth in section 49.24(l) of this part.

(i) A swap data repository shall conduct such security incident response plan testing at a frequency determined by an appropriate risk analysis, but no less frequently than annually.

(ii) A swap data repository's security incident response plan shall include, without limitation, the swap data repository'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) A swap data repository 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) A swap data repository may conduct security incident response plan testing by engaging independent contractors or by using employees of the swap data repository.

(7) Enterprise technology risk assessment. A swap data repository shall conduct enterprise technology risk assessment of a scope sufficient to satisfy the requirements set forth in section 49.24(l) of this part.

(i) A swap data repository shall conduct an enterprise technology risk assessment at a frequency determined by an appropriate risk analysis, but no less frequently than annually. A swap data repository that has conducted an enterprise technology risk assessment that complies with this section may conduct subsequent assessments by updating the previous assessment.

(ii) A swap data repository may conduct enterprise technology risk assessments by using independent contractors or employees of the swap data repository who are not responsible for development or operation of the systems or capabilities being assessed.

(k) To the extent practicable, a swap data repository shall:

* * * * *

(l) Scope of testing and assessment. The scope for all system safeguards testing and assessment required by this part shall be broad enough to include the testing of automated systems and controls that the swap data repository'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 swap data repository's operations or with fulfillment of its statutory and regulatory responsibilities;

(ii) Impair or degrade the reliability, security, or adequate scalable capacity of the swap data repository's automated systems;

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

(iv) Undertake any other unauthorized action affecting the swap data repository's regulated activities or the hardware or software used in connection with those activities.

(m) Internal reporting and review. Both the senior management and the Board of Directors of a swap data repository shall receive and review reports setting forth the results of the testing and assessment required by this section. A swap data repository shall establish and follow appropriate procedures for the remediation of issues identified through such review, as provided in section 49.24(n) of this part, and for evaluation of the effectiveness of testing and assessment protocols.

(n) Remediation. A swap data repository shall identify and document the vulnerabilities and deficiencies in its systems revealed by the testing and assessment required by this section. The swap data repository shall conduct and document an appropriate analysis of

the risks presented by such vulnerabilities and deficiencies, to determine and document whether to remediate or accept the associated risk. When the swap data repository determines to remediate a vulnerability or deficiency, it must remediate in a timely manner given the nature and magnitude of the associated risk.

Issued in Washington, DC on September 8, 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 – Commission Voting Summary, Chairman's Statement, and Commissioner's Statement

Appendix 1 – Commission Voting Summary

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

Appendix 2 – Statement of Chairman Timothy G. Massad

I strongly support 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] 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

[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.

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

[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.