FEDERAL REGISTER

Vol. 80 Wednesday,
No. 246 December 23, 2015

Part V

Commodity Futures Trading Commission

17 CFR Part 37, 38 and 49
System Safeguards Testing Requirements; Proposed Rules

COMMODITY FUTURES TRADING COMMISSION

17 CFR Parts 37, 38, and 49

RIN 3038–AE30

System Safeguards Testing Requirements

AGENCY: Commodity Futures Trading Commission.

ACTION: Proposed rulemaking; advanced notice of proposed rulemaking.

SUMMARY: The Commodity Futures Trading Commission (''Commission'' or ''CFTC'') is amending its system safeguards rules for designated contract markets, swap execution facilities, and swap data repositories, by enhancing and clarifying existing provisions relating to system safeguards risk analysis and oversight and cybersecurity testing, and adding new provisions concerning certain aspects of cybersecurity testing. The Commission is clarifying the existing 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, including vulnerability testing, penetration testing, controls testing, security incident response plan testing, and enterprise technology risk assessment. The Commission is also clarifying 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. The new provisions concerning certain aspects of cybersecurity testing, applicable to covered designated markets (as defined) and all swap data repositories, include minimum frequency requirements for conducting the essential types of cybersecurity testing, and requirements for performance of certain tests by independent contractors. In this release, the Commission is also issuing an Advance Notice of Proposed Rulemaking requesting public comment concerning whether the minimum testing frequency and independent contractor testing requirements should be applied, via a future Notice of Proposed Rulemaking, to covered swap execution facilities (to be defined).

DATES: Comments must be received on or before February 22, 2016.

ADDRESSES: You may submit comments, identified by RIN number 3038–AE30, by any of the following methods:

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

Please submit your comments using only one method. All comments must be submitted in English, or must be accompanied by an English translation. Contents will be posted as received to *http://www.cftc.gov*. You should submit only information that you wish to make available publicly. If you wish the Commission to consider information that may be exempt from disclosure under the Freedom of Information Act, a petition for confidential treatment of the exempt information may be submitted according to the established procedures in CFTC Regulation 145.9.

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:

Table of Contents

I. Preamble

A. Background: The Current Cybersecurity Threat Environment and the Need for Cybersecurity Testing

1. Current Cybersecurity Landscape

Cyber threats to the financial sector continue to expand. As the Commission was informed by cybersecurity experts participating in its 2015 Staff Roundtable on Cybersecurity and System Safeguards Testing, these threats have a number of noteworthy aspects.[1]

First, the financial sector faces an escalating volume of cyber attacks. According to the Committee on Payments and Market Infrastructures (''CPMI'') of the Bank for International Settlements (''BIS''), ''Cyber attacks against the financial system are becoming more frequent, more sophisticated and more widespread.'' [2] A survey of 46 global securities exchanges conducted by the International Organization of Securities Commissions (''IOSCO'') and the World Federation of Exchanges (''WFE'') found that as of July 2013, over half of exchanges world-wide had experienced a cyber attack during the previous year.[3] Cybersecurity now ranks as the number

[1] *See generally* CFTC Staff Roundtable on Cybersecurity and System Safeguards Testing (March 18, 2015) (''CFTC Roundtable''), at 11–91, transcript available at *http://www.cftc.gov/ucm/groups/public/@newsroom/documents/file/transcript031815.pdf*. The Commission held the CFTC Roundtable due to its concern about the growing cybersecurity threat discussed in the following paragraphs, and in order to, among other things, discuss the issue and identify critical areas of concern. Similarly, a June 2015 Market Risk Advisory Committee (''MRAC'') meeting focused on cybersecurity. *See generally* MRAC Meeting (June 2, 2015), at 6, transcript available at *http://www.cftc.gov/ucm/groups/public/@aboutcftc/documents/file/mrac_060215_transcript.pdf*.

[2] Committee on Payments and Market Infrastructures of the Bank for International Settlements, *Cyber resilience in financial market infrastructures* (November 2014), at 1, available at *http://www.bis.org/cpmi/publ/d122.pdf*.

[3] IOSCO and WFE, *Cyber-crime, securities markets and systemic risk,* Staff Working Paper (SWP2/2013) (July 16, 2013) (''IOSCO–WFE Staff Report''), at 3, available at *http://www.iosco.org/research/pdf/swp/Cyber-Crime-Securities-Markets-and-Systemic-Risk.pdf*.

one concern for nearly half of financial institutions in the U.S. according to a 2015 study by the Depository Trust & Clearing Corporation (''DTCC'').[4] The annual Price Waterhouse Coopers Global State of Information Security Survey for 2015, which included 9,700 participants, found that the total number of security incidents detected in 2014 increased by 48 percent over 2013, for a total of 42.8 million incoming attacks, the equivalent of more than 117,000 attacks per day, every day.[5] As the PWC Survey pointed out, these numbers do not include undetected attacks. Verizon's 2015 Data Breach Investigations Report noted that during 2014 the financial services sector experienced an average of 350 malware attacks per week.[6]

Second, financial sector entities also face increasing numbers of more dangerous cyber adversaries with expanding and worsening motivations and goals. Until recently, most cyber attacks on financial sector institutions were conducted by criminals whose aim was monetary theft or fraud.[7] As noted at the CFTC Roundtable, while such attacks continue, there has also been a rise in attacks by politically motivated hacktivists or terrorists, and by nation state actors, aimed at disruption of their targets' operations, at theft of data or intellectual property, at extortion, at cyber espionage, at corruption or destruction of data, or at degradation or destruction of automated systems.[8] IOSCO and the WFE note that attacks on securities exchanges now tend to be disruptive in nature, and note that ''[t]his suggests a shift in motive for cyber-crime in securities markets, away from financial gain and towards more destabilizing aims.'' [9]

Third, financial institutions may now encounter increasing cyber threat capabilities. According to a CFTC Roundtable participant, one current trend heightening cyber risk for the financial sector is the emergence of cyber intrusion capability—typically highest when supported by nation state resources—as a key tool of statecraft for most states.[10] Another trend noted by Roundtable participants is an increase in sophistication on the part of most actors in the cyber arena, both in terms of technical capability and of capacity to organize and carry out attacks.[11]

Fourth, the cyber threat environment includes an increase in cyber attack duration.[12] While attacks aimed at monetary theft or fraud tend to manifest themselves quickly, more sophisticated attacks may involve cyber adversaries having a cyber presence inside a target's automated systems for an extended period of time, and avoiding detection.[13] IOSCO and the WFE noted in 2013 that:

> The rise of a relatively new class of cyber-attack is especially troubling. This new class is referred to as an 'Advanced Persistent Threat.' Advanced Persistent Threats (APTs) are usually directed at business and political targets for political ends. APTs involve stealth to persistently infiltrate a system over a long period of time, without the system displaying any unusual symptoms.[14]

Fifth, there is now a broadening cyber threat field. Financial institutions should consider cyber vulnerabilities not only with respect to their desktop computers, but also with respect to mobile devices used by their employees.[15] In some cases, their risk analysis should address not only protecting the integrity of data in their own automated systems, but also protecting data in the cloud.[16] Adequate risk analysis should also address both the vulnerabilities of the entity's automated systems and human vulnerabilities such as those posed by social engineering or by disgruntled or coerced employees.[17] The cyber threat field includes automated systems that are not directly internet-facing, which can be vulnerable to cyber attacks despite their isolation behind firewalls.[18] In practice, there is interconnectivity between internet-facing and corporate information technology (''IT'') and operations technology, since the two can be and often are connected for maintenance purposes or in error.[19] Non-internet-facing systems are also vulnerable to insertion of malware-infected removable media, phishing attacks, and other social engineering techniques, and to supply-chain risk involving both hardware and software.[20]

Finally, financial institutions cannot achieve cyber resilience by addressing threats to themselves alone: They also face threats relating to the increasing interconnectedness of financial services firms.[21] In today's environment, a financial entity's risk assessments should consider cybersecurity across the financial sector, from exchanges and clearinghouses to counterparties and customers, technology providers, other third party service providers, and the businesses and products in the entity's supply chain.[22]

2. Need for Cybersecurity Testing

Cybersecurity testing by designated contract markets (''DCMs''), swap execution facilities (''SEFs''), derivatives clearing organizations (''DCOs''), swap data repositories (''SDRs''), and other entities in the financial sector can harden cyber defenses, mitigate operations, reputation, and financial risk, and maintain cyber resilience and ability to recover from cyber attack.[23] To ensure the effectiveness of cybersecurity controls, a financial sector entity must test in order to find and fix its vulnerabilities before an attacker exploits them. A financial sector entity's testing should assess, on the basis of information with respect to current threats, how the entity's controls and countermeasures stack up against the techniques, tactics, and procedures used by its potential adversaries.[24] Testing should include periodic risk assessments made in light of changing business conditions, the changing threat landscape, and changes to automated systems. It should also include recurring tests of controls and automated system components to verify their effectiveness and operability, as well as continuous monitoring and scanning of system operation and vulnerabilities.[25] Testing should focus on the entity's ability to detect, contain, respond to, and recover from cyber attacks, not just on its perimeter defenses designed to prevent

[4] DTCC, *Systemic Risk Barometer Study* (Q1 2015), at 1, available at *http://dtcc.com/~/media/Files/pdfs/Systemic-Risk-Report-2015-Q1.pdf*.

[5] PricewaterhouseCoopers, *Managing Cyber Risks in an Interconnected World: Key Findings from the Global State of Information Security Survey 2015* (September 30, 2014), at 7, available at *www.pwc.com/gsiss2015* (''PWC Survey'').

[6] *Id.*

[7] CFTC Roundtable, at 41–42.

[8] *See* CFTC Roundtable, at 12, 14–15, 17–24, 42–44, 47.

[9] IOSCO–WFE Staff Report, at 3–4, available at *http://www.iosco.org/research/pdf/swp/Cyber-Crime-Securities-Markets-and-Systemic-Risk.pdf*.

[10] CFTC Roundtable, at 20–21.

[11] *Id.* at 21–22.

[12] *Id.* at 74–76, 81–82.

[13] *Id.*

[14] IOSCO–WFE Staff Report, at 3, available at *http://www.iosco.org/research/pdf/swp/Cyber-Crime-Securities-Markets-and-Systemic-Risk.pdf*.

[15] CFTC Roundtable, at 22–23.

[16] *Id.*

[17] *Id.* at 14, 79–80.

[18] *Id.* at 60–69.

[19] *Id.* at 72–74. As Roundtable panelists also noted, experienced penetration testers are finding that when they are able to penetrate a financial institution, they often are able to move between internet-facing and non-internet-facing systems by harvesting passwords and credentials and exploiting access privileges associated with them. *Id.*

[20] *Id.* at 62–64, 77–79.

[21] *Id.* at 24–25.

[22] *Id.* at 47–55.

[23] *Id.* at 24.

[24] *Id.* at 44.

[25] *Id.* at 46.

intrusions.[26] It should 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, which tend to be the main focus of many best practices.[27] Both internal testing by the entity itself and independent testing by third party service providers are essential components of an adequate testing regime.[28]

Cybersecurity testing is a well-established best practice generally and for financial sector entities. The Federal Information Security Management Act (''FISMA''), which is a source of cybersecurity best practices and also establishes legal requirements for federal government agencies, calls for ''periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually.'' [29] The National Institute of Standards and Technology (''NIST'') Framework for Improving Critical Infrastructure Cybersecurity (''NIST Framework'') calls for testing of cybersecurity response and recovery plans and cybersecurity detection processes and procedures.[30] The Financial Industry Regulatory Authority (''FINRA'') 2015 Report on Cybersecurity Practices notes that ''Risk assessments serve as foundational tools for firms to understand the cybersecurity risks they face across the range of the firm's activities and assets,'' and calls for firms to develop, implement and test cybersecurity incident response plans.[31] FINRA notes that one common deficiency with respect to cybersecurity is ''failure to conduct adequate periodic cybersecurity assessments.'' [32] The critical security controls established by the Council on CyberSecurity (''the Council'') call for entities to ''[c]ontinuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.'' [33] The Council notes that ''[o]rganizations that do not scan for vulnerabilities and proactively address discovered flaws face a significant likelihood of having their computer systems compromised.'' [34] The Council's critical security controls also call for entities to ''test the overall strength of an organization's defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.'' [35] The Council calls for implementation of this control by conducting ''regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully,'' from both outside and inside the boundaries of the organization's network perimeter,[36] and also calls for use of vulnerability scanning and penetration testing in concert.[37]

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

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

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

Cybersecurity testing is also supported internationally. IOSCO has emphasized the importance of testing to ensure effective controls, in light of risks posed by the complexity of markets caused by technological advances.[41] IOSCO has stated that trading venues should ''appropriately monitor critical systems and have appropriate control mechanisms in place.'' [42] The European Securities and Markets Authority (''ESMA'') Guidelines for automated trading systems call for trading platforms to test trading systems and system updates to ensure that the system meets regulatory requirements, that risk management controls work as intended, and that the system can function effectively in stressed market conditions.[43] Further, the Principles for Financial Market Infrastructures (''PFMIs'') published by the Bank for International Settlements' Committee on Payments and Market Infrastructures (''CPMI'') and IOSCO's Technical Committee (together, ''CPMI–IOSCO'') note that with respect to operational risks, which include cyber risk, ''[a financial market infrastructure]'s arrangements with participants, operational policies, and operational procedures should be periodically, and whenever necessary, tested and reviewed, especially after significant changes occur to the system or a major incident occurs. . . .'' [44]

---

[26] *Id.* at 80–84. As one cybersecurity expert has remarked, ''Organizations are too focused on firewalls, spam filters, and other Maginot Line-type defenses that have lost their effectiveness. That's a misguided philosophy. There's no such thing as a perimeter anymore.'' Associated Press, *Cyber theft of personnel info rips hole in espionage defenses* (June 15, 2015), available at *http://bigstory.ap.org/article/93077d547f074bed8ce9eb292a3bbd47/cybertheft-personnel-info-rips-hole-espionage-defenses.*

[27] CFTC Roundtable, at 15–16, 65, 71–73, 80–83.

[28] *Id.* at 87–88.

[29] FISMA section 3544(b)(5), available at *http://csrc.nist.gov/drivers/documents/FISMA-final.pdf.*

[30] 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.*

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

[32] *Id.* at 8.

[33] Council on CyberSecurity, *The Critical Security Controls for Effective Cyber Defense Version 5.1,* Critical Security Control (''CSC'') 4, at 27, available at *http://www.counciloncybersecurity.org/critical-controls/.*

[34] *Id.*

[35] *Id.,* CSC 20, at 102.

[36] *Id.,* CSC 20–1, at 102.

[37] *Id.,* CSC 20–6, at 103.

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

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

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

[41] IOSCO Consultation Report, *Mechanisms for Trading Venues to Effectively Manage Electronic Trading Risks and Plans for Business Continuity* (April 2015) (''IOSCO 2015 Consultation Report''), at 3, available at *http://www.iosco.org/library/pubdocs/pdf/IOSCOPD483.pdf.*

[42] *Id.* at 9.

[43] European Securities and Markets Authority (''ESMA''), *Guidelines: Systems and controls in an automated trading environment for trading platforms, investment firms and competent authorities* (February 24, 2012), at 7, available at *http://www.esma.europa.eu/system/files/esma_2012_122_en.pdf.*

[44] CPMI–IOSCO, *Principles for Financial Market Infrastructures,* (Apr. 2012), at 96, available at

B. 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 each DCM, SEF, and SDR to maintain a program of risk analysis and oversight to identify and minimize sources of operational risk.[45] The Act provides that each such entity must have appropriate controls and procedures for this purpose, and must have automated systems that are reliable, secure, and have adequate scalable capacity.[46] Commission regulations concerning system safeguards for DCMs, SEFs, and SDRs provide that the program of risk analysis and oversight required of each such entity must address specified categories of risk analysis and oversight, and applicable regulations and guidance provide that such entities should follow generally accepted standards and best practices for development, operation, reliability, security, and capacity of automated systems.[47]

Six categories of risk analysis and oversight are specified in the Commission's current regulations for DCMs, SEFs, and SDRs: 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.[48] The current DCM, SEF, and SDR system safeguards regulations address specific requirements concerning BC–DR, but do not provide any further guidance respecting the other five required categories.[49] In this Notice of Proposed Rulemaking (''NPRM''), the Commission proposes to clarify what is already required of all DCMs, SEFs, and SDRs regarding the other five specified categories, by defining each of them. The proposed definitions are grounded in generally accepted best practices regarding appropriate risk analysis and oversight with respect to system safeguards, which all DCMs, SEFs, and SDRs should follow as provided in the current regulations. As the proposed definitions explicitly state, they are not intended to be all-inclusive; rather, they highlight important aspects of the required risk analysis and oversight categories.

The Commission is also proposing to add and define another enumerated category, enterprise risk management and governance, to the list of required categories of system safeguards-related risk analysis and oversight. As explained below, generally accepted best practices regarding appropriate risk analysis and oversight with respect to system safeguards—which form the basis for the proposed definition of this added category—also establish enterprise risk management and governance as an important category of system safeguards-related risk analysis and oversight. This category is therefore implicit in the Commission's existing system safeguard regulations, which already require each DCM, SEF, and SDR to maintain a program of risk analysis and oversight with respect to system safeguards.[50] The proposed rule would make it an explicitly listed category for the sake of clarity. As with the other proposed category definitions, the definition of the proposed additional category of enterprise risk management and governance clarifies what is already required and will continue to be required of all DCMs, SEFs, and SDRs with regard to their system safeguards-related risk analysis and oversight programs under the existing rules. As such, addition of this category does not impose additional obligations on such entities. The Commission sets forth below the best practices surrounding enterprise risk management and governance. In connection with its further definition of five of the other six categories of risk analysis and oversight already enumerated in the existing regulations, the Commission will also cite some examples of the best practices underlying those categories.

1. Enterprise Risk Management and Governance

As stated in the proposed rules, this category of risk analysis and oversight includes the following five areas:

- Assessment, mitigation, and monitoring of security and technology risk.
- Capital planning and investment with respect to security and technology.
- Board of directors and management oversight of system safeguards.
- Information technology audit and controls assessments.
- Remediation of deficiencies.

The category also includes any other enterprise risk management and governance elements included in generally accepted best practices. As noted above, this category of risk analysis and oversight is already implicit in the Commission's existing system safeguards rules for all DCMs, SEFs, and SDRs, as an essential part of an adequate program of risk analysis and oversight according to generally accepted standards and best practices. The Commission sets out below the best practices basis for its proposed definition of this category, which like the other proposed definitions is provided for purposes of clarity.

a. Assessment, Mitigation, and Monitoring of Security and Technology Risk

In the area of assessment, mitigation, and monitoring of security and technology risk, NIST calls for organizations to develop appropriate and documented risk assessment policies, to make effective risk assessments, and to develop and implement a comprehensive risk management strategy relating to the operation and use of information systems.[51] NIST notes that risk assessment is a fundamental component of an organization's risk management process, which should include framing, assessing, responding to, and monitoring risks associated with operation of information systems or with any compromise of data confidentiality, integrity, or availability.[52] According to NIST:

> Leaders must recognize that explicit, well-informed risk-based decisions are necessary in order to balance the benefits gained from the operation and use of these information systems with the risk of the same systems being vehicles through which purposeful attacks, environmental disruptions, or human errors cause mission or business failure.[53]

NIST standards further provide that an organization's risk management strategy regarding system safeguards

http://www.iosco.org/library/pubdocs/pdf/IOSCOPD377.pdf. See also CPMI, *Cyber resilience in financial market infrastructures,* (Nov. 2014), available at *http://www.bis.org/cpmi/publ/d122.pdf.*

[45] 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).

[46] *Id.*

[47] 17 CFR 38.1051(a) and (b); 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; 17 CFR 49.24(b) and (c).

[48] *See* 17 CFR 38.1051(a); 17 CFR 37.1401(a); and 17 CFR 49.24(b).

[49] *See* 17 CFR 38.1051(c) and 38.1051(i) (for DCMs); 17 CFR 37.1401(b) and Appendix A to Part 37, Core Principle 14 of Section 5h of the Act—System Safeguards (a) Guidance (3) Coordination (for SEFs); 17 CFR 49.24(d) and 49.24(k) (for SDRs).

[50] 17 CFR 38.1050(a) (for DCMs); 17 CFR 37.1400(a) (for SEFs); 17 CFR 49.24(a)(1) (for SDRs).

[51] *See* NIST Special Publication (''SP'') 800–53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations Controls* (''NIST SP 800–53 Rev. 4''), RA–1, RA–2, and RA–3, available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.*

[52] 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.*

[53] *Id.* at 1.

should include risk mitigation strategies, processes for evaluating risk across the organization, and approaches for monitoring risk over time.[54] ISACA's Control Objectives for Information and Related Technology (''COBIT'') 5 calls for organizations to continually identify, assess, and reduce IT-related risk in light of levels of system safeguards risk tolerance set by the organization's executive management.[55] As part of such assessment, COBIT 5 calls for maintaining an updated risk profile that includes known risks and risk attributes as well as an inventory of the organization's related resources, capabilities, and controls.[56]

b. Capital Planning and Investment Respecting Security and Technology

Security and technology capital planning and investment are also recognized as best practices for enterprise risk management and governance. NIST standards call for entities to determine, as part of their capital planning and investment control process, both the information security requirements of their information systems and the resources required to protect those systems.[57] NIST standards further provide that entities should ensure that their capital planning and investment includes the resources needed to implement their information security programs, and should document all exceptions to this requirement.[58] ISACA's COBIT 5 also addresses capital planning, budgeting, and investment with respect to information technology and system safeguards.[59]

c. Board of Directors and Management Oversight of System Safeguards

Board of directors and management oversight of system safeguards is another recognized best practice for enterprise risk management and governance. NIST defines requirements for board of directors and management oversight of cybersecurity.[60] The FFIEC calls for financial sector organizations to review the system safeguards-related credentials of the board of directors or the board committee responsible for oversight of technology and security, and to determine whether the directors responsible for such oversight have the appropriate level of experience and knowledge of information technology and related risks to enable them to provide adequate oversight.[61] If directors lack the needed level of experience and knowledge, the FFIEC calls for the organization to consider bringing in outside independent consultants to support board oversight.[62] ISACA's COBIT 5 calls for entities to maintain effective governance of the enterprise's IT mission and vision, and to maintain mechanisms and authorities for managing the enterprise's use of IT in support of its governance objectives, in light of the criticality of IT to its enterprise strategy and its level of operational dependence on IT.[63] In a three-lines-of-defense model for cybersecurity, the important third line of defense consists of having an independent audit function report to the board of directors concerning independent tests, conducted with sufficient frequency and depth, that determine whether the organization has appropriate and adequate cybersecurity controls in place which function as they should.[64]

d. Information Technology Audit and Controls Assessment

Information technology audit and controls assessments are an additional major aspect of best practices regarding enterprise risk management and governance. As the FFIEC has stated:

> A well-planned, properly structured audit program is essential to evaluate risk management practices, internal control systems, and compliance with corporate policies concerning IT-related risks at institutions of every size and complexity. Effective audit programs are risk-focused, promote sound IT controls, ensure the timely resolution of audit deficiencies, and inform the board of directors of the effectiveness of risk management practices.[65]

The FFIEC has also noted that today's rapid rate of change with respect to information technology and cybersecurity make IT audits essential to the effectiveness of an overall audit program.[66] Further:

> The audit program should address IT risk exposures throughout the institution, including the areas of IT management and strategic planning, data center operations, client/server architecture, local and wide-area networks, telecommunications, physical and information security . . . systems development, and business continuity planning. IT audit should also focus on how management determines the risk exposure from its operations and controls or mitigates that risk.[67]

e. Remediation of Deficiencies

Finally, remediation of deficiencies is another important part of enterprise risk management and governance best practices. NIST calls for organizations to ensure that plans of action and milestones for IT systems and security are developed, maintained, and documented, and for organizations to review such plans for consistency with organization-wide risk management strategy and priorities for risk response actions.[68] As noted above, ISACA's COBIT 5 establishes best practices calling for entities to reduce IT-related risk within levels of tolerance set by enterprise executive management.[69] The FFIEC calls for management to take appropriate and timely action to address identified IT problems and weaknesses, and to report such actions to the board of directors.[70] FFIEC further calls for the internal audit function to determine whether management sufficiently corrects the root causes of all significant system safeguards deficiencies.[71]

2. Information Security

As stated in the proposed rules, this category of risk analysis and oversight includes, without limitation, controls relating to each of the following:

---

[54] NIST SP 800–53 Rev. 4, control PM–9 *Risk Management Strategy,* available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.*

[55] ISACA, *Control Objectives for Information and Related Technology (''COBIT'') 5,* Align, Plan and Organize (''APO'') APO12, available at *https://cobitonline.isaca.org/.*

[56] *Id.* at APO12.03.

[57] NIST 800–53 Rev. 4, SA–2, *Allocation of Resources,* available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.*

[58] *Id.* at PM–3, *Information Security Resources.*

[59] COBIT 5, APO06, available at *https://cobitonline.isaca.org/.*

[60] *See, e.g.,* NIST 800–53 Rev. 4, Program Management Controls PM–1, *Information Security Program Plan,* PM–2, *Senior Information Security Officer,* and PM 9, *Risk Management Strategy,* available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.*

[61] FFIEC, *Audit IT Examination Handbook,* Objective 3, at A–2, available at *http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_Audit.pdf.*

[62] *Id.*

[63] COBIT 5, APO01, available at *https://cobitonline.isaca.org/.*

[64] CFTC Roundtable, at 242–243. In addition, boards of directors can now face litigation alleging breach of fiduciary duty based on failure to monitor cybersecurity risk and ensure maintenance of proper cybersecurity controls. *See, e.g., Kulla* v. *Steinhafel,* D. Minn. No. 14–CV–00203, (U.S. Dist. 2014) (shareholder derivative suit against Target board of directors), and *Palkon* v. *Holmes,* D. NJ No. 2:14–CV–01234 (U.S. Dist. 2014) (shareholder derivative suit against Wyndham Worldwide Corporation board members).

[65] FFIEC, *Audit IT Examination Handbook,* at 1, available at *http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_Audit.pdf.*

[66] *Id.*

[67] *Id.*

[68] NIST 800–53 Rev. 4, control PM–4, *Plan of Action and Milestones Process,* available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.*

[69] COBIT 5, APO12, available at *https://cobitonline.isaca.org/.*

[70] FFIEC, *Audit IT Examination Handbook,* Objective 6, at A–4, available at *http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_Audit.pdf.*

[71] *Id.*

- Access to systems and data (*e.g.,* least privilege, separation of duties, account monitoring and control).[72]
- User and device identification and authentication.[73]
- Security awareness training.[74]
- Audit log maintenance, monitoring, and analysis.[75]
- Media protection.[76]
- Personnel security and screening.[77]
- Automated system and communications protection (*e.g.,* malware defenses, software integrity monitoring).[78]
- Automated system and information integrity (*e.g.,* network port control, boundary defenses, encryption).[79]
- Vulnerability management.[80]
- Penetration testing.[81]
- Security incident response and management.[82]

The category also includes any other elements of information security included in generally accepted best practices. All of these important aspects of information security are grounded in generally accepted standards and best practices, such as the examples cited in the footnotes for each aspect given above. The Commission believes that information security programs that address each of these aspects continue to be essential to maintaining effective system safeguards in today's cybersecurity threat environment.

3. Business Continuity-Disaster Recovery Planning and Resources

The Commission's current system safeguards regulations for DCMs, SEFs, and SDRs already contain detailed description of various aspects of this category of risk analysis and oversight. The regulations require DCMs, SEFs, and SDRs to maintain a BC–DR plan and BC–DR resources, emergency procedures, and backup facilities sufficient to enable timely resumption of the DCM's, SEF's, or SDR's operations, and resumption of its fulfillment of its responsibilities and obligations as a CFTC registrant following any such disruption.[83] In this connection, the regulations address applicable recovery time objectives for resumption of operations.[84] The regulations also require regular, periodic, objective testing and review of DCM, SEF, and SDR BC–DR capabilities.[85] Applicable regulations and guidance provide that the DCM, SEF, or SDR, to the extent practicable, should coordinate its BC–DR plan with those of other relevant parties as specified, initiate and coordinate periodic, synchronized testing of such coordinated plans.[86] They further provide that the DCM, SEF, or SDR should ensure that its BC–DR plan takes into account the BC–DR plans of its telecommunications, power, water, and other essential service providers.[87] In addition, the regulations and guidance call for DCMs, SEFs, and SDRs to follow generally accepted best practices and standards with respect to BC–DR planning and resources, as similarly provided for the other specified categories of system safeguards risk analysis and oversight.[88]

Because the current system safeguards regulations already address these various aspects of the category of BC–DR planning and resources, the Commission is not proposing to further define this category at this time. The Commission notes that participants in the CFTC Roundtable discussed whether BC–DR planning and testing is at an inflection point: while such planning and testing has traditionally focused on kinetic events such as storms or physical attacks by terrorists, today cybersecurity threats may also result in loss of data integrity or long-term cyber intrusion. Future development of different types of BC–DR testing focused on cyber resiliency, and of new standards for recovery and resumption of operations may be warranted.[89]

4. Capacity and Performance Planning

As provided in the proposed rule, this category of risk analysis and oversight includes (without limitation): Controls for monitoring DCM, SEF, or SDR systems to ensure adequate scalable capacity (*e.g.,* testing, monitoring, and analysis of current and projected future capacity and performance, and of possible capacity degradation due to planned automated system changes);[90] and any other elements of capacity and performance planning included in generally accepted best practices. All of these important aspects of capacity and performance planning are grounded in generally accepted standards and best practices, such as the examples cited in the footnote above. The Commission believes that capacity and performance planning programs that address these aspects are essential to maintaining

[72] NIST SP 800–53 Rev. 4, *Access Controls (''AC'') control family,* available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf;* Council on CyberSecurity, CSC 7, 12, 15, available at *http://www.counciloncybersecurity.org/critical-controls/.*

[73] NIST SP 800–53 Rev. 4, *Identification and Authentication (''IA'') control family,* available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf;* Council on CyberSecurity, CSC 1, 2, available at *http://www.counciloncybersecurity.org/critical-controls/.*

[74] NIST SP 800–53 Rev. 4, *Awareness and Training (''AT'') control family,* available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf;* Council on CyberSecurity, CSC 9, available at *http://www.counciloncybersecurity.org/critical-controls/.*

[75] NIST SP 800–53 Rev. 4, *Audit and Accountability (''AU'') control family,* available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf;* Council on CyberSecurity, CSC 14, available at *http://www.counciloncybersecurity.org/critical-controls/.*

[76] NIST SP 800–53 Rev. 4, *Media Protection (''MP'') control family,* available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.*

[77] NIST SP 800–53 Rev. 4, *Personnel Security (''PS'') control family,* available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.*

[78] NIST SP 800–53 Rev. 4, *System and Communication Protection (''SC'') control family,* available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf;* Council on CyberSecurity, CSC 7, 10, 11, 13, available at *http://www.counciloncybersecurity.org/critical-controls/.*

[79] NIST SP 800–53 Rev. 4, *System and Information Integrity (''SI'') control family,* available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf;* Council on CyberSecurity, CSC 3, 5, 17, available at *http://www.counciloncybersecurity.org/critical-controls/.*

[80] NIST SP 800–53 Rev. 4, control *RA–5,* available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf;* Council on CyberSecurity, CSC 4, 5, available at *http://www.counciloncybersecurity.org/critical-controls/.*

[81] NIST SP 800–53 Rev. 4, control *CA–8,* available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf;* Council on CyberSecurity, CSC 20, available at *http://www.counciloncybersecurity.org/critical-controls/.*

[82] NIST SP 800–53 Rev. 4, *Incident Response (''IR'') control family,* available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf;* NIST SP 800–61 Rev. 2, *Computer Security Incident Handling Guide* (''NIST SP 800–61 Rev. 2''), available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.*

[83] 17 CFR 38.1051(c) (for DCMs); 17 CFR 37.1401(b) (for SEFs); 17 CFR 49.24(a)(2) (for SDRs).

[84] 17 CFR 38.1051(c) and (d) (for DCMs); 17 CFR 37.1401(b) and (c) (for SEFs); 17 CFR 49.24(d), (e), and (f) (for SDRs).

[85] 17 CFR 38.1051(h) (for DCMs); 17 CFR 37.1401(g) (for SEFs); 17 CFR 49.24(j) (for SDRs).

[86] 17 CFR 38.1051(i)(1) and (2) (for DCMs); Appendix A to Part 37, Core Principle 14 of Section 5h of the Act—System Safeguards (a) Guidance (3)(i) and (ii) (for SEFs); 17 CFR 49.24(k)(1) and (2) (for SDRs).

[87] 17 CFR 38.1051(i)(3) (for DCMs); Appendix A to Part 37, Core Principle 14 of Section 5h of the Act—System Safeguards (a) Guidance (3)(iii) (for SEFs); 17 CFR 49.24(k)(3) (for SDRs).

[88] 17 CFR 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); 17 CFR 49.24(c) (for SDRs). For such best practices, *see generally, e.g.,* NIST SP 800–34 Rev. 1, *Contingency Planning Guide for Federal Information Systems,* available at *http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf.*

[89] CFTC Roundtable, at 277–363.

[90] ISACA, *COBIT 5,* Build, Acquire and Implement (''BAI'') BAI04, available at *https://cobitonline.isaca.org/*; FFIEC, *Operations IT Examination Handbook,* at 33–34, 35, 40–41, available at *http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_Operations.pdf.*

effective system safeguards in today's cybersecurity threat environment.

5. Systems Operations

As set out in the proposed rule, this category of risk analysis and oversight includes (without limitation) each of the following elements:

- System maintenance.[91]
- Configuration management (*e.g.,* baseline configuration, configuration change and patch management, least functionality, inventory of authorized and unauthorized devices and software).[92]
- Event and problem response and management.[93]

It also includes any other elements of system operations included in generally accepted best practices. All of these important aspects of systems operations are grounded in generally accepted standards and best practices, for example those cited in the footnotes for each aspect given above. The Commission believes that systems operations programs that address each of these aspects are essential to maintaining effective system safeguards in today's cybersecurity threat environment.

6. Systems Development and Quality Assurance

As set out in the proposed rule, this category of risk analysis and oversight includes (without limitation) each of the following elements:

- Requirements development.[94]
- Pre-production and regression testing.[95]
- Change management procedures and approvals.[96]
- Outsourcing and vendor management.[97]
- Training in secure coding practices.[98]

It also includes any other elements of systems development and quality assurance included in generally accepted best practices. All of these important aspects of systems development and quality assurance are grounded in generally accepted standards and best practices, such as the examples cited in the footnotes for each aspect given above. The Commission believes that systems development and quality assurance programs that address each of these aspects are essential to maintaining effective system safeguards in today's cybersecurity threat environment.

7. Physical Security and Environmental Controls.

As stated in the proposed rule, this category of risk analysis and oversight includes (without limitation) each of the following elements: [99]

- Physical access and monitoring.
- Power, telecommunication, environmental controls.
- Fire protection.

It also includes any other elements of physical security and environmental controls included in generally accepted best practices. All of these important aspects of physical security and environmental controls are grounded in generally accepted standards and best practices, such as the examples cited in the footnote given above. The Commission believes that physical security and environmental controls programs that address each of these aspects are essential to maintaining effective system safeguards in today's cybersecurity threat environment.

C. 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 risk analysis and oversight are required to include.[100] 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).[101] They further provide that such entities should coordinate their BC–DR plans with the BC–DR plans of market participants and essential service providers.[102]

In this NPRM, the Commission is proposing to make these three provisions mandatory for all DCMs, SEFs, and SDRs. The proposed rule provisions reflect this at appropriate points.[103] Making these provisions 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. The Commission believes that in today's cybersecurity threat environment (discussed above), following generally accepted standards and best practices, ensuring tester independence, and coordinating BC–DR plans appropriately are essential to adequate system safeguards and cyber resiliency for DCMs, SEFs, and SDRs, as well as for DCOs. For this reason, the Commission believes that making these provisions mandatory will benefit DCMs, SEFs, and SDRs, their market participants and customers, and the public interest. The Commission

---

[91] NIST SP 800–53 Rev. 4, *Maintenance (''MA'') control family,* available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.*

[92] NIST SP 800–53 Rev. 4, *Configuration Management (''CM'') control family,* available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf;* Council on CyberSecurity, CSC 1, 2, 3, 10, 11, 12, available at *http://www.counciloncybersecurity.org/critical-controls/.*

[93] FFIEC, *Operations IT Examination Handbook,* at 28, and Objective 10, at A–8 to A–9, available at *http://ithandbook.ffiec.gov/ITBooklets/FFIEC_IT Booklet_Operations.pdf;* ISACA, *COBIT 5,* Deliver, Service and Support (''DSS'') process DSS03, available at *https://cobitonline.isaca.org/.*

[94] NIST SP 800–53 Rev. 4, control SA–4, available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf;* FFIEC Development and Acquisition IT Examination Handbook, at 2–3, available at *http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_DevelopmentandAcquisition.pdf.*

[95] NIST SP 800–53 Rev. 4, controls SA–8, SA–10, SA–11, available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf;* NIST SP 800–64 Rev. 2, *Security Considerations in the System Development Life Cycle* (''NIST SP 800–64 Rev. 2''), at 26–27, available at *http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf;* FFIEC, *Development and Acquisition IT Examination Handbook,* at 8–9, and Objective 9, at A–6 to A–7, available at *http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_Developmentand Acquisition.pdf.*

[96] *Id.* at 47–48.

[97] NIST SP 800–53 Rev. 4, controls SA–9, SA–12, available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf;* FFIEC, *Outsourcing Technology Services IT Examination Handbook,* at 2, available at *http://ithandbook.ffiec.gov/ITBooklets/F FIEC_ITBooklet_Outsourcing TechnologyServices.pdf.*

[98] NIST SP 800–53 Rev. 4, controls AT–3, SA–11, available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.*

[99] 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.*

[100] *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).

[101] *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).

[102] 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).

[103] Regarding following best practices, *see* proposed rule § 38.1051(b) (for DCMs); § 37.1401(b) (for SEFs); and § 49.24(c) (for SDRs). Regarding tester independence, *see* proposed rules §§ 38.1051(h)(2)(iv), (3)(i)(C), (3)(ii)(B), (4)(iii), (5)(iv), and (6)(ii) (for DCMs); §§ 37.1401(h)(2)(i), (3)(i)(A), (4)(i), (5)(iii), and (6)(i) (for SEFs); and §§ 49.24(j)(2)(iii), (3)(i)(B), (4)(ii), (5)(iv), and (6)(ii) (for SDRs). Regarding BC–DR plan and plan testing coordination, *see* proposed rule § 38.1051(i) (for DCMs); § 37.1401(i) (for SEFs); and § 49.24(k) (for SDRs).

understands that most DCMs, SEFs, and SDRs have been following the provisions of the current regulations and guidance in these respects, and thus already meet these proposed requirements.

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

The Commission is proposing amendment of the current system safeguards rules requiring 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 updated as frequently as required by appropriate risk analysis, but at a minimum at least annually. Updating such plans and procedures at least annually is a best practice. 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.'' [104] NIST also states that information systems contingency plans (''ISCPs'') ''should be reviewed for accuracy and completeness at least annually, as well as upon significant changes to any element of the ISCP, system, mission/business processes supported by the system, or resources used for recovery procedures.'' [105]

As noted previously, current Commission system safeguards regulations and guidance provide that all DCMs, SEFs, and SDRs should follow best practices in their required programs of risk analysis and oversight. The Commission understands that many DCMs, SEFs, and SDRs currently update their BC–DR plans and emergency procedures at least annually. In light of these facts, the Commission believes that the proposed requirement for updating such plans and procedures as often as indicated by appropriate risk analysis, and at a minimum at least annually, may not impose substantial additional burdens or costs on DCMs, SEFs, or SDRs.

E. 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.[106] The proposed rule includes a provision amending these document production provisions, to further clarify requirements for document production by all DCMs, SEFs, and SDRs relating to system safeguards. The proposed provision would require each DCM, SEF, and SDR to provide to the Commission, promptly on the request of Commission staff: Current copies of its BC–DR plans and other emergency procedures, updated at a frequency determined by appropriate risk analysis but at a minimum no less than annually; all assessments of its operational risks or system safeguards-related controls; all reports concerning system safeguards testing and assessment required by the Act or Commission regulations; and all other documents requested by Commission staff in connection with Commission oversight of system safeguards.

As noted in the text of the proposed rule, production of all such books and records is already required by the Act and Commission regulations, notably by Commission regulation § 1.31.[107] No additional cost or burden is created by this provision. This section is included in the proposed rule solely to provide additional clarity to DCMs, SEFs, and SDRs concerning their statutory and regulatory obligation to produce all such system safeguards-related documents promptly upon request by Commission staff.

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

1. Clarification of Existing Testing Requirements for All DCMs, SEFs, and SDRs

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.[108] 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.[109]

The Commission's existing 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.[110] In this NPRM, as discussed in detail below, the Commission proposes to clarify this system safeguards and cybersecurity testing requirement, by specifying and defining five types of system safeguards testing that a DCM, SEF, or SDR necessarily must perform to fulfill the requirement. The Commission believes, as the generally accepted standards and best practices noted in this NPRM make clear, that it would be essentially impossible for a DCM, SEF, or SDR to fulfill its existing 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 proposed rule. Each of these types of testing is a generally recognized best practice for system safeguards.[111] For these reasons, the

[104] NIST SP 800–61 Rev. 2, at 8, available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.*

[105] NIST SP 800–34 Rev. 1, at 8, available at *http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf.*

[106] 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).

[107] 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).

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

[109] *Id.*

[110] 17 CFR 38.1051(h) (for DCMs); 17 CFR 37.1401(g) (for SEFs); 17 CFR 49.24(j) (for SDRs).

[111] The Commission's existing 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,

Continued

provisions of the proposed rule calling for each DCM, SEF, and SDR to conduct each of these types of testing and assessment clarify the testing requirements of the existing system safeguards rules for DCMs, SEFs, and SDRs; they do not impose new requirements. Providing this clarification of the testing provisions of the existing system safeguards rules is a primary purpose of this proposed rule.

The Commission's clarification of existing testing requirements for DCMs, SEFs, and SDRs by specifying and defining five types of cybersecurity testing essential to fulfilling those testing requirements is designed to set out high-level, minimum requirements for these types of testing, with the expectation 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. This parallels the inclusion in the Commission's existing system safeguards rules and guidance for DCMs, SEFs, and SDRs of provisions that call for those entities to follow generally accepted standards and best practices in their programs of risk analysis and oversight with respect to system safeguards. Those similarly high-level provisions were also designed to allow DCMs, SEFs, and SDRs flexibility in adapting their programs to current industry best practices, which the Commission recognized and continues to recognize will evolve over time.

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

In this NPRM, as discussed in detail below, the Commission is also proposing that covered DCMs (as defined) and all SDRs would be subject to new minimum testing frequency requirements with respect to each type of system safeguards testing included in the clarification of the system safeguards testing requirement in the Commission's existing system safeguards rules. To strengthen the objectivity and reliability of the testing, assessment, and information available to the Commission regarding covered DCM and SDR system safeguards, the Commission is also proposing that for certain types of testing, covered DCMs and SDRs would be subject to new independent contractor testing requirements. The Commission believes that in light of the current cyber threat environment described above, the minimum frequency requirements being proposed are necessary and appropriate, and will give additional clarity concerning what is required in this respect. As discussed above, and discussed in detail below, the proposed minimum frequency requirements are all grounded in generally accepted standards and best practices.[112] Best practices also call for testing by both entity employees and independent contractors as a necessary means of ensuring the effectiveness of cybersecurity testing and of the entity's program of risk analysis and oversight.[113]

The Commission believes that the minimum testing frequency and independent contractor testing requirements in the proposed rule should be applied 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, as well as to all SDRs. 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. As a matter of policy, the Commission believes it is appropriate to reduce possible costs and burdens for smaller entities when it is possible to do so consistent with achieving the fundamental goals of the Act and Commission rules. Accordingly, the Commission believes that applying the minimum frequency and independent contractor requirements in this proposed rule only to DCMs whose annual volume is five percent or more of the total annual volume of all regulated DCMs, and to SDRs, would be appropriate, in light of the fact that smaller DCMs will still be required to conduct testing of all the types clarified in the proposed rule as essential to fulfilling the testing requirements of the existing DCM system safeguards rules.[114]

To give effect to this concept, the proposed rule would make this five percent volume threshold the basis for its definition of a ''covered designated contract market,'' and would require all DCMs to report their annual total trading volume to the Commission each year, as discussed below in section H. The proposed rule defines ''annual total trading volume'' as the total number of all contracts traded on or pursuant to the rules of a designated contract market. Under the proposed rule, a DCM would become a covered DCM, and thus become subject to the proposed testing frequency and independent contractor testing requirements, if it meets the five percent volume threshold with respect to calendar year 2015 or any calendar year thereafter.

It is possible that a DCM which has previously become a covered DCM subject to these requirements by meeting the five percent volume threshold could cease to meet the definition of a covered DCM if its annual total trading volume later fell below the five percent volume threshold. The proposed rule's frequency requirements for controls testing and for independent contractor testing of key controls specify that such testing must be performed no less frequently than every two years, the longest minimum frequency requirement included in the proposed rule. The Commission believes that a DCM which has become a covered DCM should complete an entire cycle of the testing required of covered DCMs before it ceases to be subject to those requirements by virtue of its annual total trading volume falling below the five percent threshold. Accordingly, the proposed rule's definition of ''covered designated contract market'' also specifies that such a DCM would cease to be a covered DCM when it has fallen below the five percent volume threshold for two consecutive years.

3. Vulnerability Testing

a. Need for Vulnerability Testing

Testing to identify cyber and automated system vulnerabilities is a significant component of a DCM's, SEF's, or SDR's program of risk analysis

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*.

[112] *See* discussion above concerning the need for cybersecurity testing.

[113] *Id.*

[114] These considerations do not apply to SDRs. Each SDR contains reported swap data that constitutes a unique part of the total picture of the entire swap market that the Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. 111–203, 124 Stat. 1376 (2010) (''Dodd-Frank Act'') requires the Commission to have. Therefore, the highest level of system safeguards protection must be required for all SDRs. The Commission also notes that, because the Commission is proposing a parallel cybersecurity testing rule that would cover all DCOs, a non-covered DCM that shares common ownership and automated systems with a DCO would in practice fulfill the testing frequency and independent contractor testing requirements proposed for covered DCMs, by virtue of sharing automated systems and system safeguards with the DCO.

and oversight to identify and minimize sources of operational risk, and a necessary prerequisite for remediating vulnerabilities, minimizing exposure to attackers, and enhancing automated system resilience in the face of cyber threats. The Council on Cybersecurity explains the need for ongoing vulnerability testing as follows:

> Cyber defenders must operate in a constant stream of new information: Software updates, patches, security advisories, threat bulletins, etc. Understanding and managing vulnerabilities has become a continuous activity, requiring significant time, attention, and resources.
>
> Attackers have access to the same information, and can take advantage of gaps between the appearance of new knowledge and remediation. For example, when new vulnerabilities are reported by researchers, a race starts among all parties, including: Attackers (to ''weaponize'', deploy an attack, exploit); vendors (to develop, deploy patches or signatures and updates), and defenders (to assess risk, regression-test patches, install).
>
> *Organizations that do not scan for vulnerabilities and proactively address discovered flaws face a significant likelihood of having their computer systems compromised.* Defenders face particular challenges in scaling remediation across an entire enterprise, and prioritizing actions with conflicting priorities, and sometimes-uncertain side effects.[115]

Vulnerability testing is essential to cyber resilience.[116] CFTC Roundtable participants noted that for a financial sector institution, vulnerability testing will scan and assess the security controls of the entity's automated systems, on an ongoing basis, to ensure that they are in place and operating properly.[117] In the automated system context, such testing will include ongoing review that includes automated scanning, to ensure that timely software updates and patches have been made for operating systems and applications, that network components are configured properly, and that no known vulnerabilities are present in operating systems and application software.[118]

b. Best Practices Call for Vulnerability Testing

Conducting ongoing vulnerability testing, including automated scanning, is a best practice with respect to cybersecurity. NIST standards call for organizations to scan for automated system vulnerabilities both on a regular and ongoing basis and when new vulnerabilities potentially affecting their systems are identified and reported.[119] NIST adds that organizations should employ vulnerability scanning tools and techniques that automate parts of the vulnerability management process, with respect to enumerating platforms, software flaws, and improper configurations; formatting checklists and test procedures, and measuring vulnerability impacts.[120] NIST states that vulnerability scans should address, for example: Patch levels; functions, ports, protocols, and services that should not be accessible to users or devices; and improperly configured or incorrectly operating information flow controls.[121] NIST also calls for the organization to remediate vulnerabilities identified by vulnerability testing, in accordance with its assessments of risk.[122]

The Council on CyberSecurity's Critical Security Controls call for organizations to ''continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.'' [123] The Council states that organizations should use vulnerability scanning tools that look for both code-based and configuration-based vulnerabilities, run automated vulnerability scans against all systems on the network at a minimum on a weekly basis, and deliver to management prioritized lists of the most critical vulnerabilities found.[124]

The Data Security Standards (''DSS'') of the Payment Card Industry (''PCI'') Security Standards Council note that ''[v]ulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software,'' and accordingly provide that ''[s]ystem components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.'' [125] These standards call for running internal and external network vulnerability scans both regularly and after any significant change in the network.[126]

c. Proposed Vulnerability Testing Definitions and Related Provisions

The Commission is proposing to clarify the existing testing requirements for all DCMs, all SEFs, and all SDRs by specifying vulnerability testing as an essential means of fulfilling those requirements, and defining it 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. This definition is consistent with NIST standards for such testing.[127] For purposes of this definition, the term ''reconnaissance analysis'' is used to combine various aspects of vulnerability testing.[128] The proposed definition deliberately refers broadly to vulnerability testing in order to avoid prescribing use of any particular technology or tools, because vulnerability assessments may not always be automated, and technology may change.[129]

The proposed rule would require that vulnerability testing include automated vulnerability scanning, as well as an analysis of the test results to identify and prioritize all vulnerabilities that require remediation.[130] Best practices

---

[115] Council on Cybersecurity, CSC 4, *Continuous Vulnerability Assessment and Remediation: Why Is This Control Critical?* (emphasis added), available at *http://www.counciloncybersecurity.org/critical-controls/*.

[116] CFTC Roundtable, at 95–96.

[117] *Id.*

[118] *Id.*

[119] NIST SP 800–53 Rev. 4, control RA–5 *Vulnerability Scanning,* available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf*.

[120] *Id.*

[121] *Id.*

[122] *Id.*

[123] Council on Cybersecurity, CSC 4, *Continuous Vulnerability Assessment and Remediation,* available at *http://www.counciloncybersecurity.org/critical-controls/*.

[124] *Id.* at CSC 4–1.

[125] Security Standards Council, *Payment Card Industry Data Security Standards* (v.3.1, 2015) (''PCI DSS''), *Requirement 11: Regularly test security systems and processes,* available at *https://www.pcisecuritystandards.org/security_standards/index.php*.

[126] *Id.,* Requirement 11.2.

[127] *See* NIST SP 800–53 Rev. 4, control RA–5, available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf*.

[128] *See, e.g.,* NIST SP 800–115, *Technical Guide to Information Security Testing and Assessment* (2008) (''NIST 800–115''), at 2–4, available at *http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf*, noting that ''[e]xternal testing often begins with reconnaissance techniques that search public registration data, Domain Name System (DNS) server information, newsgroup postings, and other publicly available information to collect information (*e.g.,* system names, Internet Protocol [IP] addresses, operating systems, technical points of contact) that may help the assessor to identify vulnerabilities.''

[129] *See, e.g.,* SANS Institute, *Penetration Testing: Assessing Your Overall Security Before Attackers Do* (June 2006), at 7, available at *https://www.sans.org/reading-room/whitepapers/analyst/penetration-testing-assessing-security-attackers-34635*, noting: ''A wide variety of tools may be used in penetration testing. These tools are of two main types; reconnaissance or vulnerability testing tools and exploitation tools. While penetration testing is more directly tied to the exploitation tools, the initial scanning and reconnaissance is often done using less intrusive tools.''

[130] *See,* PCI DSS, at 94, available at *https://www.pcisecuritystandards.org/security_standards/index.php*, defining a vulnerability scan as ''a combination of automated or manual tools, techniques, and/or methods run against external and internal network devices and servers, designed to expose potential vulnerabilities that could be found and exploited by malicious individuals.'' *See also* NIST SP 800–115, *supra* note 111, available at

Continued

note that in most situations, vulnerability monitoring is most efficient and cost-effective when automation is used.[131] Participants in the CFTC Roundtable agreed that automated vulnerability scanning provides important benefits.[132] Where indicated by appropriate risk analysis, automated scanning would be required to be conducted on an authenticated basis (*i.e.,* using log-in credentials).[133] Where automated scans are unauthenticated (*i.e.,* conducted without using usernames or passwords), effective compensating controls would be required.[134]

The proposed rule would require all DCMs, SEFs, and SDRs to conduct vulnerability testing at a frequency determined by an appropriate risk analysis. Testing as often as indicated by appropriate risk analysis is a best practice. For example, the FFIEC states that ''[t]he frequency of testing should be determined by the institution's risk assessment.'' [135] Best practices call for risk assessments to include consideration of a number of important factors in this regard, including, for example, the frequency and extent of changes in the organization's automated systems and operating environment; the potential impact if risks revealed by testing are not addressed appropriately; the degree to which the relevant threat environment or potential attacker profiles and techniques are changing; and the results of other testing.[136] Frequency appropriate to risk analysis can also vary depending on the type of monitoring involved; for example, with whether automated monitoring or procedural testing is being conducted.[137]

d. Minimum Vulnerability Testing Frequency Requirements for Covered DCMs and SDRs

The proposed rule would require covered DCMs and SDRs to conduct vulnerability testing no less frequently than quarterly. Best practices support this requirement. 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.[138] The Council on CyberSecurity calls for entities to ''continuously acquire, assess, and take action on new information in order to identify vulnerabilities.'' [139] In light of these best practices and the current level of cyber threat to the financial sector discussed above, the Commission believes that the proposed rule provisions regarding vulnerability testing frequency are appropriate in today's cybersecurity environment.[140]

e. Independent Contractor Vulnerability Testing Requirements for Covered DCMs and All SDRs

The proposed rule would require covered DCMs and SDRs to engage independent contractors to conduct two of the required quarterly vulnerability tests each year, while permitting covered DCMs and SDRs to conduct other vulnerability testing using employees not responsible for development or operation of the systems or capabilities being tested.

Participants in the CFTC Roundtable agreed that important benefits are provided when a testing program includes both testing by independent contractors and testing by entity employees not responsible for building or operating the system being tested. As one participant noted, ''[t]here are advantages to both, but neither can stand alone.'' [141] Much testing needs to happen internally, but much also needs to be conducted from the viewpoint of an outsider, particularly where testing against the possible tactics or techniques of a particular threat actor is concerned.[142] Third-party vendors offer specialized expertise concerning the latest threat intelligence, the latest attack vectors against the financial sector, and the recent experience of other entities with similar systems and similar vulnerabilities.[143] One benefit offered by testing conducted by entity employees is that internal vulnerability testing and scanning can utilize viewpoints that the outside world would not have, based on intimate knowledge of the entity's network and systems.[144] Conversely, an additional benefit provided by independent contractor testing comes from the outsider's different perspective, and his or her ability to look for things that entity employees may not have contemplated during the design or

http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf; noting that testing techniques that include vulnerability scanning ''. . . can identify systems, ports, services, and potential vulnerabilities, and may be performed manually but are generally performed using automated tools.''

[131] NIST SP 800–39, at 47–48, available at *http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.*

[132] CFTC Roundtable, at 170–171.

[133] The PCI Monitor, published by the PCI Security Standards Council, explains the differences between unauthenticated and authenticated vulnerability scanning, and the benefits of each type, as follows: [U]nauthenticated web application scan tests are conducted with no usernames and/or passwords as part of the test. Authenticated web application scan tests use usernames and passwords to simulate user activity on the Web site or system being tested. Essentially, unauthenticated scan testing is ''logged-out testing'' and authenticated scanning is ''logged-in testing.'' . . . Unauthenticated scan testing is typically much easier than authenticated testing; it can be performed with basic tools and doesn't require a great deal of technical expertise or understanding of the systems, Web pages or workflows being tested. Unauthenticated tests are also much quicker and can be effective in detecting recognizable vulnerabilities without investing a great deal of time and resources. However, unauthenticated testing alone is not an effective method of simulating targeted attacks. The results may be limited, producing a false sense of assurance that the systems have been thoroughly assessed. . . . [A]uthenticated testing is more thorough since user interaction and functionality . . . can be more accurately simulated. Performing authenticated testing does require a broader and deeper skill set and should only be performed by qualified, experienced professionals. . . . Additionally, since authenticated testing often includes manual techniques, the amount of time required to perform such tests can increase significantly. . . . As a general guideline, if the desire is to simulate what users on the system are able to do, then authenticated testing is the most effective approach. If the intent is to quickly identify the highest risks that any user or tool could exploit, then unauthenticated testing may suffice. Once the unauthenticated vulnerabilities are identified and remediated, then authenticated testing should be considered to achieve a more comprehensive assessment.

PCI Monitor, Vol. 2, Issue 26 (June 25, 2014), available at *http://training.pcisecuritystandards.org/the-pci-monitor-weekly-news-updates-and-insights-from-pci-ssc2?ecid=ACsprvuuirRbrU3vDlk76s_ngGKJKEYlvaBJzvvUMldZv4KKh6V1guIKOR5VLTNfAqPQ_Gmox3zO&utm_campaign=Monitor&utm_source=hs_email&utm_medium=email&utm_content=13292865&_hsenc=p2ANqtz_LIkkHURyUmyq1p2OxB39R5nOpRh1XHE_jW6wCC6EEUAow15E7AuExcIGwdYxyh_6YNxVvKorcurk6r90E3d7dG71fbw&_hsmi=13292865%20-%20web.*

[134] *See* PCI DSS, *supra* note 125, App. B at 112, available at *https://www.pcisecuritystandards.org/security_standards/index.php*: ''Compensating controls may be considered . . . when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other, or compensating, controls.''

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

[136] *See* NIST SP 800–39, at 47–48, available at *http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf*; FFIEC, *Information Security IT Examination Handbook,* at 82, available at *http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_InformationSecurity.pdf.*

[137] *Id.*

[138] PCI DSS, Requirement 11.2, available at *https://www.pcisecuritystandards.org/security_standards/index.php.*

[139] Council on CyberSecurity, CSC 4, *Continuous Vulnerability Assessment and Remediation,* available at *http://www.counciloncybersecurity.org/critical-controls/.*

[140] The Commission understands that most covered DCMs and SDRs currently conduct vulnerability testing on at least a quarterly basis and in many cases on a continuous basis.

[141] CFTC Roundtable, at 88.

[142] *Id.* at 88–89.

[143] *Id.* at 103–104.

[144] *Id.* at 177.

operation of the system involved.[145] One Roundtable participant observed that the vulnerability assessments which are the goal of vulnerability testing done by entity employees need to themselves be tested and validated by independent, external parties.[146] In short, an overall testing program that includes both testing by independent contractors and testing by entity employee can offer complementary benefits.

Regarding the benefits provided by independent contractor testing, NIST notes that:

> [E]ngaging third parties (*e.g.,* auditors, contractor support staff) to conduct the assessment offers an independent view and approach that internal assessors may not be able to provide. Organizations may also use third parties to provide specific subject matter expertise that is not available internally.[147]

FFIEC states that testing by independent contractors provides credibility to test results.[148] Where testing is conducted by entity employees, FFIEC calls for tests performed ''by individuals who are also independent of the design, installation, maintenance, and operation of the tested system.'' [149] In its COBIT 5 framework, ISACA states that those performing system safeguards testing and assurance should be independent from the functions, groups, or organizational components being tested.[150] With respect to system safeguards testing by internal auditors, FFIEC states that the auditors should have both independence and authority from the Board of Directors to access all records and staff necessary for their audits.[151] It also states that they should not participate in activities that may compromise or appear to compromise their independence, such as preparing or developing the types of reports, procedures, or operational duties normally reviewed by auditors.[152] The data security standards of the Payment Card Industry Security Standards Council call for conducting both internal and external vulnerability scans, with external scans performed by an approved vendor.[153]

Current Commission system safeguards rules leave to a DCM or SDR the choice of whether vulnerability testing or other system safeguards testing is conducted by independent contractors or entity employees not responsible for building or operating the systems being tested. The proposed requirement for some vulnerability testing to be performed by independent contractors is intended to ensure that covered DCM and SDR programs of risk analysis and oversight with respect to system safeguards include the benefits coming from a combination of testing by both entity employees and independent contractors, as discussed above. In light of the best practices and the current level of cyber threat to the financial sector discussed above, the Commission believes that the proposed rule provisions regarding vulnerability testing by independent contractors are appropriate in today's cybersecurity environment.

4. Penetration Testing

a. Need for Penetration Testing

Penetration testing to exploit cyber and automated system vulnerabilities, a testing type which complements vulnerability testing, is also a significant component of a DCM's, SEF's, or SDR's program of risk analysis and oversight to identify and minimize sources of operational risk. Penetration tests go beyond the uncovering of an organization's automated system vulnerabilities that vulnerability testing aims to achieve: They subject the system to real-world attacks by testing personnel, in order to identify both the extent to which an attacker could compromise the system before the organization detects and counters the attack, and the effectiveness of the organization's response mechanisms.[154] NIST defines penetration testing as ''[a] test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system.'' [155] NIST describes the benefits of penetration testing as follows:

> Penetration testing is a specialized type of assessment conducted on information systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Such testing can be used to either validate vulnerabilities or determine the degree of resistance organizational information systems have to adversaries within a set of specified constraints (*e.g.,* time, resources, and/or skills). Penetration testing attempts to duplicate the actions of adversaries in carrying out hostile cyber attacks against organizations and provides a more in-depth analysis of security-related weaknesses/deficiencies.[156]

The Council on CyberSecurity explains the need for penetration testing as follows:

> Attackers often exploit the gap between good defensive designs and intentions and implementation or maintenance. . . . In addition, successful defense requires a comprehensive program of technical defenses, good policy and governance, and appropriate action by people. In a complex environment where technology is constantly evolving, and new attacker tradecraft appears regularly, organizations should periodically test their defenses to identify gaps and to assess their readiness.
>
> Penetration testing starts from the identification and assessment of vulnerabilities that can be identified in the enterprise. It complements this by designing and executing tests that demonstrate specifically how an adversary can either subvert the organization's security goals (*e.g.,* the protection of specific Intellectual Property) or achieve specific adversarial objectives (*e.g.,* establishment of a covert Command and Control infrastructure). The result provides deeper insight, through demonstration, into the business risks of various vulnerabilities.
>
> [Penetration testing] exercises take a comprehensive approach at the full spectrum of organization policies, processes, and defenses in order to improve organizational readiness, improve training for defensive practitioners, and inspect current performance levels. Independent Red Teams can provide valuable and objective insights about the existence of vulnerabilities and the efficacy of defenses and mitigating controls already in place and even of those planned for future implementation.[157]

Anecdotally, one CFTC Roundtable participant characterized the need for penetration testing by stating that, ''you will never know how strong your security is until you try to break it yourself and try to bypass it,'' adding that ''if you're not testing to see how strong it is, I guarantee you, somebody

---

[145] *Id.* at 171.

[146] *Id.*

[147] NIST SP 800–115, at 6–6, available at *http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf.* NIST also notes that giving outsiders access to an organization's systems can introduce additional risk, and recommends proper vetting and attention to contractual responsibility in this regard.

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

[149] *Id.*

[150] ISACA, COBIT 5, Monitor, Evaluate and Assess (''MEA'') MEA02.05, *Ensure that assurance providers are independent and qualified,* available at *https://cobitonline.isaca.org.*

[151] *Id.* at 6.

[152] *Id.*

[153] PCI DSS, Requirement 11, *Regularly test security systems and processes,* at 94–96, available at *https://www.pcisecuritystandards.org/security_standards/index.php.*

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

[155] NIST SP 800–53 Rev. 4, App. B at B–17, available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.*

[156] *Id.* at F–62, CA–8 *Penetration Testing.*

[157] Council on Cybersecurity, CSC 20, *Penetration Tests and Red Team Exercises: Why Is This Control Critical?* available at *http://www.counciloncybersecurity.org/critical-controls/.*

else is.'' [158] Another Roundtable participant described the essential function of penetration testing as intruding into a network as stealthily as possible, mimicking the methodologies used by attackers, seeing whether and at what point the entity can detect the intrusion, and identifying gaps between the entity's current defenses and attacker capabilities, with the goal of reducing the time needed to detect an intrusion from multiple days to milliseconds, and closing the gaps between attacker and defender capabilities.[159]

b. Best Practices Call for Both External and Internal Penetration Testing

Best practices and standards provide that organizations should conduct two types of penetration testing: External and internal. Many best practices sources also describe the benefits of both types of penetration testing. The Council on CyberSecurity states that organizations should:

Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully. Penetration testing should occur from outside the network perimeter (*i.e.,* the Internet or wireless frequencies around an organization) as well as from within its boundaries (*i.e.,* on the internal network) to simulate both outsider and insider attacks.[160]

FINRA's recent Report on Cybersecurity Practices provides a useful description of the benefits of penetration testing:

Penetration Testing (also known as ''Pen Testing'') is an effective practice that simulates a real-world attack against a firm's computer systems. The goal of a third-party penetration test is to get an attacker's perspective on security weaknesses that a firm's technology systems may exhibit.

Penetration Tests are valuable for several reasons:

- Determining the feasibility of a particular set of attack vectors;
- identifying higher-risk vulnerabilities that result from a combination of lower-risk vulnerabilities exploited in a particular sequence;
- identifying vulnerabilities that may be difficult or impossible to detect with automated network or application vulnerability scanning software;
- assessing the magnitude of potential business and operational impacts of successful attacks;
- testing the ability of network defenders to successfully detect and respond to the attack; and
- providing evidence to support increased investments in security personnel and technology.

Penetration Tests can take different forms depending on a firm's specific objectives for the test. Each of these contributes in its own way to an overall defense-in-depth strategy.[161]

FINRA also describes the different benefits of external and internal penetration testing, and emphasizes the need for both types:

External penetration testing is designed to test a firm's systems as they are exposed to the outside world (typically via the Internet), while internal penetration testing is designed to test a firm's systems' resilience to the insider threat. An 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.[162]

NIST standards for system safeguards call for organizations to conduct penetration testing, and reference both external and internal testing.[163] NIST describes the benefits of external penetration tests as follows:

External security testing is conducted from outside the organization's security perimeter. This offers the ability to view the environment's security posture as it appears outside the security perimeter—usually as seen from the Internet—with the goal of revealing vulnerabilities that could be exploited by an external attacker.[164]

NIST notes that internal penetration tests offer different benefits, as follows:

For internal security testing, assessors work from the internal network and assume the identity of a trusted insider or an attacker who has penetrated the perimeter defenses. This kind of testing can reveal vulnerabilities that could be exploited, and demonstrates the potential damage this type of attacker could cause. Internal security testing also focuses on system-level security and configuration—including application and service configuration, authentication, access control, and system hardening.[165]

c. Proposed Penetration Testing Definitions and Related Provisions

The Commission is proposing to clarify the existing testing requirements for all DCMs, all SEFs, and all SDRs by specifying both external and internal penetration testing as essential to fulfilling those requirements, and defining both. External penetration testing would be defined as attempts to penetrate a DCM's, SEF's, or SDR's automated systems or networks from outside their boundaries to identify and exploit vulnerabilities (including, but not limited to, methods for circumventing the security features of an application, system, or network). Internal penetration testing would be defined as attempts to penetrate a DCM's, SEF's, or SDR's automated systems or networks from inside their boundaries to identify and exploit vulnerabilities (including, but not limited to, methods for circumventing the security features of an application, system, or network). These definitions are consistent with the standards and best practices discussed above. In light of the best practices, and the external and internal penetration testing benefits noted above, the Commission believes that such testing is important in the context of today's cybersecurity threat environment.

The proposed rule would require all DCMs, SEFs, and SDRs to conduct both external and internal penetration testing at a frequency determined by an appropriate risk analysis. As discussed above, testing as often as indicated by appropriate risk analysis is a best practice.[166]

d. Minimum Penetration Testing Frequency Requirements for Covered Dcms and Sdrs

The proposed rule would require covered DCMs and SDRs to conduct both external and internal penetration testing no less frequently than annually.[167] Best practices support this

[158] *Id.* at 96.

[159] *Id.* at 58–60.

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

[161] 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.*

[162] *Id.*

[163] NIST SP 800–53 Rev. 4, control CA-8 *Penetration Testing,* available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.*

[164] NIST SP 800–115, at 2–4 to 2–5, available at *http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf.*

[165] *Id. See also, e.g.,* System Administration, Networking, and Security Institute (''SANS''), *Penetration Testing in the Financial Services Industry* (2010), at 17, available at *https://www.sans.org/reading-room/whitepapers/testing/penetration-testing-financial-services-industry-33314* (''Penetration testing is essential given the context of high operational risk in the financial services industry.'')

[166] *See* discussion above concerning vulnerability testing.

[167] The SEC's Regulation System Compliance and Integrity (''Regulation SCI''), issued in final form in December 2014, also requires penetration testing by SCI entities, defined as including, among other things, national securities exchanges, alternative trading systems, and registered clearing agencies. It requires each SCI entity to conduct SCI reviews that include penetration testing at least every three years. The Commission's proposed rule would require covered DCMs and SDRs to conduct penetration testing at a frequency determined by an appropriate risk analysis, but no less frequently than annually. In light of the multiple best practices cited above, and the importance of covered DCMs and SDRs to the national economy, the Commission believes that conducting penetration testing at least annually is appropriate.

requirement.[168] NIST calls for at least annual penetration testing of an organization's network and systems.[169] The FFIEC calls for independent penetration testing of high risk systems at least annually, and for quarterly testing and verification of the efficacy of firewall and access control defenses.[170] 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.[171]

e. Independent Contractor Penetration Testing Requirements for Covered DCMS and All SDRS

The proposed rule would require covered DCMs and SDRs to engage independent contractors to conduct the required minimum of an annual external penetration test. It would allow covered DCMs and SDRs to have internal penetration testing, and any additional external penetration testing needed in light of appropriate risk analysis, conducted either by independent contractors or by entity employees who are not responsible for development or operation of the systems or capabilities being tested.

As noted above, best practices support having some testing conducted by independent contractors.[172] NIST notes that:

> [E]ngaging third parties (*e.g.,* auditors, contractor support staff) to conduct the assessment offers an independent view and approach that internal assessors may not be able to provide. Organizations may also use third parties to provide specific subject matter expertise that is not available internally.[173]

The data security standards of the Payment Card Industry Security Standards Council call for external testing to be performed by an approved vendor.[174] Participants in the CFTC Roundtable agreed that important benefits are provided when a testing program includes testing by independent contractors, noting that vendor testing has particular value with respect to what external penetration does, namely test from the viewpoint of an outsider and against the current tactics, techniques, and threat vectors of current threat actors as revealed by current threat intelligence.[175]

Current Commission system safeguards rules leave to a DCM or SDR the choice of whether penetration testing or other system safeguards testing is conducted by independent contractors or entity employees not responsible for building or operation of the systems being tested. The proposed requirement for the required minimum annual external penetration testing to be performed by independent contractors is intended to ensure that covered DCM and SDR programs of risk analysis and oversight with respect to system safeguards include the benefits provided when independent contractors perform such testing. In light of the best practices and the current level of cyber threat to the financial sector discussed above, the Commission believes that the proposed rule provisions regarding external penetration testing by independent contractors are appropriate in today's cybersecurity environment.[176]

5. Controls Testing

a. Need for Controls Testing

As defined in the proposed rule, controls are the safeguards or countermeasures used by a DCM, SEF, or SDR to protect the reliability, security, or capacity of its automated systems or the confidentiality, integrity, and availability of its data and information, so as to fulfill its statutory and regulatory responsibilities. Controls testing is defined as assessment of all of the DCM's, SEF's, or SDR's system safeguards-related controls, to determine whether they are implemented correctly, are operating as intended, and are enabling the organization to meet system safeguards requirements. Regular, ongoing testing of all of an organization's system safeguards-related controls for these purposes is a crucial part of the program of risk analysis and oversight required of all DCMs, SEFs, and SDRs by the Act and Commission regulations.[177] As noted in NIST's standards and best practices, there are three broad types of system safeguards-related controls, including technical controls, operational controls, and management controls.[178] Some controls provide safeguards against automated system failures or deficiencies, while others guard against human error, deficiencies, or malicious action. Controls testing as addressed by the proposed rule includes all of these types of system safeguards controls.

Describing some of the important benefits of controls assessment, NIST notes that ''[u]nderstanding the overall effectiveness of implemented security and privacy controls is essential in determining the risk to the organization's operations and assets . . . resulting from the use of the system,''[179] and observes that controls assessment ''is the principal vehicle used to verify that implemented security controls . . . are meeting their stated goals and objectives.'' [180] NIST adds that:

> Security assessments: (i) Ensure that information security is built into organizational information systems; (ii) identify weaknesses and deficiencies early in the development process; (iii) provide essential information needed to make risk-based decisions as part of security authorization processes; and (iv) ensure compliance to vulnerability mitigation procedures.[181]

The Commission believes that 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 and of its program of risk analysis and oversight.

---

[168] The Commission understands that most covered DCMs (as defined) and most SDRs currently conduct external and internal penetration testing at least annually.

[169] 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.*

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

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

[172] *See* discussion above concerning vulnerability testing.

[173] NIST SP 800-115, at 6–6, available at *http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf.* NIST also notes that giving outsiders access to an organization's systems can introduce additional risk, and recommends proper vetting and attention to contractual responsibility in this regard.

[174] PCI DSS, Requirement 11, *Regularly test security systems and processes,* at 94–96, available at *https://www.pcisecuritystandards.org/security_standards/index.php.*

[175] CFTC Roundtable, at 88–89, 103–104, 171.

[176] The Commission understands that most DCMs that would be covered by the proposed covered DCM definition, and most SDRs, currently have external penetration testing conducted by independent contractors at least annually.

[177] 17 CFR 38.1050(a) (for DCMs); 17 CFR 37.1400(a) (for SEFs); 17 CFR 49.24(a)(1) (for SDRs).

[178] NIST SP 800–53 Rev. 4, at F–3, available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf; See also* CFTC Roundtable, at 194–196.

[179] NIST SP 800–53A Rev. 4, *Assessing Security and Privacy Controls to Federal Information Systems and Organizations* (''NIST SP 800–53A Rev. 4''), at 1, available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf.*

[180] *Id.* at xi (Foreword).

[181] NIST SP 800–53 Rev. 4, control CA–2 *Security Assessments,* available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.*

b. Best Practices Call for Controls Testing

Best practices and standards call for organizations to conduct regular, ongoing controls testing that over time includes testing of all their system safeguards-related controls. NIST calls for organizations to have a security assessment plan that:

> Assesses the security controls in the information system and its environment of operation to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements.[182]

NIST notes that the results of such testing can allow organizations, among other things to identify potential cybersecurity problems or shortfalls, identify security-related weaknesses and deficiencies, prioritize risk mitigation decisions and activities, confirm that weaknesses and deficiencies have been addressed, and inform related budgetary decisions and capital investment.[183] FFIEC calls for controls testing because ''[c]ontrols should not be assumed to be completely effective,'' and states that a controls testing program ''is sound industry practice and should be based on an assessment of the risk of non-compliance or circumvention of the institution's controls.'' [184] ISACA's COBIT standards call for organizations to ''[c]ontinuously monitor and evaluate the control environment, including self-assessments and independent assurance reviews,'' [185] and to ''[r]eview the operation of controls . . . to ensure that controls within business process operate effectively.'' [186] ISACA observes that this enables management ''to identify control deficiencies and inefficiencies and to initiate improvement actions.'' [187]

c. Controls Testing Definitions and Related Provisions

In this NPRM, the Commission is proposing to clarify the existing testing requirements for all DCMs, SEFs, and SDRs by specifying controls testing as essential to fulfilling those requirements, and defining it. The proposed rule's definitions of controls and controls testing are discussed above.[188] The proposed rule also defines ''key controls'' as those controls that an appropriate risk analysis determines are either critically important for effective system safeguards, or intended to address risks that evolve or change more frequently and therefore require more frequent review to ensure their continuing effectiveness in addressing such risks.

The proposed rule would require each DCM, SEF, and SDR to conduct controls testing, including testing of each control included in its program of system safeguards-related risk analysis and oversight, at a frequency determined by an appropriate risk analysis. As discussed above, testing at such a frequency is a best practice.[189]

d. Minimum Controls Testing Frequency Requirements for Covered DCMs and SDRs

The proposed rule would call for a covered DCM or an SDR to conduct controls testing, including testing of each control included in its program of system safeguards-related risk analysis and oversight, no less frequently than every two years. It would permit such testing to be conducted on a rolling basis over the course of the two-year period or the period determined by appropriate risk analysis, whichever is shorter.[190]

The proposed rule includes this frequency provision in order to ensure that in all cases, each control included in the system safeguards risk analysis and oversight program of a covered DCM or an SDR is tested at least every two years, or tested more frequently if that is indicated by appropriate analysis of the entity's system safeguards-related risks. The Commission believes that it is essential for each 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. The Commission also recognizes that appropriate risk analysis may well determine that more frequent testing of either certain key controls or all controls is necessary.

The provision permitting such testing to be done on a rolling basis is included in recognition of the fact that an adequate system safeguards program for a covered DCM or an SDR must necessarily include large numbers of controls of all the various types discussed above, and that therefore it could be impracticable and unduly burdensome to require testing of all controls in a single test. The rolling basis provision is designed to give flexibility to a covered DCM or an SDR concerning which controls are tested when during the applicable minimum period—either every two years or more often if called for by appropriate risk analysis—as long as each control is tested within the applicable minimum period. This flexibility is intended to reduce burdens associated with testing every control to the extent possible while still ensuring the needed minimum testing frequency. Testing on a rolling or recursive basis is also congruent with best practices. NIST states that a controls test can consist of either complete assessment of all controls or a partial assessment of controls selected for a particular assessment purpose.[191] NIST notes that over time, organizations can increase cybersecurity situational awareness through appropriate testing, which provides increased insight into and control of the processes used to manage the organization's security, which in turn enhances situational awareness, in a recursive process.[192]

e. Independent Contractor Controls Testing Requirements for Covered DCMs and SDRs

The proposed rule would require covered DCMs and SDRs to engage independent contractors to test and assess each of the entity's key controls no less frequently than every two years.[193] It permits the covered DCM or SDR to conduct any other required controls testing by using either independent contractors or entity employees not responsible for development or operation of the systems of capabilities involved in the test. Independent testing of key controls is consonant with best practices. ISACA

[182] *Id.*

[183] NIST SP 800–53A Rev. 4, at 3, available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf.*

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

[185] ISACA, COBIT 5, *MEA02 Evaluate and Assess the System of Internal Control,* available at *https://cobitonline.isaca.org/.*

[186] *Id.,* Section 02.02 *Review Business Process Controls Effectiveness.*

[187] *Id.,* Section 02.

[188] *See* discussion above concerning the need for controls testing.

[189] *See* discussion above concerning vulnerability testing.

[190] The Commission understands that the proposed rule could result in some additional controls testing costs for some covered DCMs or SDRs, because they are not currently conducting testing of all their system safeguards controls at the minimum frequency required by the proposed rule. In such cases, the covered DCM or SDR would need to accelerate the testing of some controls to comply with the two-year minimum frequency requirement.

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

[192] NIST SP–800–137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,* at 6, available at *http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf.*

[193] The Commission understands that most DCMs that would be covered by the proposed covered DCM definition, and most SDRs, currently retain independent contractors to perform testing of their key controls.

standards call for controls testing to include independent assurance reviews as well as self-assessments, in order to assure control effectiveness.[194] NIST calls 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.[195] The proposed rule's requirement for testing of key controls by independent contractors at least every two years is designed to ensure that covered DCM and SDR programs of risk analysis and oversight with respect to system safeguards include these benefits with regard to the testing of their key controls. In light of the best practices and the current level of cyber threat to the financial sector discussed above, the Commission believes that having each of a covered DCM's or SDR's key controls tested by independent contractors at least every two years is appropriate and important in today's cybersecurity environment. The rolling basis provision of the proposed rule regarding controls testing would leave to a covered DCM or SDR the choice of whether to have key controls testing by independent contractors done in a single test at least every two years, or in multiple, partial tests by independent contractors that cover each key control within the two-year minimum period.[196]

6. Security Incident Response Plan Testing

a. Need for Security Incident Response Plans and Testing

Financial sector entities should maintain and test a security incident response plan (''SIRP''). As the Council on CyberSecurity explains in addressing its Critical Security Control calling for incident response plans and testing:

> Cyber incidents are now just part of our way of life. Even large, well-funded, and technically sophisticated enterprises struggle to keep up with the frequency and complexity of attacks. The question of a successful cyber-attack against an enterprise is not ''if'' but ''when''. When an incident occurs, it is too late to develop the right procedures, reporting, data collection, management responsibility, legal protocols, and communications strategy that will allow the enterprise to successfully understand, manage, and recover. Without an incident response plan, an organization may not discover an attack in the first place, or, if the attack is detected, the organization may not follow good procedures to contain damage, eradicate the attacker's presence, and recover in a secure fashion. Thus, the attacker may have a far greater impact, causing more damage, infecting more systems, and possibly exfiltrate more sensitive data than would otherwise be possible were an effective incident response plan in place.[198]

Adequate cyber resilience requires that organizations have the capacity to detect, contain, eliminate, and recover from a cyber intrusion. The Commission believes that SIRPs and their testing are essential to such capabilities.

CFTC Roundtable participants recommended that the Commission consider SIRP testing in addressing the various types of testing needed in today's cyber threat environment.[199] Panelists stated that testing an organization's ability to recover from cyber attacks, in particular from attacks aimed at destruction of data or automated systems or at degradation of data integrity, is very important.[200] They noted that when a security incident actually happens, it is helpful to have an incident response plan, but more helpful to have tested it. Panelists explained if the organization has practiced its plan or framework for responding to a security incident, the people who must make decisions—often with incomplete or conflicting information—will know what numbers to call, where to go, what is expected, and what the framework is for making the quick decisions that are needed. They also noted that failure to practice the response process can delay or paralyze timely response and cause severe consequences, and that this makes practicing an incident response plan or framework crucial to effective incident response.[201] Panelists also noted that much financial sector business continuity testing has focused in the past on an entity's ability to respond to physical security incidents such as storms, transportation or electric power outages, fire, flood, etc. In addition to physical security incident response testing, adequate testing today must take into account the fact that the risk landscape has changed and now includes increased cyber threat.[202]

b. Best Practices Call for Maintaining and Testing a SIRP

Having and testing a cyber and physical security incident response plan is a best practice with regard to cybersecurity. NIST urges organizations to have a cyber incident response plan that:

> Establishes procedures to address cyber attacks against an organization's information system(s). These procedures are designed to enable security personnel to identify, mitigate, and recover from malicious computer incidents, such as unauthorized access to a system or data, denial of service, or unauthorized changes to system hardware, software, or data (*e.g.,* malicious logic, such as a virus, worm, or Trojan horse).[203]

NIST notes that such plans may be included as an appendix to the organization's business continuity plan.[204]

NIST best practices for cybersecurity also call for organizations to test their incident response capabilities with respect to their information systems, at appropriate frequencies, to determine their effectiveness, and to document test results.[205] They provide that organizations should:

---

[194] ISACA, COBIT 5, MEA02, *Monitor, Evaluate and Assess the System of Internal Control,* available at *https://cobitonline.isaca.org/.*

[195] NIST SP 800–53 Rev. 4, control CA–2 *Security Assessments,* Control Enhancements 1, *Security Assessments: Independent Assessors,* available at *http://nvlpubs.nist.gov/nistpubs/Special Publications/NIST.SP.800-53r4.pdf.*

[196] The requirements proposed by the Commission regarding controls testing are generally consistent with the SEC's Regulation SCI, issued in final form in December 2014. Regulation SCI applies to SCI entities, defined as including, among other things, national securities exchanges, alternative trading systems, and registered clearing agencies. It requires each SCI entity to conduct SCI reviews that include assessments of the design and effectiveness of internal controls, in a manner consistent with industry standards. SCI reviews must be conducted at least annually.

[197] NIST defines a ''security incident'' as ''[a]n occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.'' NIST SP 800–53 Rev. 4, at B–9, available at *http://nvlpubs.nist.gov/nistpubs/Special Publications/NIST.SP.800-53r4.pdf.* NIST further defines a ''computer security incident'' as ''a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.'' NIST SP 800–61 Rev. 2, available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.* The FFIEC defines a ''security incident'' as ''the attempted or successful unauthorized access, use, modification, or destruction of information systems or customer data. If unauthorized access occurs, the financial institution's computer systems could potentially fail and confidential information could be compromised.'' FFIEC IT Examination Handbook, *Business Continuity Planning IT Examination Handbook,* at 25, available at *http://ithandbook.ffiec.gov/ ITBooklets/FFIEC_ITBooklet_BusinessContinuityPlanning.pdf.*

[198] Council on CyberSecurity, *The Critical Security Controls for Effective Cyber Defense Version 5.1,* CSC 18, at 96, available at *http://www.counciloncybersecurity.org/critical-controls/.*

[199] CFTC Roundtable, at 82–84.

[200] *Id.* at 79–80.

[201] *Id.* at 284–287.

[202] *Id.* at 283–284, 290–294.

[203] NIST SP 800–34 Rev. 1, *Contingency Planning Guide for Federal Information Systems* (''NIST SP 800–34 Rev. 1''), § 2.2.5 *Cyber Incident Response Plan,* at 11, available at *http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf.*

[204] *Id.*

[205] NIST SP 800–53 Rev. 4, control IR–3 *Incident Response Testing*, available at *http://*

Continued

[H]ave information technology (IT) plans in place, such as contingency and computer security incident response plans, so that they can respond to and manage adverse situations involving IT. These plans should be maintained in a state of readiness, which should include having personnel trained to fulfill their roles and responsibilities within a plan, having plans exercised to validate their content, and having systems and system components tested to ensure their operability in an operational environment specified in a plan. These three types of events can be carried out efficiently and effectively through the development and implementation of a test, training, and exercise (TT&E) program. Organizations should consider having such a program in place because tests, training, and exercises are so closely related. For example, exercises and tests offer different ways of identifying deficiencies in IT plans, procedures, and training.[206]

NIST adds that:

Organizations should conduct TT&E events periodically; following organizational changes, updates to an IT plan, or the issuance of new TT&E guidance; or as otherwise needed. This assists organizations in ensuring that their IT plans are reasonable, effective, and complete, and that all personnel know what their roles are in the conduct of each IT plan. TT&E event schedules are often dictated in part by organizational requirements. For example, NIST Special Publication 800–53 requires Federal agencies to conduct exercises or tests for their systems' contingency plans and incident response capabilities at least annually.[207]

In addition, NIST states that an organization following best practices:

Coordinates contingency planning activities with incident handling activities. By closely coordinating contingency planning with incident handling activities, organizations can ensure that the necessary contingency planning activities are in place and activated in the event of a security incident.[208]

According to NIST, an organization following best practices tests the contingency plan for an information system at an appropriate frequency, using organization-defined tests, to determine the effectiveness of the plan and the organizational readiness to execute the plan. It then reviews the test results, and initiates corrective actions if needed.[209]

FINRA's best practices also call for SIRPs. FINRA's 2015 Report on Cybersecurity Practices states that:

Firms should establish policies and procedures, as well as roles and responsibilities for escalating and responding to cybersecurity incidents. Effective practices for incident response include involvement in industry-wide and firm-specific simulation exercises as appropriate to the role and scale of a firm's business.[210]

The FFIEC has said that ''[e]very financial institution should develop an incident response policy that is properly integrated into the business continuity planning process.'' [211] The FFIEC also calls for incident response plan testing, stating that ''[f]inancial institutions should assess the adequacy of their preparation by testing incident response guidelines to ensure that the procedures correspond with business continuity strategies.[212]

The Council on CyberSecurity's Critical Security Controls provide that organizations should protect their information, as well as their reputations, by developing and implementing an incident response plan and infrastructure ''for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.'' [213] The Critical Security Controls also call for organizations to ''conduct periodic incident scenario sessions for personnel associated with the incident handling team, to ensure that they understand current threats and risks, as well as their responsibilities in supporting the incident handling teams.'' [214]

c. Flexibility Regarding Forms of SIRP Testing

SIRP testing can take a number of possible forms, consistent with generally accepted standards and best practices, and accordingly, the proposed rule would apply the general requirement that the forms of testing addressed in an entity's security incident response plan should be aligned with an entity's appropriate analysis of its system safeguards-related risks. As noted in NIST's best practices regarding security incident response testing:

Organizations test incident response capabilities to determine overall effectiveness of the capabilities and to identify potential weaknesses or deficiencies. Incident response testing includes, for example, the use of checklists, walk-through or tabletop exercises, simulations (parallel/full interrupt), and comprehensive exercises. Incident response testing can also include a determination of the effects on organizational operations (*e.g.,* reduction in mission capabilities), organizational assets, and individuals due to incident response.[215]

As provided in the proposed rule, the scope of the plan and its testing should be broad enough to support entity resilience with respect to security incidents that is sufficient to enable the entity to fulfill its statutory and regulatory responsibilities. Such resilience should include the ability to detect, contain, respond to, and recover from both cyber and physical security incidents in a timely fashion.

d. Best Practices Provide Guidance Regarding Appropriate SIRP Contents

The Commission notes that its existing system safeguards rules and guidance for DCMs, SEFs, and SDRs provide that those entities should follow generally accepted standards and best practices in meeting the testing requirements applicable to their required program of risk analysis and oversight with respect to system safeguards, and that this applies with respect to SIRPs and their testing.[216] Best practices provide useful guidance concerning the contents of an adequate SIRP.

For example, NIST calls for an organization to develop, document, and distribute to the appropriate personnel ''an incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance,'' as well as ''procedures to facilitate the implementation of the incident response policy and associated incident response controls.'' [217] NIST further recommends that an

---

nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[206] NIST SP 800–84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities* (''NIST SP 800–84''), at ES–1, available at *http://csrc.nist.gov/publications/nistpubs/800-84/SP800-84.pdf.*

[207] *Id.* at ES–2.

[208] NIST SP 800–53 Rev. 4, control CP–2 *Contingency Plan,* available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-3r4.pdf.*

[209] NIST SP 800–53 Rev. 4, control CP–4 *Contingency Plan Testing,* available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.*

[210] FINRA, *Report on Cybersecurity Practices* (February 2015), at 23, available at *https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf.*

[211] FFIEC, *Business Continuity Planning IT Examination Handbook,* at 25, available at *http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_BusinessContinuityPlanning.pdf.*

[212] *Id.* at 25–26.

[213] Council on CyberSecurity, *The Critical Security Controls for Effective Cyber Defense Version 5.1,* CSC 18, at 96, available at *http://www.counciloncybersecurity.org/critical-controls/.*

[214] *Id.* at 97.

[215] NIST SP 800–53 Rev. 4, control IR–3 *Incident Response Testing,* available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.*

[216] 17 CFR 38.1050; 17 CFR 38.1051(a) and (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); 17 CFR 49.24(a) through (c) (for SDRs).

[217] NIST SP 800–53 Rev. 4, control IR–1 *Incident Response Policy and Procedures,* available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.*

organization should develop and maintain an incident response plan that:

1. Provides the organization with a roadmap for implementing its incident response capability;
2. Describes the structure and organization of the incident response capability;
3. Provides a high-level approach for how the incident response capability fits into the overall organization;
4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
5. Defines reportable incidents;
6. Provides metrics for measuring the incident response capability within the organization;
7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
8. Is reviewed and approved by [appropriate organization-defined personnel or roles].[218]

NIST also calls for the organization to distribute copies of the plan to appropriate personnel; review the plan at an appropriate frequency; update the plan ''to address system/organizational changes or problems encountered during plan implementation, execution, or testing;'' communicate plan changes to appropriate personnel; and protect the plan from unauthorized disclosure and modification.[219] NIST notes that while incident response policies are individualized to the organization, most policies include the same key elements:

- Statement of management commitment.
- Purpose and objectives of policy.
- Scope of the policy (to whom and what it applies and under what circumstances).
- Definition of computer security incidents and related terms.
- Organizational structure and definition of roles, responsibilities, and levels of authority; should include the authority of the incident response team to confiscate or disconnect equipment and to monitor suspicious activity, the requirements for reporting certain types of incidents, the requirements and guidelines for external communications and information sharing (*e.g.,* what can be shared with whom, when, and over what channels), and the handoff and escalation points in the incident management process.
- Prioritization or severity ratings of incidents.
- Performance measures.
- Reporting and contact forms.[220]

[218] NIST SP 800–53 Rev. 4, control IR–8 *Incident Response Plan,* available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.*

[219] *Id.*

[220] NIST SP 800–61 Rev. 2, section 2.3.1 *Policy Elements,* available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.*

e. Proposed SIRP Definitions and Related Provisions

In this NPRM, the Commission is proposing to clarify the existing testing requirements for all DCMs, SEFs, and SDRs by specifying SIRP testing as essential to fulfilling those requirements, and defining it. The proposed rule would define ''security incident'' as a cyber or physical security event that actually or potentially jeopardizes automated system operation, reliability, security, or capacity, or the availability, confidentiality, or integrity of data. The proposed rule would define ''security incident response plan'' as a written plan that documents the DCM's, SEF's, or SDR's policies, controls, procedures, and resources for identifying, responding to, mitigating, and recovering from security incidents, as well as the roles and responsibilities of management, staff, and independent contractors in responding to security incidents. This definition notes that a SIRP may be a separate document or a BC–DR plan section or appendix dedicated to security incident response. The proposed rule would define ''security incident response plan testing'' as testing of a DCM's, SEF's, or SDR's SIRP to determine its effectiveness, identify its potential weaknesses or deficiencies, enable regular updating and improvement, and maintain the entity's preparedness and resiliency with respect to security incidents. This definition adds that methods of conducting SIRP testing may include (without limitation) checklist completion, walk-through or table-top exercises, simulations, and comprehensive exercises.

The proposed rule would require all DCMs, SEFs, and SDRs to conduct SIRP testing at a frequency determined by an appropriate risk analysis. As discussed above, testing as often as indicated by appropriate risk analysis is a best practice.[221] The Commission believes that in today's cybersecurity threat environment, appropriate risk analysis may well call for conducting frequent SIRP tests of various types. The flexibility regarding forms of SIRP testing provided by the proposed rule is designed in part to encourage appropriately frequent SIRP testing.

f. Minimum SIRP Testing Frequency Requirements for Covered DCMs and SDRs

The proposed rule would call for a covered DCM or an SDR to conduct SIRP testing no less frequently than annually.[222] Best practices support this requirement. For example, NIST calls for organizations to test their systems-related contingency plans and incident response capabilities at least annually.[223]

[221] *See* discussion above concerning vulnerability testing.

g. Who Performs Security Incident Response Plan Testing

The proposed rule would leave to covered DCMs and SDRs (as well as to all other DCMs and to all SEFs) the choice of having security incident response plan testing conducted by independent contractors or by employees of the covered DCM or SDR. This provision of the proposed rule therefore would not impose any additional burdens or costs on DCMs or SDRs.

7. Enterprise Technology Risk Assessment

a. Enterprise Technology Risk Assessment Definition and Purpose

The proposed rule would clarify the testing requirements of the Commission's current system safeguards rules for all DCMs, SEFs, and SDRs by specifying that conducting regular enterprise technology risk assessments (''ETRAs'') is essential to meeting those testing requirements. The proposed rule would define ETRAs as written assessments that include (without limitation) an analysis of threats and vulnerabilities in the context of mitigating controls. As further defined, an ETRA identifies, estimates, and prioritizes a DCM's, SEF's or SDR's risks to operations or assets, or to market participants, individuals, or other entities, resulting from impairment of the confidentiality, integrity, or availability of data and information or the reliability, security, or capacity of automated systems. The purpose of assessments of enterprise risk is identifying (a) threats and vulnerabilities, (b) the harm that could occur given the potential for threats that exploit vulnerabilities, and (c) the likelihood that such harm will occur, in order to produce a broad determination of the organization's system safeguards-related risks.[224] According to NIST, such risk assessment is necessary for well-informed, risk-based leadership

[222] The Commission understands that many covered DCMs (as defined) and many SDRs currently conduct SIRP testing at least annually.

[223] 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).

[224] NIST SP 800–39, at 1, available at *http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.*

decisions that ''balance the benefits gained from the operation and use of . . . information systems with the risk of the same systems being vehicles through which purposeful attacks, environmental disruptions, or human errors cause mission or business failure.'' [225]

An ETRA may be used as the 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 order to identify and mitigate its system safeguards-related risks. As NIST observes, ''[s]ince no one technique can provide a complete picture of the security of a system or network, organizations should combine appropriate techniques to ensure robust security assessments.'' [226]

The proposed rule's testing scope provisions would require that DCMs, SEFs, and SDRs conduct ETRAs of a scope broad enough to identify any vulnerability that, if exploited or accidentally triggered, could enable: (1) Interference with the organization's operations or the fulfillment of its statutory and regulatory responsibilities, (2) impairment or degradation of the reliability, security, or capacity of the organization's automated systems, (3) addition, deletion, modification, exfiltration, or compromise of any data relating to the organization's regulated activities, or (4) any other unauthorized action affecting the organization's regulated activities or the hardware or software used in connection with them. The proposed rule would not, however, specify particular methods, structures, or frameworks for ETRAs. Best practices provide a number of sources for such risk assessment frameworks,[227] and a DCM, SEF, or SDR would have flexibility to choose the assessment framework it believes most appropriate to its particular circumstances. FINRA notes that approaches to integrating threats and vulnerabilities in an overall risk assessment report often differ, with some organizations following proprietary risk assessment methodologies and others using vendor products tailored to their particular needs, and with firms using a variety of cyber incident and threat intelligence inputs for their risk assessments.[228] The flexibility provided by the proposed rule in this respect is intended to reduce the costs of performing an ETRA to the extent practicable while still ensuring the sufficiency of the important assessment process.

The proposed rule would require all DCMs, SEFs, and SDRs to conduct ETRAs at a frequency determined by an appropriate risk analysis. As noted above, conducting testing and assessment as often as indicated by such risk analysis is a best practice.[229]

b. Best Practices Call for ETRAs

Regular performance of ETRAs is a best practice. In describing such assessments and emphasizing their importance, FFIEC states that:

> Financial institutions must maintain an ongoing information security risk assessment program that effectively:
> • Gathers data regarding the information and technology assets of the organization, threats to those assets, vulnerabilities, existing security controls and processes, and the current security standards and requirements;
> • Analyzes the probability and impact associated with the known threats and vulnerabilities to their assets; and
> • Prioritizes the risks present due to threats and vulnerabilities to determine the appropriate level of training, controls, and assurance necessary for effective mitigation.[230]

FINRA calls for firms to conduct regular risk assessments to identify cybersecurity risks, and for such assessments to include ''an assessment of external and internal threats and asset vulnerabilities, and prioritized and time-bound recommendations to remediate identified risks.'' [231] FINRA calls such risk assessments ''a key driver in a firm's risk management-based cybersecurity program.'' [232] ISACA standards contain similar provisions.[233]

c. Minimum ETRA Frequency Requirements for Covered DCMs and SDRs

The proposed rule would call for covered DCMs and SDRs to conduct an ETRA no less frequently than annually.[234] Either annual or more frequent assessment of technology and cybersecurity risk is a best practice. 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.[235] As noted above, FFIEC calls for financial institutions to maintain ongoing information security risk assessment programs.[236]

The proposed requirement to prepare a written assessment on at least an annual basis would 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 proposed requirement is intended to formalize the risk assessment process and ensure that it is documented at a minimum frequency. As noted in the FFIEC Handbook: ''Monitoring and updating the security program is an important part of the ongoing cyclical security process. Financial institutions should treat security as dynamic with active monitoring; prompt, ongoing risk assessment; and appropriate updates to controls.'' [237]

d. Who Conducts ETRAs

The proposed rule would permit covered DCMs and SDRs (as well as all other DCMs and all SEFs) to conduct ETRAs using either independent contractors or employees not responsible for development or operation of the systems or capabilities being assessed. Assessment by independent contractors is congruent with best practices. NIST and FFIEC note that assessment by independent contractors offers the benefit of an independent view and approach that might not be provided by internal assessors, and can lend credibility to assessment results.[238] Best practices

[225] *Id.*

[226] NIST SP 800–115, available at *http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf.*

[227] *See, e.g.,* ISACA, COBIT 5; *International Organisation for Standardisation and International Electrotechnical Commission (''ISO/IEC'') 27001;* FFIEC.

[228] 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.*

[229] *See* discussion of vulnerability testing frequency.

[230] FFIEC, *Information Security IT Examination Handbook,* at 7–8, available at *http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_InformationSecurity.pdf.*

[231] FINRA, *Report on Cybersecurity Practices* (February 2015), at 12, available at *https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf.*

[232] *Id.* at 13.

[233] ISACA, COBIT 5, APO12, *Manage Risk,* available at *https://cobitonline.isaca.org.*

[234] The Commission understands that most covered DCMs and most SDRs currently perform cybersecurity and system safeguards risk assessments on at least an annual basis.

[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.*

[236] FFIEC, *Information Security IT Examination Handbook,* at 7–8, available at *http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_InformationSecurity.pdf.*

[237] *Id.* at 86.

[238] *See* NIST SP 800–115, at 6–6, available at *http://csrc.nist.gov/publications/nistpubs/800-115/*

also support assessment by entity employees, provided that they are suitably independent of the design, installation, maintenance, and operation of systems being assessed.[239] A dedicated risk department, an internal audit department, or a Chief Compliance Officer would be examples of entity employees who could appropriately conduct an ETRA. Because the proposed rule gives flexibility to covered DCMs and SDRs regarding who conducts ETRAs, this provision will not impose additional costs.[240]

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

As noted above, 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.[241] 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.[242] The Commission's existing 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.[243] The existing rules and guidance also provide that a DCM's, SEF's, or SDR's entire program of risk analysis and oversight, which includes such testing, should be based on generally accepted standards and best practices with respect to the development, operation, reliability, security, and capacity of automated systems.[244]

In this NPRM, in addition to clarifying the existing testing requirements for DCMs, SEFs, and SDRs by specifying and defining the five types of testing that these entities necessarily must perform to fulfill those requirements, the Commission also proposes to clarify the testing requirements by specifying and defining three other 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. 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. These risk analysis and oversight program aspects are generally recognized best practice for system safeguards. As best practices and also the Act and the regulations themselves make clear, it would be essentially impossible for a DCM, SEF, or SDR to fulfill its obligation to conduct testing sufficient to ensure the reliability, security, and capacity of its automated systems without conducting testing of appropriate scope; without performing appropriate internal reporting and review of test results; or without remediating vulnerabilities and deficiencies disclosed by testing, in line with appropriate risk analysis.[245] This has been true since before the testing requirements of the Act and the current regulations were adopted.[246] Accordingly, the provisions of the proposed rule addressing testing scope, internal reporting and review, and remediation clarify the testing requirements of the existing system safeguards rules for DCMs, SEFs, and SDRs; they do not impose new requirements.

1. Scope of Testing and Assessment

The Commission is proposing that the scope of all testing and assessment required by its 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.

Testing scope should take into account not only an organization's particular automated systems and networks and vulnerabilities, including any recent changes to them, but also the nature of the organization's possible adversaries and their capabilities as revealed by current cybersecurity threat analysis: iI short, it should be based on proper risk analysis.[247] The Commission recognizes that, as Roundtable panelists noted, the scope set for particular instances of the various types of cybersecurity testing can vary appropriately.[248] The scope provisions

SP800-115.pdf; and FFIEC, *Information Security IT Examination Handbook,* at 81, available at *http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_InformationSecurity.pdf.*

[239] *Id. See also, e.g.,* ISACA, COBIT 5, MEA02.05, *Ensure that assurance providers are independent and qualified,* available at *https://cobitonline.isaca.org/.*

[240] The requirements proposed by the Commission regarding enterprise technology risk assessment are generally consistent with the SEC's Regulation SCI, issued in final form in December 2014. Regulation SCI applies to SCI entities, defined as including, among other things, national securities exchanges, alternative trading systems, and registered clearing agencies. It requires each SCI entity to conduct SCI reviews that include automated system risk assessments, in a manner consistent with industry standards. SCI reviews must be conducted at least annually.

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

[242] *Id.*

[243] 17 CFR 38.1051(h) (for DCMs); 17 CFR 37.1401(g) (for SEFs); 17 CFR 49.24(j) (for SDRs).

[244] *See* 17 CFR 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); 17 CFR 49.24(c) (for SDRs).

[245] *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*; NIST SP 800–53A Rev. 4, at 10, available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf;* FFIEC, *Information Security IT Examination Handbook,* at 5, available at *http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_InformationSecurity.pdf*; NIST SP 800–53 Rev. 4, *Program Management (''PM'') control family,* available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf*; FINRA, *Report on Cybersecurity Practices,* February 2015, at 8, available at *https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf;* FFIEC, *Audit IT Examination Handbook,* Objective 6, at A–4, available at *http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_Audit.pdf*; ISACA, COBIT 5, APO12, available at *https://cobitonline.isaca.org/.*

[246] The current system safeguards provisions of the CEA and the Commission's regulations became effective in August 2012. Generally accepted best practices called for appropriate testing scope, internal reporting and review of test results, and remediation of vulnerabilities and deficiencies disclosed by testing well before that date, as shown in the following examples. Regarding scope of testing and assessment, *see, e.g.,* NIST SP 800–115, *Technical Guide to Information Security Testing and Assessment,* at 6–10 to 6–12, September 2008, available at *http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf.* Regarding internal reporting and review, *see, e.g.,* FFIEC, *Information Security IT Examination Handbook,* at 5, available at *http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_InformationSecurity.pdf.* Regarding remediation, *see, e.g.,* FFIEC, *Audit IT Examination Handbook,* Objective 6, at A–4, available at *http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_Audit.pdf.*

[247] CFTC Roundtable, at 97, 100–101, 107–111, 127–130, 139–141, 172–180.

[248] *Id.*

of the proposed rule are designed to give a DCM, SEF, or SDR flexibility with regard to setting the scope of particular cybersecurity tests, so long as its overall program of testing is sufficient to provide adequate assurance of the overall effectiveness of its cybersecurity controls with respect to its system safeguards-related risks. The Commission believes that the scope of testing and assessment set out in the proposed rule is broad enough to provide the needed flexibility, while still providing sufficient guidance regarding the testing scope necessary for an adequate program of system safeguards-related risk analysis and oversight. Such flexibility should reduce costs and burdens associated with the proposed scope requirements to the extent possible while still ensuring the system safeguards resilience necessary in today's cybersecurity threat environment.

2. Internal Reporting and Review

The proposed rule would require that 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. It also would require 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.

Oversight of an organization's cybersecurity and system safeguards program by both senior management and the Board of Directors is a best practice. According to FINRA:

> Active executive management—and as appropriate to the firm, board-level involvement—is an essential effective practice to address cybersecurity threats. Without that involvement and commitment, a firm is unlikely to achieve its cybersecurity goals.[249]

FINRA observes that ''[b]oards should play a leadership role in overseeing firms' cybersecurity efforts,'' and states that they should understand and approach cybersecurity as an enterprise-wide risk management issue rather than merely an information technology issue.[250] As noted by FINRA, the absence of proactive senior management and board involvement in cybersecurity can make firms more vulnerable to successful cybersecurity attacks.[251] The FFIEC states that regular reports to the board should address the results of the organization's risk assessment process and of its security monitoring and testing, including both internal and external audits and reviews.[252] In addition, FFIEC calls for boards to review recommendations for changes to the information security program resulting from testing and assessment, and to review the overall effectiveness of the program.[253]

3. Remediation

The proposed rule would require 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. The proposed rule would require such remediation to be timely in light of appropriate risk analysis with respect to the risks presented.

Remediation of vulnerabilities and deficiencies revealed by cybersecurity testing is a best practice and a fundamental purpose of such testing. FFIEC calls for management of financial sector organizations to take appropriate and timely action to address identified cybersecurity and system safeguards problems and weaknesses.[254] ISACA's COBIT 5 standards call for organizations to continually identify, assess, and reduce IT-related risk within levels of tolerance set by executive management.[255]

Best practices recognize that risk mitigation decisions and activities need to be prioritized in light of appropriate risk analysis, and that prompt and sufficient corrective action should target not only significant deficiencies noted in testing and assessment reports but also the root causes of such deficiencies.[256] The minimum basis for system safeguards remediation decisions, priorities, and actions by DCMs, SEFs, and SDRs is set out in the proposed rule: DCMs, SEFs, and SDRs must remediate system safeguards vulnerabilities and deficiencies sufficiently to enable them to meet applicable system safeguards requirements and fulfill their statutory and regulatory obligations. Remediation that failed to meet this standard would not provide adequate system safeguards protection in today's cybersecurity threat environment, and could result in unacceptable harm to the public or the national economy.

H. Required Production of Annual Total Trading Volume

As discussed above in preamble section F, the proposed rule would create requirements applicable to covered DCMs, as defined, as well as to SDRs, concerning system safeguards testing frequency and testing by independent contractors. As also discussed above, the Commission believes that the minimum testing frequency and independent contractor testing requirements in the proposed rule should be applied 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. 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. With respect to DCMs, the Commission believes that applying the proposed frequency and independent contractor requirements only to DCMs whose annual total trading volume is five percent or more of the annual total trading volume of all regulated DCMs may be appropriate, in light of the fact that smaller DCMs will still be required to conduct testing of all the types addressed in the proposed rule pursuant to the existing DCM system safeguards rules.

In order to provide certainty to all DCMs concerning whether the testing frequency and independent contractor provisions of the propose rule would apply to them, it is necessary for the Commission to receive annually from each DCM, beginning in 2016, its annual total trading volume for the preceding year, and to notify each DCM annually, beginning in 2016, 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. The proposed rule therefore would require each DCM to report its annual total trading volume for 2015 to the Commission within 30 calendar days of the effective date of the

[249] FINRA, *Report on Cybersecurity Practices,* February 2015, at 7, available at *https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf.*

[250] *Id.*

[251] *Id.* at 8.

[252] FFIEC, *Information Security IT Examination Handbook,* at 5, available at *http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_Information Security.pdf.*

[253] *Id. See also, e.g.,* NIST SP 800–53 Rev. 4, *Program Management (''PM'') control family,* available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.*

[254] FFIEC, *Audit IT Examination Handbook,* Objective 6, at A–4, available at *http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_Audit.pdf.*

[255] ISACA, COBIT 5, APO12, available at *https://cobitonline.isaca.org/.*

[256] *See, e.g.,* NIST SP 800–53A Rev. 4, at 3, available at *http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf*; FFIEC, *Audit IT Examination Handbook,* Objective 6, at A–4, available at *http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_Audit.pdf.*

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.[257]

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

The Commission is considering proposing, by means of a future NPRM, that the most systemically important SEFs should be subject to the same new minimum testing frequency requirements proposed in this NPRM for covered DCMs and SDRs. It is also considering proposing, by means of a future NPRM, that the most systemically important SEFs should be subject to the same independent contractor testing requirements proposed in this NPRM for covered DCMs and SDRs. Accordingly, by means of this concluding section of the preamble and the related set of questions and requests for comment at the conclusion of the Requests for Comment section, the Commission is issuing an Advance Notice of Proposed Rulemaking (''ANPRM'') with respect to these subjects.

As discussed above, the Commission believes that, in light of the current cyber threat environment, the minimum frequency requirements and independent contractor testing requirements proposed in this NPRM for covered DCMs and SDRs are necessary and appropriate for ensuring the cybersecurity and resiliency of such entities, and are essential to the effectiveness of their cybersecurity testing and the adequacy of their programs of system safeguards risk analysis and oversight. As noted above, these requirements are grounded in generally accepted standards and best practices.[258] The Commission also believes, as discussed above, that the independent contractor testing requirements proposed in this NPRM for covered DCMs and SDRs will appropriately strengthen the objectivity and reliability of the testing, assessment, and information available to the Commission regarding covered DCM and SDR system safeguards.

For the same reasons, the Commission believes that it is appropriate and necessary to consider applying these same minimum testing frequency and independent contractor testing requirements to the most systemically important SEFs. The Commission is aware that at this time SEFs are new CFTC-regulated entities still awaiting final registration by the Commission, and that the SEF market is still in an early stage of development. Nevertheless, the Commission believes that SEFs that trade swaps with significant notional value or that trade significant numbers of swaps may have become systemically important enough that such requirements for them may now have become essential, in light of today's cybersecurity threat environment (discussed above), the importance of the swap market to the U.S. economy, as recognized by the Dodd-Frank Act, and the notional value and volume of swaps traded on larger SEFs or pursuant to their rules.

Preliminarily, the Commission believes it is appropriate to consider defining the ''covered SEFs'' to which these requirements would be applied as those SEFs for which the annual total notional value of all swaps traded on or pursuant to the rules of the SEF is ten percent (10%) 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. This threshold would give SEFs that have less than ten percent of the annual total notional value of all swaps traded more flexibility regarding the testing they must conduct. As a matter of policy, the Commission believes it is appropriate to reduce possible costs and burdens for smaller entities when it is possible to do so consistent with achieving the fundamental goals of the Act and Commission rules. Accordingly, the Commission believes, preliminarily, that applying the minimum frequency and independent contractor requirements in this proposed rule only to SEFs that have ten percent or more of the annual total notional value of all swap traded would be appropriate, in light of the fact that smaller SEFs will still be required, pursuant to this current NPRM, to conduct testing of all the types clarified in the NPRM as essential to fulfilling the testing requirements of the existing SEF system safeguards rules. The Commission also notes that, under this current NPRM and the parallel NPRM being issued with respect to DCOs, a non-covered SEF that shares common ownership and automated systems with a DCO, a covered DCM, or an SDR would in practice fulfill the testing frequency and independent contractor testing requirements by virtue of sharing automated systems and system safeguards with the DCO, covered DCM, or SDR.

However, the Commission will also consider whether it would be more appropriate to define ''covered SEF'' in terms of annual total notional value of swaps traded, or in terms of annual total number of swaps traded, and how notional value would best be defined in this context. It will also consider what percentage share of the annual total notional value of all swaps traded on all SEFs regulated by the Commission, or of the annual total number of swaps traded, should be used to define ''covered SEF.'' It will further consider whether it would be more appropriate for the definition to be applied with respect to the notional value or the number of swaps in each asset class separately, or to be applied with respect to the notional value or the number of all swaps combined regardless of asset class.

Accordingly, in the final part of the Request for Comment section below, the Commission is seeking comments regarding each of these considerations. The Commission will consider all such comments in determining what definition of ''covered SEF'' it should propose in a future NPRM on this subject, if such a proposal is made. The Commission is also seeking information relating to the possible costs and benefits of applying the minimum testing frequency and independent contractor testing requirements to covered SEFs, and how such benefits or costs could be quantified or estimated. In addition, the Commission seeks additional information regarding the extent to which SEFs are currently meeting these requirements. Finally, the Commission seeks additional information concerning the most appropriate method for SEFs to report annually to the Commission their annual total notional value of swaps traded or their annual total number of swaps traded.

II. Related Matters

A. Regulatory Flexibility Act

The Regulatory Flexibility Act (''RFA'') requires that agencies consider whether the regulations they propose will have a significant economic impact on a substantial number of small entities and, if so, provide a regulatory flexibility analysis respecting the impact.[259] The rules proposed by the Commission will impact DCMs, SEFs, and SDRs. The Commission has

[257] The SEC's Regulation SCI, issued in final form in December 2014, employs similar methodology to distinguish in some cases which entities are subject to SCI review requirements. Regulation SCI uses percentages of average daily dollar volume of stock trading to determine whether alternative trading systems are subject to Regulation SCI as SCI entities.

[258] *See* discussion above concerning the need for cybersecurity testing.

[259] 5 U.S.C. 601 *et seq.*

previously established certain definitions of ''small entities'' to be used by the Commission in evaluating the impact of its regulations on small entities in accordance with the RFA.[260] The Commission has previously determined that DCMs, SEFs, and SDRs are not small entities for the purpose of the RFA.[261] Therefore, the Chairman, on behalf of the Commission pursuant to 5 U.S.C. 605(b), certifies that the proposed 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'')[262] imposes certain requirements on Federal agencies, including the Commission, in connection with their conducting or sponsoring any collection of information, as defined by the PRA. An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid control number. This proposed rulemaking contains recordkeeping and reporting requirements that are collections of information within the meaning of the PRA.

The proposed rulemaking contains provisions that would qualify as collections of information, for which the Commission has already sought and obtained control numbers from the Office of Management and Budget (''OMB''). The titles for these collections of information are ''Part 38–Designated Contract Markets'' (OMB Control Number 3038–0052), ''Part 37–Swap Execution Facilities'' (OMB Control Number 3038–0074), and ''Part 49–Swap Data Repositories; Registration and Regulatory Requirements'' (OMB Control Number 3038–0086). If adopted, responses to these collections of information would be mandatory. As discussed below, with the exception of proposed § 38.1051(n) that would require all DCMs to submit annual trading volume information to the Commission, the Commission believes the proposal will not impose any new recordkeeping or reporting requirements that are not already accounted for in existing collections 3038–0052,[263] 3038–0074,[264] and 3038–0086.[265] Accordingly, the Commission invites public comment on the accuracy of its estimate regarding the impact of proposed § 38.1051(n) on collection 3038–0052 and its determination that no additional recordkeeping or information collection requirements or changes to existing collection requirements would result from the proposal.

The Commission will protect proprietary information according to the Freedom of Information Act (''FOIA'') and 17 CFR part 145, ''Commission Records and Information.'' In addition, section 8(a)(1) of the Act strictly prohibits the Commission, unless specifically authorized by the Act, from making public ''data and information that would separately disclose the business transactions or market positions of any person and trade secrets or names of customers.'' The Commission is also required to protect certain information contained in a government system of records according to the Privacy Act of 1974.

2. Clarification of Collections 3038–0052, 3038–0074, and 3038–0086

The Commission notes that all DCMs, SEFs, and SDRs are already subject to system safeguard-related books and records obligations. However, with the exception of business continuity-disaster recovery testing, the records relating to a particular system safeguard test or assessment are not explicitly addressed in the current rules. Therefore, as discussed above in Section I.E., the Commission is proposing to 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 proposed regulations would require these entities, in accordance with Commission regulation § 1.31,[266] 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 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 pertinent recordkeeping and reporting requirements of proposed § 38.1051(g) are contained in the provisions of current Commission regulations §§ 38.1051(g)[267] and (h),[268] which were adopted on June 19, 2012 (''DCM Final Rules'').[269] In the DCM Final Rules, the Commission estimated that each respondent subject to the part 38 requirements would experience a 10 percent increase, or 30 additional hours, in the information collection burden as a result of the regulations implementing certain core principles, including Core Principle 20 (System Safeguards).[270] The pertinent recordkeeping and reporting burdens of proposed § 37.1401(g) are contained in the provisions of current Commission regulations §§ 37.1041(f)[271] and (g),[272]

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

[261] *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.

[262] 44 U.S.C. 3501 *et seq.*

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

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

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

[266] Commission regulation § 1.31(a)(1) specifically provides that ''all 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.'' The rule further provides that ''all such books and records shall be open to inspection by any representative of the Commission or the United States Department of Justice.'' *See* 17 CFR 1.31(a)(1).

[267] Commission regulation § 38.1051(g) specifically provides that ''a designated contract market must provide to the Commission upon request current copies of the business-continuity disaster recovery plan and other emergency procedures, its assessments of its operational risks, and other documents requested by Commission staff for the purpose of maintaining a current profile of the designated contract market's systems.'' *See* 17 CFR 38.1051(g).

[268] Commission regulation § 38.1051(h) specifically provides that ''a designated contract market must conduct regular, periodic, objective testing and review of its automated systems to ensure that they are reliable, secure, and have adequate scalable capacity. It must also conduct regular, periodic testing and review of its business continuity-disaster recovery capabilities.'' The regulation further provides that ''pursuant to Core Principle 18 (Recordkeeping) and §§ 38.950 and 38.951, the designated contract market must keep records of all such tests, and make all test results available to the Commission upon request.'' *See* 17 CFR 38.1051(h).

[269] 77 FR 36612 (June 19, 2012).

[270] 77 FR 36664–65 (June 19, 2012).

[271] Commission regulation § 37.1401(f) specifically provides that a swap execution facility shall provide to the Commission, upon request, current copies of its business continuity-disaster recovery plan and other emergency procedures, its assessments of its operational risks, and other documents requested by Commission staff for the purpose of maintaining a current profile of the swap execution facility's automated systems. *See* 17 CFR 37.1401(f).

[272] Commission regulation § 37.1401(g) specifically provides that a swap execution facility shall conduct regular, periodic, objective testing and review of its automated systems to ensure that

which were adopted on June 4, 2103 (''SEF Final Rules'').[273] In the SEF Final Rules, the Commission estimated that each respondent subject to the part 37 requirements would incur a collection burden of 308 hours annually as a result of the regulations implementing certain core principles, including Core Principle 14 (System Safeguards).[274] Additionally, the pertinent recordkeeping and reporting requirements of proposed § 49.24(i) are contained in the provisions of current Commission regulations §§ 49.24(i) [275] and (j),[276] which were adopted on September 1, 2011 (''SDR Final Rules'').[277] In the SDR Final Rules, the Commission determined that the collection burdens created by the Commission's proposed rules, which were discussed in detail in the proposing release, are identical to the collective burdens of the final rules.[278] The Commission estimated in the proposing release that the total ongoing annual burden for all of the § 49.24 requirements is 15,000 burden hours per respondent.[279] The Commission believes that proposed §§ 38.1051(g) and 49.24(i) would not impact the burden estimates currently provided for in OMB Control Numbers 3038–0052, 3038–0074, and 3038–0086.

3. Proposed Revision to Collection 3038–0052

Proposed § 38.1051(n) would require all DCMs to provide to the Commission for calendar year 2015, and each calendar year thereafter, its annual total trading volume. This information would be required 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. 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. Consequently, the Commission believes that any burden incurred by the DCMs as a result of proposed § 38.1051(n) would be minimal. Presently, there are 15 registered DCMs that would be required to comply with proposed § 38.1051(n) and the burden hours for this collection have been estimated as follows:

Estimated number of respondents: 15.

Annual responses by each respondent: 1.

Total annual responses: 15.

Estimated average hours per response: 0.5.

Aggregate annual reporting burden: 7.5.

With the respondent burden for this collection estimated to average 0.5 hours per response, the total annual cost burden per respondent is estimated to be $22.015. The Commission based its calculation on an hourly wage rate of $44.03 for a Compliance Officer.[280]

4. Information Collection Comments

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

Copies of the submission from the Commission to OMB are available from the CFTC Clearance Officer, 1155 21st Street NW., Washington, DC 20581, (202) 418–5160 or from *http://RegInfo.gov*. Persons desiring to submit comments on the proposed information collection requirements should send those comments to: The Office of Information and Regulatory Affairs, Office of Management and Budget, Room 10235, New Executive Office Building, Washington, DC 20503, Attention: Desk Officer of the Commodity Futures Trading Commission; (202) 395–6566 (fax); or *OIRAsubmissions@omb.eop.gov* (email). Please provide the Commission with a copy of submitted comments so that all comments can be summarized and addressed in the final rulemaking, and please refer to the **ADDRESSES** section of this rulemaking for instructions on submitting comments to the Commission. OMB is required to make a decision concerning the proposed information collection requirements between thirty (30) and sixty (60) days after publication of the Proposal in the **Federal Register**. Therefore, a comment to OMB is best assured of receiving full consideration if OMB (as well as the Commission) receives it within thirty (30) days of publication of the Proposal.

C. Consideration of Costs and Benefits

1. Introduction

Section 15(a) of the CEA requires the Commission to consider the costs and benefits of its actions before promulgating a regulation under the CEA or issuing certain orders.[281] Section 15(a) further specifies that the costs and benefits shall be evaluated in light of five broad areas of market and public concern: (1) Protection of market participants and the public; (2) efficiency, competitiveness, and financial integrity of futures markets; (3) price discovery; (4) sound risk management practices; and (5) other public interest considerations. The Commission considers below the costs and benefits resulting from its discretionary determinations with respect to the section 15(a) factors.

As an initial matter, the Commission considers the incremental costs and benefits of these regulations, that is the

they are reliable, secure, and have adequate scalable capacity. A swap execution facility shall also conduct regular, periodic testing and review of its business continuity-disaster recovery capabilities. The rule further provides that pursuant to Core Principle 10 under section 5h of the Act (Recordkeeping and Reporting) and §§ 37.1000 through 37.1001, the swap execution facility shall keep records of all such tests, and make all test results available to the Commission upon request. *See* 17 CFR 37.1401(g).

[273] 78 FR 33476 (June 4, 2013).

[274] 78 FR 33551 (June 4, 2013).

[275] Commission regulation § 49.24(i) specifically provides that a registered swap data repository shall provide to the Commission upon request current copies of its business continuity and disaster recovery plan and other emergency procedures, its assessments of its operational risks, and other documents requested by Commission staff for the purpose of maintaining a current profile of the swap data repository's automated systems. *See* 17 CFR 49.24(i).

[276] Commission regulation § 49.24(j) specifically provides that a registered 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. The rule further provides that pursuant to §§ 1.31, 49.12 and 45.2 of the Commission's Regulations, the swap data repository shall keep records of all such tests, and make all test results available to the Commission upon request. *See* 17 CFR 49.24(j).

[277] 76 FR 54538 (Sept. 1, 2011).

[278] 76 FR 54572 (Sept. 1, 2011).

[279] 75 FR 80924 (Dec. 23, 2010).

[280] 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 (2014 Report). The hourly rate for a Compliance Officer in the Securities and Commodity Exchanges as published in the 2014 Report was $44.03 per hour.

[281] 7 U.S.C. 19(a).

costs and benefits that are not already present in the current system safeguard practices and requirements under the Act and the Commission's regulations for DCMs, SEFs, and SDRs. Where reasonably feasible, the Commission has endeavored to estimate quantifiable costs and benefits. Where quantification is not feasible, the Commission identifies and describes costs and benefits qualitatively.[282]

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

2. Background and Baseline for the Proposal

As discussed above in Section I.A., the Commission believes that the current cyber threats to the financial sector, including DCMs, SEFs, and SDRs regulated by the Commission, have expanded over the course of recent years. According to the Committee on Payments and Market Infrastructures of the Bank for International Settlements, ''Cyber attacks against the financial system are becoming more frequent, more sophisticated and more widespread.'' [283] A survey of 46 global securities exchanges conducted by IOSCO and the WFE found that as of July 2013, over half of exchanges world-wide had experienced a cyber attack during the previous year.[284] The Ponemon Institute 2015 Cost of Data Breach Study, which included 350 companies, found that the average cost of a data breach is $3.79 million, which represents a 23 percent increase from the 2014 study.[285] Moreover, the study concluded that the consequences of lost business are having a greater impact on the cost of a data breach with the average cost increasing from $1.33 million last year to $1.57 million this year.[286] Accordingly, the current cyber threat environment highlights the need to consider an updated regulatory framework with respect to cybersecurity testing for DCMs, SEFs, and SDRs. Although the Commission acknowledges that the proposal would likely result in some additional costs, particularly for some covered DCMs and SDRs, the proposal would also bring several overarching benefits to the futures and swaps industry. A comprehensive cybersecurity testing program is important to efforts by the regulated entities to harden cyber defenses, to mitigate operations, reputation, and financial risk, and to maintain cyber resilience and ability to recover from cyber attack.[287] Significantly, to ensure the effectiveness of cybersecurity controls, a financial sector entity must test in order to find and fix its vulnerabilities before an attacker exploits them.

The Commission recognizes that any economic effects, including costs and benefits, should be compared to a baseline that accounts for current regulatory requirements. The baseline for this cost and benefit consideration is the set of existing requirements under the Act and the Commission's regulations for DCMs, SEFs, and SDRs. As discussed in the preamble, 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.[288] The Act also 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.[289] The Commission's existing 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.[290]

As discussed above, the Commission proposes to clarify the system safeguards and cybersecurity testing requirements of its existing rules 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. Each of the types of testing and assessment that would be required under the proposed rule—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, as discussed above and discussed in detail below. Moreover, the Commission believes, as the generally accepted standards and best practices noted in this NPRM make it clear, that it would be essentially impossible for a DCM, SEF, or SDR to fulfill its existing 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 proposed rule. 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 issuing this NPRM.[291] Accordingly, as

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

[283] Committee on Payments and Market Infrastructures of the Bank for International Settlements, *Cyber resilience in financial market infrastructures* (November 2014), at 1.

[284] IOSCO and WFE, *Cyber-crime, securities markets and systemic risk,* Staff Working Paper (SWP2/2013) (July 16, 2013), at 3, available at *http://www.iosco.org/research/pdf/swp/Cyber-Crime-Securities-Markets-and-Systemic-Risk.pdf.*

[285] Ponemon Institute Research Report sponsored by IBM, *2015 Cost of Data Brach Study: Global Analysis* (May 2015), at 1.

[286] *Id.* at 2. The cost component includes the abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill. The growing awareness of identity theft and customers' concerns about the security of their personal data following a breach has contributed to the lost business.

[287] CFTC Roundtable, at 24.

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

[289] *Id.*

[290] 17 CFR 38.1051(h) (for DCMs); 17 CFR 37.1401(g) (for SEFs); 17 CFR 49.24(j) (for SDRs).

[291] The Commission's existing 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 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

discussed below in this consideration of costs and benefits section, the Commission believes that, with the exception of the minimum testing frequency and independent contractor requirements for covered DCMs and SDRs, the proposed rules calling for each DCM, SEF, and SDR to conduct each of these types of testing and assessment will not impose any new costs on DCMs, SEFs, and SDRs. If compliance with the clarified testing requirements proposed herein results in costs to DCMs, SEFs, and SDRs, the Commission believes that those are costs associated with compliance with existing testing requirements and not the proposed rules.

To assist the Commission in its understanding of the current system safeguard practices at DCMs and SDRs, Commission staff collected some 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'').[292] Some of the cost estimates provided by the DCMs and SDRs included estimates at the parent company level of the DCM and SDR as the entities were unable to apportion the actual costs to a particular entity within their corporate structure, within which entities may share the same automated systems and system safeguard programs. 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 is difficult in some cases to distinguish between the system safeguard-related costs of DCMs, SEFs, SDRs, and DCOs. In light of the above factors, the cost estimates discussed below are simple cost averages of the affected entities' estimates, without regard to the type of entity.[293] The data from the DMO Preliminary Survey, information received by Commission staff in administering the Commission's system safeguard program,[294] and information the Commission received during the CFTC Roundtable on March 18, 2015, are reflected below in the Commission's effort to estimate the costs and benefits of the proposal.

As noted above, and discussed more fully below, the Commission believes that to the extent that the proposal will impose additional costs, such costs will primarily impact covered DCMs (as defined) and SDRs as a result of the minimum testing frequency and independent contractor requirements.[295] The Commission expects that the costs and benefits may vary somewhat among the covered DCMs and SDRs. In this same regard, the Commission notes that some covered DCMs and SDRs are larger or more complex than others, and the proposed requirements may impact covered DCMs and SDRs differently depending on their size and the complexity of their systems.[296] The Commission recognizes 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 in which they choose to implement compliance with the proposed new requirements. The Commission is sensitive to the economic effects of the proposed regulations, including costs and benefits. Accordingly, the Commission seeks comment on the costs and benefits associated with the proposed regulations, including, where possible, quantitative data.

While certain costs are amenable to quantification, other costs are not easily estimated, such as the costs to the public or market participants in the event of a cybersecurity incident at a DCM, SEF, or SDR. The public interest is served by these critical infrastructures performing their functions. The Commission's proposed 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. Although the benefits of effective regulation are difficult to estimate in dollar terms, the Commission believes that they are of equal importance in light of the Commission's mandate to protect market participants and the public and to promote market integrity.

The discussion of costs and benefits that follows begins with a summary of each proposed regulation and a consideration, where appropriate, of the corresponding costs and benefits. At the conclusion of this discussion, the Commission considers the costs and benefits of the proposed regulations collectively in light of the five factors set forth in section 15(a) of the CEA.

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

a. Summary of Proposed Rules

As discussed above in Section I.B., the proposed rules would, among other things, add enterprise risk management and governance to the list of required categories of system safeguards-related risk analysis and oversight.

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*.

[292] The Commission notes that the DCMs and SDRs that provided the information for the DMO Preliminary Survey requested confidential treatment. Additionally, because the Commission's cost estimates are only based on preliminary data from some DCMs and SDRs, the Commission is including questions throughout the consideration of costs and benefits section for commenters to provide the Commission with specific cost estimates regarding the proposed rules.

[293] By definition, averages are meant to serve only as a reference point; the Commission understands that due to the nature of the proposed 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.

[294] Commission staff conduct system safeguard examinations (''SSEs'') to evaluate DCMs' compliance with Core Principle 20 (System Safeguards) and Commission regulations §§ 38.1050 and 38.1051. *See* 17 CFR 38.1050 and 38.1051. With respect to SDRs, Commission staff conduct SSEs to evaluate SDRs' compliance with Commission regulation § 49.24. *See* 17 CFR 49.24.

[295] The Commission believes that the proposed requirement in §§ 38.1051(c), 37.1041(c), and 49.24(d) that would require all DCMs (covered and non-covered), SEFs, and SDRs to update BC–DR plans and emergency procedures no less frequently than annually will impose new costs relative to the current requirements. Additionally, the proposed provisions that would make it mandatory for such entities to follow best practices, ensure tester independence, and coordinate BC–DR plans will also impose new costs relative to the current requirements. The Commission also expects that all DCMs will incur additional costs as a result of proposed requirement in § 38.1051(n) for the reporting of annual trading volume to the Commission.

[296] Based on information obtained from the DMO Preliminary Survey and the Commission's system safeguard compliance program, the Commission understands that most covered DCMs and SDRs currently conduct system safeguard testing at the proposed minimum frequency for most of the five tests in the proposal. Additionally, the Commission understands that most covered DCMs and SDRs currently engage independent contractors for the testing required by the proposal.

b. Costs and Benefits

As discussed in the preamble, the Commission believes that enterprise risk management and governance is implicit in the Commission's existing system safeguard regulations, which already require each DCM, SEF, and SDR to maintain a program of risk analysis and oversight with respect to system safeguards.[297] The proposed rules would make enterprise risk management and governance an explicitly listed category for the sake of clarity. The Commission believes that this clarification will not impose any new costs for DCMs, SEFs, and SDRs.

4. Requirements to Follow Best Practices, Ensure Testing Independence, and Coordinate BC–DR Plans: Sections for Best Practices—38.1051(b); 37.1401(b); and § 49.24(c). Sections for Tester Independence—38.1051(h)(2)(iv), (3)(i)(C), (3)(ii)(B), (4)(iii), (5)(iv), and (6)(ii); 37.1401(h)(2)(i), (3)(i)(A), (4)(i), (5)(iii), and (6)(i); and 49.24(j)(2)(iii), (3)(i)(B), (4)(ii), (5)(iv), and (6)(ii). Sections for BC–DR Plans—38.1051(i); § 37.1401(i); and § 49.24(k)

a. Summary of Proposed Rules

As discussed above in Section I.C., the proposed rules would make the existing provisions with respect to following best practices, ensuring tester independence, and coordinating BC–DR plans mandatory for DCMs, SEFs, and SDRs.

b. Costs

As discussed in the preamble, the Commission's existing 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.[298] They 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 systems or capabilities being tested).[299] They further provide that such entities should coordinate their BC–DR plans with the BC–DR plans of market participants and essential service providers.[300] In light of the language in the proposed rules that would make these provisions mandatory, the proposed rules will impose new costs relative to the current requirements. However, the Commission does not have quantification or estimation of these potential costs.

c. Benefits

Making the provisions 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. The Commission believes that in today's cybersecurity threat environment, following generally accepted standards and best practices, ensuring tester independence, and coordinating BC–DR plans appropriately are essential to adequate system safeguards and cyber resiliency for DCMs, SEFs, and SDRs. The Commission also believes that clarity concerning necessary requirements in these respects will benefit DCMs, SEFs, and SDRs, their market participants and customers, and the public interest.

d. Request for Comments

The Commission requests comment on the potential costs and benefits associated with the proposed provisions that would make it mandatory for DCMs, SEFs, and SDRs to follow best practices, ensure tester independence, and coordinate BC–DR plans, including, where possible, quantitative data.

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

a. Summary of Proposed Rules

As discussed above in Section I.D., the proposed rules would 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.

b. Costs

The Commission's existing 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.[301] The proposed rules will impose new costs relative to the requirements of the current rules.[302] However, the Commission does not have quantification or estimation of these potential costs.

c. 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 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.'' [303]

d. Request for Comments

The Commission requests comment on the potential costs and benefits associated with complying with proposed regulations §§ 38.1051(c), 37.1401(c), and 49.24(d), including, where possible, quantitative data.

6. Required system safeguards-related books and records obligations: Sections 38.1051(g), 37.1041(g), and 49.24(i)

a. Summary of Proposed Rules

As discussed above in Section I.E., proposed §§ 38.1051(g), 37.1401(g), and 49.24(i) would require a DCM, SEF, or SDR, in accordance with Commission regulation § 1.31,[304] to provide the Commission with the following system safeguards-related books and records promptly upon request of any

[297] 17 CFR 38.1050(a) (for DCMs); 17 CFR 37.1400(a) (for SEFs); and 17 CFR 49.24(a)(1) (for SDRs).

[298] *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).

[299] *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).

[300] *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).

[301] 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).

[302] 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.

[303] 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.*

[304] Commission regulation § 1.31(a)(1) specifically provides that ''all 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.'' The rule further provides that ''all such books and records shall be open to inspection by any representative of the Commission or the United States Department of Justice.'' *See* 17 CFR 1.31(a)(1).

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

b. Costs

As discussed more fully above in the PRA section, all DCMs, SEFs, and SDRs are already subject to system safeguard-related books and records requirements. However, with the exception of BC–DR testing, the records relating to a particular system safeguard test or assessment are not explicitly addressed in the current rules. Therefore, the Commission is proposing §§ 38.1051(g), 37.1401(g), and 49.24(i) to clarify the system safeguard recordkeeping and reporting requirements for these entities. The Commission notes that the pertinent recordkeeping and reporting requirements of proposed § 38.1051(g) are contained in the provisions of current Commission regulations §§ 38.1051(g) and (h). The pertinent recordkeeping and reporting requirements of proposed § 37.1041(g) are contained in the provisions of current §§ 37.1041(f) and (g). In addition, the pertinent recordkeeping and reporting requirements of proposed § 49.24(i) are contained in the provisions of current Commission regulations §§ 49.24(i) and (j). Because the production of system-safeguard records is already required by the current rules, the Commission believes that the proposed rules would not impose any additional costs on DCMs, SEFs, and SDRs.

c. Benefits

The recordkeeping requirements for DCMs, SEFs, and SDRs allow the Commission to fulfill its oversight role and 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 efficient examinations of DCMs, SEFs, and SDRs, and increase the likelihood that Commission staff may identify conduct inconsistent with the requirements. 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 the DCMs, SEFs, and SDRs.

7. Definitions: Sections 38.1051(h)(1), 37.1041(h)(1), and 49.24(j)(1)

a. Summary of Proposed Rules

Proposed §§ 38.105(h)(1), 37.1041(h)(1), and 49.24(j)(1) would 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) would include the definition for covered designated contract market.

b. Costs and Benefits

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

8. Vulnerability Testing: Sections 38.1051(h)(2), 37.1401(h)(2), and 49.24(j)(2)

a. Summary of Proposed Rules

As discussed above in Section I.F.3., proposed §§ 38.1051(h)(1), 37.1401(h)(1), and 49.24(j)(1) would 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. The proposed rules would require a DCM, SEF, or SDR to conduct vulnerability testing that is sufficient to satisfy the testing scope requirements in proposed §§ 38.1051(k), 37.1401(k), and 49.24(l), at a frequency determined by an appropriate risk analysis. Vulnerability testing would include automated vulnerability scanning, with some such scanning to be conducted on an authenticated basis (*e.g.,* using log-in credentials). Where scanning is conducted on an unauthenticated basis, implementation of effective compensating controls would be required. At a minimum, covered DCMs and SDRs would be required to conduct vulnerability testing no less frequently than quarterly. Covered DCMs and SDRs would be required to engage independent contractors to perform two of the required quarterly tests each year, although the entity could have other vulnerability testing conducted by employees not responsible for development or operation of the systems or capabilities being tested.

b. Costs

1. Vulnerability Testing Requirement for All DCMs, SEFs, and SDRs

As discussed in the preamble, 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.[305] 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.[306]

The Commission's existing 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.[307] The Commission believes, as the generally accepted standards and best practices noted in this NPRM make clear, that it would be essentially impossible for a DCM, SEF, or SDR to fulfill its existing obligation to conduct testing sufficient to ensure the reliability, security, and capacity of its automated systems without conducting vulnerability testing. The proposed rules clarify the existing testing requirements by specifying vulnerability testing as a necessary component. The Commission believes that this has always been the case.[308] If compliance with the existing testing requirements as clarified by the proposed 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 would be attributable to compliance with the

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

[306] *Id.*

[307] 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).

[308] *See supra* note 291.

existing regulations and not to the proposed rules. Accordingly, the Commission believes that this clarification will not impose any new costs for DCMs, SEFs, and SDRs.

2. Minimum Vulnerability Testing Frequency Requirements for Covered DCMs and SDRs

As discussed above, the proposed rules would require covered DCMs and SDRs to conduct vulnerability testing no less frequently than quarterly.[309] The current rules require DCMs and SDRs to conduct regular, periodic, objective testing of their automated systems.[310] Accordingly, the proposed rules will impose new costs relative to the requirements of the current rules.[311] The Commission notes that the proposed frequency comports with industry best practices.[312]

3. Independent Contractor Requirement for Covered DCMs and SDRs

As discussed above, the proposed rules would require at least two of the required quarterly vulnerability tests each year to be conducted by an independent contractor. Current regulations §§ 38.1051(h) and 49.24(j) provide that testing of automated systems should be conducted by qualified, independent professionals.[313] 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 proposed independent contractor requirement will impose new costs relative to the requirements of the current rules.[314] The Commission notes that best practices also support the use of independent contractors to conduct vulnerability testing.[315]

4. Cost Estimates for Covered DCMs and SDRs

The Commission's preliminary cost estimate for vulnerability testing, based on data collected from the DMO Preliminary Survey, suggests that on average, a covered DCM or SDR currently spends approximately $3,495,000 annually.[316] The data also suggests that with respect to the entities that currently use independent contractors to conduct vulnerability testing, a covered DCM or SDR spends approximately $71,500 to hire an independent contractor to conduct one vulnerability test annually and $143,000 to conduct two tests annually. In providing these estimates, 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 any vulnerability tests, the Commission expects that such entities may also 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 effective and appropriate. Moreover, although the Commission believes that all covered DCMs and SDRs have substantial policies and procedures in place for vulnerability testing conducted by internal staff, the Commission acknowledges that affected entities who do not already use independent contractors for some vulnerability testing may need to dedicate time to reviewing and revising their existing policies and procedures to ensure that they are sufficient in the context of the proposed requirements. The Commission believes that any costs incurred by the entities as result of such review would be minor.

c. Benefits

Vulnerability testing identifies, ranks, and reports vulnerabilities that, if exploited, may result in an intentional or unintentional compromise of a system.[317] 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 *ex ante* understanding by the DCM's, SEF's, or SDR's management of the challenges the entity would face in a cyber threat scenario, and thus better preparation to meet those challenges. This improved preparation in turn 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, a DCM's, SEF's, or SDR's operations would have on market participants, parties required by the Act or Commission regulations to report swaps data to SDRs, 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 proposed 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

[309] While the existing 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 would avoid applying the addition minimum frequency requirements to non-covered DCMs in order to give smaller markets with fewer resources somewhat more flexibility regarding the testing they must conduct. The Commission believes that such a reduced burden for smaller DCMs may be appropriate, in light of the fact that they will still be required to conduct such testing and assessments, and to have security incident response plans, pursuant to the existing system safeguards rules for DCMs.

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

[311] Based on the information collected in the DMO Preliminary Survey, the Commission understands that most covered DCMs and SDRs currently conduct vulnerability testing at the proposed frequency.

[312] PCI DSS standards, 11.2, at 94, available at *https://www.pcisecuritystandards.org/security_standards/index.php.*

[313] *Id.*

[314] Based on the information collected in the DMO Preliminary Survey, the Commission understands that some covered DCMs and SDRs may not be engaging independent contractors at all, or may not be engaging such contractors at a frequency that would satisfy proposed frequency requirement.

[315] *See* CFTC Roundtable, at 88–89; NIST SP 800–115, at 6–6, available at *http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf*; FFIEC, *Information Security IT Examination Handbook,* at 81, available at *http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_InformationSecurity.pdf*; PCI–DSS Version 3.1, Requirement 11, *Regularly test security systems and processes,* at 94–96, available at *https://www.pcisecuritystandards.org/security_standards/index.php.*

[316] During the CFTC Roundtable, one of the participants noted the difficulty in providing cost estimates for vulnerability and penetration testing, but emphasized that vulnerability testing is generally automated while penetration testing is usually more manual. See CFTC Roundtable, at 98.

[317] *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.*

organization and reduce the likelihood that attackers could exploit vulnerabilities. Best practices 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.[318] Moreover, the Commission believes that the proposed frequency requirement will give additional clarity to covered DCMs and SDRs concerning what is required of them in this respect.

As noted above, the proposed rules would also require covered DCMs and SDRs to engage independent contractors to conduct two of the required quarterly vulnerability tests each year, while providing covered DCMs and SDRs with the flexibility to conduct other vulnerability testing using employees not responsible for development or operation of the systems or capabilities being tested. Consistent with the views shared by the panelists at the CFTC Roundtable, the Commission believes there are important benefits when a testing program includes both testing by independent contractors and testing by entity employees not responsible for building or operating the system being tested. One participant in the CFTC Roundtable noted, ''[t]here are advantages to both, but neither can stand alone.'' [319] Much testing needs to happen internally, but much also needs to be conducted from the viewpoint of an outsider, particularly where testing against the possible tactics or techniques of a particular threat actor is concerned.[320] With respect to testing conducted by entity employees, one benefit is that internal vulnerability testing and scanning can utilize viewpoints that the outside world would not have, based on intimate knowledge of the entity's network and systems.[321] An additional benefit provided by independent contractor testing comes from the outsider's different perspective, and his or her ability to look for things that entity employees may not have contemplated during the design or operation of the system involved.[322] The Commission also notes that best practices support having testing conducted by both independent contractors and entity employees.[323] Accordingly, the Commission believes the proposed rules are appropriate and would strike the appropriate balance between both entity employees and independent contractors conducting the vulnerability tests.

d. Request for Comments

As set out in more detail below in the Request for Comments section, the Commission seeks additional information regarding the costs and benefits of vulnerability testing, including the minimum testing frequency and independent contractor requirement, and the extent to which the proposed rules clarify the standard. The Commission particularly solicits comments concerning the need for vulnerability testing and the associated costs and benefits, from DCMs, SEFs, and SDRs, from futures and swap market participants, from best practices and standards organizations, from cybersecurity service providers and cybersecurity experts in both the private and public sectors, and from other financial regulators.

9. External Penetration Testing: Sections 38.1051(h)(3)(i), 37.1401(h)(3)(i), and 49.24(j)(3)(i)

a. Summary of Proposed Rules

As discussed above in Section I.F.4., proposed §§ 38.1051(h)(1), 37.1401(h)(1), and 49.24(j)(1) would 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. The proposed rules would require a DCM, SEF, or SDR to conduct external penetration testing that is sufficient to satisfy the scope requirements in proposed §§ 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 would be required to conduct external penetration testing no less frequently than annually. Covered DCMs and SDRs would also be required to engage independent contractors to perform the required annual external penetration test, although the entity could have other external penetration testing conducted by employees not responsible for development or operation of the systems or capabilities being tested.

b. Costs

1. External Penetration Testing for All DCMs, SEFs, and SDRs

As discussed in the preamble, 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.[324] 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.[325]

The Commission's existing 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.[326] The Commission believes, as the generally accepted standards and best practices noted in this NPRM make clear, that it would be essentially impossible for a DCM, SEF, or SDR to fulfill its existing obligation to conduct testing sufficient to ensure the reliability, security, and capacity of its automated systems without conducting external penetration testing.

The proposed rules clarify the existing testing requirements by specifying external penetration testing as a necessary component. The Commission believes it has always been the case.[327] If compliance with the existing testing requirements as clarified by the proposed 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 would be attributable to compliance with the existing regulations and not to the proposed rules. Accordingly, the Commission believes that this clarification will not impose any new costs for DCMs, SEFs, and SDRs.

[318] PCI DSS, Requirement 11.2 *Regularly test security systems and processes,* at 94, available at *https://www.pcisecuritystandards.org/security_standards/index.php.*

[319] CFTC Roundtable, at 88.

[320] *Id.* at 88–89.

[321] *Id.* at 177.

[322] *Id.* at 171.

[323] *See* NIST SP 800–115, at 6–6, available at *http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf*; FFIEC, *Information Security IT Examination Handbook,* at 81, available at *http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_InformationSecurity.pdf*; ISACA, COBIT 5, MEA02.05, *Ensure that assurance providers are independent and qualified,* available at *https://cobitonline.isaca.org/.*

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

[325] *Id.*

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

[327] *See supra* note 291.

2. Minimum External Penetration Testing Frequency Requirements for Covered DCMs and SDRs

As discussed above, the proposed rules would require covered DCMs and SDRs to conduct external penetration testing no less frequently than annually. The current rules require DCMs and SDRs to conduct regular, periodic, objective testing of their automated systems.[328] Therefore, the proposed rules will impose new costs relative to the requirements of the current rules.[329] The Commission notes that the proposed frequency requirement is consistent with industry best practices.[330]

3. Independent Contractor Requirement for Covered DCMs and SDRs

As discussed above, the proposed rules would require the annual external penetration test to be conducted by an independent contractor. Current regulations §§ 38.1051(h) and 49.24(j) provide that testing of automated systems should be conducted by qualified, independent professionals.[331] 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 proposed rules will impose new costs relative to the requirements of the current rules.[332] The Commission notes that best practices support using independent contractors to conduct external penetration testing.[333]

4. Cost Estimates for Covered DCMs and SDRs

Based on the cost information from the DMO Preliminary Survey, the Commission estimates that the average cost for a covered DCM or SDR to conduct external penetration testing annually is approximately $244,625. 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 also 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 effective and appropriate. The Commission acknowledges that covered DCMs and SDRs that currently do not use independent contractors for the external penetration test may need to dedicate time to reviewing and revising their existing policies and procedures to ensure that they are sufficient in the context of the proposed requirements. The Commission believes that any costs incurred by the entities as result of such review would be minor.

c. Benefits

The benefits for external penetration testing, including the minimum testing frequency and independent contractors, are discussed below in conjunction with the benefits for internal penetration testing.

d. Request for Comments

As set out in more detail below in the Request for Comments section, the Commission seeks additional information regarding the costs and benefits of external penetration testing, including the minimum testing frequency and independent contractor requirement. The Commission particularly solicits comments concerning the need for external penetration testing and the associated costs and benefits, from DCMs, SEFs, and SDRs, from futures and swap market participants, from best practices and standards organizations, from cybersecurity service providers and cybersecurity experts in both the private and public sectors, and from other financial regulators.

10. Internal Penetration Testing: Sections 38.1051(h)(3)(ii), 37.1401(h)(3)(ii), and 49.24(j)(3)(ii)

a. Summary of Proposed Rules

As discussed above in Section I.F.4., proposed §§ 38.1051(h)(1), 37.1401(h)(1), and 49.24(j)(1) would 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. The proposed rules would require a DCM, SEF, or SDR to conduct internal penetration testing that is sufficient to satisfy the scope requirements in proposed §§ 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 would be required to conduct the internal penetration testing no less frequently than annually. The DCM or SDR may engage independent contractors to conduct the test, or the entity may use employees of the DCM or SDR who are not responsible for development or operation of the systems or capabilities being tested.

b. Costs

1. Internal Penetration Testing for All DCMs, SEFs, and SDRs

As discussed in the preamble, 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.[334] 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.[335]

The Commission's existing 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.[336] The Commission believes, as the generally accepted standards and best practices noted in this NPRM make clear, that it would be essentially

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

[329] Based on the information collected in the DMO Preliminary Survey, the Commission understands that most covered DCMs and SDRs currently conduct external penetration testing at the proposed frequency.

[330] 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*.

[331] *Id.*

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

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

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

[335] *Id.*

[336] 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).

impossible for a DCM, SEF, or SDR to fulfill its existing obligation to conduct testing sufficient to ensure the reliability, security, and capacity of its automated systems without conducting internal penetration testing. The proposed rules clarify the existing testing requirements by specifying internal penetration testing as a necessary component. The Commission believes that this has always been the case.[337] If compliance with the existing testing requirements as clarified in the proposed 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 would be attributable to compliance with the existing regulations and not to the proposed rules. Accordingly, the Commission believes that this clarification will not impose any new costs on DCMs, SEFs, and SDRs.

2. Minimum Internal Penetration Testing Frequency Requirements for Covered DCMs and SDRs

As discussed above, the proposed rules would require covered DCMs and SDRs to conduct internal penetration testing no less frequently than annually. The current rules require DCMs and SDRs to conduct regular, periodic, objective testing of their automated systems.[338] Therefore, the proposed rules will impose new costs relative to the requirements of the current rules.[339] The Commission notes that the proposed frequency is consistent with industry best practices.[340]

3. Cost Estimates for Covered DCMs and SDRs

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. In providing these estimates, 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. Additionally, 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 would be minor.

c. Benefits

External penetration testing benefits DCMs, SEFs, and SDRs by identifying the extent to which its systems can be compromised before an attack is identified.[341] Such testing is conducted outside a DCM's, SEF's, or SDR's security perimeter to help reveal vulnerabilities that could be exploited by an external attacker. Accordingly, the Commission believes that the external penetration testing strengthens DCMs', SEFs', and SDRs' systems, thereby protecting not only the DCMs, SEFs, and SDRs, but also market participants and parties required by the Act or Commission regulations to report swaps data to the SDRs from a disruption in services, which could potentially disrupt the functioning of the broader financial markets.

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.'' [342] As discussed above in the costs section, the proposed rules would address the required minimum frequency for covered DCMs and SDRs in performing external and internal penetration testing. Best practices support 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.[343] 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.[344] 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.[345] The Commission believes the specified frequency levels would increase the likelihood that the affected entities will be adequately protected against the level of cybersecurity threat now affecting the financial sector. The Commission also notes that identifying and fixing vulnerabilities that could be exploited by adversaries would likely be a more cost effective alternative to dealing with a successful cyber attack.

With respect to external penetration testing, the proposed requirement for annual testing to be performed by independent contractors is intended to ensure that covered DCM and SDR programs of risk analysis and oversight with respect to system safeguards include the benefits provided when independent contractors perform such testing. The Commission shares the view expressed by participants in the CFTC Roundtable that vendor testing has particular value with respect to external penetration testing because the test comes from the viewpoint of an outsider and against the current tactics, techniques, and threat vectors of current threat actors as revealed by current threat intelligence.

d. Request for Comments

As set out in more detail below in the Request for Comments section, the Commission seeks additional information regarding the costs and benefits of internal penetration testing, including the minimum testing frequency requirement. The Commission particularly solicits comments concerning the need for internal penetration testing and the associated costs and benefits, from DCMs, SEFs, and SDRs, from futures and swap market participants, from best

[337] *See supra* note 291.

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

[339] Based on the information from the DMO Preliminary Survey, the Commission understands that most covered DCMs and SDRs currently conduct internal penetration testing at the proposed frequency.

[340] PCI DSS standards, at 96–97, available at *https://www.pcisecuritystandards.org/security_standards/index.php.*

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

[342] 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.*

[343] 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.*

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

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

practices and standards organizations, from cybersecurity service providers and cybersecurity experts in both the private and public sectors, and from other financial regulators.

11. Controls Testing: Sections 38.1051(h)(4), 37.1401(h)(4), and 49.24(j)(4)

a. Summary of Proposed Rules

As discussed above in Section I.F.5., proposed §§ 38.1051(h)(1), 37.1401(h)(1) and 49.24(j)(1) would 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. The proposed rules would require a DCM, SEF, or an SDR to conduct controls testing that is sufficient to satisfy the scope requirements in proposed §§ 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 would be required to conduct the controls testing no less frequently than every two years. The testing may be conducted on a rolling basis over the course of the minimum two-year period or over a minimum period determined by an appropriate risk analysis. The covered DCM and SDR must engage independent contractors to test and assess the key controls in the entity's risk analysis and oversight, no less frequently than every two years. The entities may conduct any other controls testing required by §§ 38.1051(h)(4) and 49.24(j)(4) by using either independent contractors or employees of the covered DCM or SDR who are not responsible for the development or operations of the systems or capabilities being tested.

b. Costs

1. Controls Testing for All DCMs, SEFs, and SDRs

As discussed in the preamble, 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.[346] 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.[347]

The Commission's existing 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.[348] The Commission believes, as the generally accepted standards and best practices noted in this NPRM make clear, that it would be essentially impossible for a DCM, SEF, or SDR to fulfill its existing obligation to conduct testing sufficient to ensure the reliability, security, and capacity of its automated systems without conducting controls testing.

The proposed rules clarify the existing testing requirements by specifying controls testing as a necessary component. The Commission believes that this has always been the case.[349] If compliance with the existing testing requirements as clarified by the proposed rules imposes costs to a DCM, SEF, or SDR beyond those it already incurs in this connection, the Commission believes that such additional costs would be attributable to compliance with the existing regulations and not to the proposed rules. Accordingly, the Commission believes that this clarification will not impose any new costs for DCMs, SEFs, or SDRs.

2. Minimum Controls Testing Frequency Requirements for Covered DCMs and SDRs

As discussed above, the proposed rules would require a covered DCM or SDR to test each control included in its program of system safeguards-related risk analysis and oversight no less frequently than every two years. The proposed rules would also permit such testing to be conducted on a rolling basis over the course of the period determined by appropriate risk analysis. The current rules require DCMs and SDRs to conduct regular, periodic, objective testing of their automated systems.[350] Therefore, the proposed rules will impose new costs relative to the requirements of the current rules.[351] The Commission notes that testing on a rolling basis is consistent with generally accepted best practices.[352]

3. Independent Contractor Requirement for Covered DCMs and SDRs

As discussed above, the proposed rules would require a DCM or SDR to engage an independent contractor to test and assess the key controls no less frequently than every two years. Current regulations §§ 38.1051(h) and 49.24(j) provide that testing of automated systems should be conducted by qualified, independent professionals.[353] 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 proposed rules will impose new costs relative to the requirements of the current rules.[354] The Commission notes that best practices support independent testing of key controls.[355]

4. Cost Estimates for Covered DCMs and SDRs

Based on the information from the DMO Preliminary Survey, the Commission estimates that the current average cost for a covered DCM or an SDR conducting controls testing is approximately $2,724,000 annually.[356] Consistent with all of the system safeguard-related tests required in the proposal, 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 DCM or SDR that does not currently use an independent contractor to conduct key controls testing, the

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

[347] *Id.*

[348] 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).

[349] *See supra* note 291.

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

[351] Based on the information collected in the DMO Preliminary Survey, the Commission understands that some covered DCMs and SDRs currently conduct controls testing at the proposed frequency level.

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

[353] *Id.*

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

[355] NIST SP 800–53 Rev. 4, control CA–2 *Security Assessments,* Control Enhancements 1, *Security Assessments:* Independent Assessors, available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.*

[356] 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.

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 substantial 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 existing policies and procedures to ensure that they are sufficient in the context of the proposed requirements. The Commission believes that any costs incurred by the entities as result of such review would be minor.

c. Benefits

Controls testing is essential in determining risk to an organization's operations and assets, to individuals, and to other organizations, and to the nation resulting from the use of the organization's systems.[357] In other words, controls testing is vital because it allows firms to be nimble in preventing, detecting, or recovering from an attack.[358] The Commission believes that the complex analysis and plan preparation that a DCM, SEF, and SDR undertakes with respect to controls testing, including designing and implementing changes to existing plans, likely contributes to a better *ex ante* understanding by the DCM's, SEF's, and SDR's management of the challenges the entity would face in a cyber threat scenario, and thus better preparation to meet those challenges. This improved preparation would help reduce the possibility of market disruptions and financial losses to market participants. Moreover, regularly conducting controls testing enables a DCM, SEF, and SDR to mitigate the impact that a cyber threat to, or a disruption of, a DCM's, SEF's, or SDR's operations would have on market participants, entities required by the Act or Commission regulations to report swaps data to SDRs, 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.

As noted above in the costs section, the proposed rules would require a covered DCM or SDR to test each control included in its program of system safeguards-related risk analysis oversight no less frequently than every two years. The Commission believes that it is essential for each 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 proposed rules would also permit such testing to be conducted on a rolling basis over the course of the period determined by appropriate risk analysis. The rolling basis provision is designed to give a covered DCM or SDR flexibility concerning which controls are tested during the required minimum frequency period. This flexibility is intended to reduce burdens associated with testing every control 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.[359]

Additionally, as noted above, the proposed rules would 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 two years. The entities would have the flexibility to conduct any other controls testing by either independent contractors or entity employees not responsible for development or operation of the systems or capabilities being tested. 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.[360] Accordingly, in light of best practices and the current cyber threat level to the financial sector, the Commission believes the independent contractor requirement would provide these substantial benefits.

d. Request for Comments

As set out in more detail below in the Request for Comments section, the Commission seeks additional information regarding the costs and benefits of controls testing, including the minimum testing frequency and independent contractor requirement. The Commission particularly solicits comments concerning the need for controls testing and the associated costs and benefits, from DCMs, SEFs, and SDRs, from futures and swap market participants, from best practices and standards organizations, from cybersecurity service providers and cybersecurity experts in both the private and public sectors, and from other financial regulators.

12. Security Incident Response Plan Testing: Sections 38.1051(h)(5), 37.1401(h)(5), and 49.24(j)(5)

a. Summary of Proposed Rules

As discussed above in Section I.F.6., proposed §§ 38.1051(h)(1), 37.1401(h)(1), and 49.24(j)(1) would define security incident response plan testing as testing of a DCM's, SEF's, or SDR's security incident response plan to determine the plan's effectiveness, identifying its potential weaknesses or deficiencies, enabling regular plan updating and improvement, and maintaining organizational preparedness and resiliency with respect to security incidents. In addition, 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. The DCM's, SEF's, or SDR's security incident response would be required to include, without limitation, the entity's definition and classification of security incidents, its policies and procedures for reporting security incidents and for internal and external communication and information sharing regarding security incidents, and the hand-off and escalation points in its security incident response process. The entities may coordinate its security incident response plan testing with other testing required by this section or with testing of its other BC–DR and crisis management plans. The proposed rules would

[357] 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.*

[358] CFTC Roundtable, at 43–44.

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

[360] NIST SP 800–53 Rev. 4, *supra* note 195.

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.

b. Costs

1. Security Incident Response Plan Testing for All DCMs, SEFs, and SDRs

As discussed in the preamble, 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.[361] 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.[362]

The Commission's existing 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.[363] The Commission believes, as the generally accepted standards and best practices noted in this NPRM make clear, that it would be essentially impossible for a DCM, SEF, or SDR to fulfill its existing obligation to conduct testing sufficient to ensure the reliability, security, and capacity of its automated systems without conducting security incident response plan testing.

The proposed rules clarify the existing testing requirements by specifying security incident response plan testing as a necessary component. The Commission believes that this has always been the case.[364] If compliance with the existing testing requirements as clarified by the proposed 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 would be attributable to compliance with the existing regulations and not to the proposed rules. Accordingly, the Commission believes that this clarification will not impose any new costs for DCMs, SEFs, and SDRs.

2. Minimum Security Incident Response Testing Frequency Requirements for Covered DCMs and SDRs

As discussed above, the proposed rules would require covered DCMs and SDRs to conduct security incident response plan testing at least annually. The current rules require DCMs and SDRs to conduct regular, periodic, objective testing of their automated systems.[365] Accordingly, the proposed rules will impose new costs relative to the requirements of the current rules.[366] The Commission notes that the proposed frequency requirement is consistent with industry best practices.[367]

3. Estimated Costs for Covered DCMs and SDRs

At present, the Commission cannot quantify or estimate the current costs associated with security incident response plan testing at a covered DCM or SDR. Nevertheless, to the extent that the proposed rules would 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 the automated systems, and the scope of the test. Additional costs incurred by the affected entities could include time in reviewing and revising existing 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 proposed requirements. In such cases, the Commission believes that any costs would be minimal.

c. 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 a DCM's, SEF's, or SDR'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 proposed rules would provide clarity to covered DCMs and SDRs concerning the minimum testing frequency. The Commission believes the proposed 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 automated system operation, reliability, security, or capacity, or the availability, confidentiality, or integrity of its futures and swaps data.

d. Request for Comments

As set out in more detail below in the Request for Comments section, the Commission seeks additional information regarding the costs and benefits of the proposed security incident response plan testing requirement, including the minimum testing frequency requirement. The Commission also seeks comments on all aspects of the proposed security incident response plan testing requirement. The Commission particularly solicits comments concerning both the need for security incident response plans and plan testing and the associated costs and benefits, from DCMs, SEFs, and SDRs, from futures and swap market participants, from best practices and standards organizations, from cybersecurity service providers and cybersecurity experts in both the private and public sectors, and from other financial regulators.

13. Enterprise Technology Risk Assessment: Sections §§ 38.1051(h)(6), 37.1401(h)(6), and 49.24(j)(6)

a. Summary of Proposed Rules

As discussed above in Section I.F.7., proposed §§ 38.1051(h)(1), 37.1401(h)(1), and 49.24(j)(1) would define ETRA 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 proposed rules

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

[362] *Id.*

[363] 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).

[364] *See supra* note 291.

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

[366] Based on the Commission's experience in administering the system safeguard compliance program, the Commission believes that many covered DCMs and SDRs currently conduct security incident response plan testing at the proposed frequency.

[367] 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).

would require a covered DCM or SDR to conduct an ETRA at a frequency determined by an appropriate risk analysis, but at a minimum no less frequently than annually. The proposed rules would provide that the assessment may be conducted by independent contractors, or employees of the DCM or SDR who are not responsible for development or operation of the systems or capabilities being tested.

b. Costs

1. ETRAs for All DCMs, SEFs, and SDRs

As discussed in the preamble, 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.[368] 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.[369]

The Commission's existing 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.[370] The Commission believes, as the generally accepted standards and best practices noted in this NPRM make clear, that it would be essentially impossible for a DCM, SEF, or SDR to fulfill its existing obligation to conduct testing sufficient to ensure the reliability, security, and capacity of its automated systems without conducting ETRAs.

The proposed rules clarify the existing testing requirements by specifying ETRAs as a necessary component.[371] The Commission believes that this has always been the case. If compliance with the existing testing requirements as clarified by the proposed 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 would be attributable to compliance with the existing regulations and not to the proposed rules. Accordingly, the Commission believes that this clarification will not impose any new costs for DCMs, SEFs, and SDRs.

2. Minimum ETRA Frequency Requirements for Covered DCMs and SDRs

As discussed above, the proposed rules would require covered DCMs and SDRs to conduct ETRAs at least annually. The current rules require DCMs and SDRs to conduct regular, periodic, objective testing of their automated systems.[372] Therefore, the proposed rules will impose new costs relative to the requirements of the current rules.[373] The Commission notes that the proposed frequency requirement comports with industry best practices.[374]

3. Estimated Costs for Covered DCMs and SDRs

Based on the information from the DMO Preliminary Survey, the Commission estimates that 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. Additionally, 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 would be minor.

c. 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 aligns its systems goals accordingly. The Commission believes that these requirements are necessary to support a strong risk management framework for DCMs, SEFs, and SDRs, thereby helping to protect DCMs, SEFs, and SDRs, market participants, parties required by the Act or Commission regulations to report swaps data to SDRs, and helping to mitigate the risk of market disruptions.

The proposed rules would 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.[375] The Commission believes the proposed frequency requirements would better position the entities to identify, estimate, and prioritize the risks facing them in today's cybersecurity threat environment.

d. Request for Comments

As set out in more detail below in the Request for Comments section, the Commission seeks additional information regarding the costs and benefits of the enterprise technology risk assessment requirement, including the minimum testing frequency requirement. The Commission particularly solicits comments concerning the need for enterprise technology risk assessments and the associated costs and benefits, from DCMs, SEFs, and SDRs, from futures and swap market participants, from best practices and standards organizations, from cybersecurity service providers and cybersecurity experts in both the private and public sectors, and from other financial regulators.

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

a. Summary of Proposed Rules

As discussed above in Section I.G.1., proposed §§ 38.1051(k), 37.1401(k), and 49.24(l) would require that the scope for all system safeguards testing and assessment required by this chapter must be broad enough to include all testing of automated systems, networks, and controls necessary to identify any vulnerability which, if triggered, could enable an intruder or unauthorized user or insider to: (1) Interfere with the entity's operations or with fulfillment of the entity's statutory and regulatory responsibilities; (2) impair or degrade the reliability, security, or adequate

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

[369] *Id.*

[370] 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).

[371] *See supra* note 291.

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

[373] Based on the information from the DMO Preliminary Survey, the Commission understands that most covered DCMs and SDRs currently conduct ETRAs at the proposed frequency.

[374] 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.*

[375] 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.*

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.

b. Costs and Benefits

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

15. Internal Review of Test and Assessment Reports: Sections 38.1051(l), 37.1401(l), and 49.24(m)

a. Summary of Proposed Rules

As discussed above in Section I.G.2. proposed §§ 38.1051(l), 37.1401(l), and 49.24(m) would 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 this section. In addition, the proposed rules would 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.

b. Costs

As discussed in the preamble, the Commission proposes to 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 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.[376] The Commission believes, as the generally accepted standards and best practices noted in this NPRM make clear, that it would be essentially impossible for a DCM, SEF, or SDR to fulfill its existing 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.[377] This has been true since before the testing requirements of the Act and the current regulations were adopted.[378] If compliance with the existing testing requirements as clarified by the proposed 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 existing regulations and not to the proposed rules. Accordingly, the Commission believes that this clarification will not impose any new costs for DCMs, SEFs, and SDRs.

c. 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 its automated systems.

d. Request for Comments

The Commission requests comment on any potential costs of proposed §§ 38.1051(l), 37.1401(l), and 49.24(m) on DCMs, SEFs, and SDRs, including, where possible, quantitative data.

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

a. Summary of Proposed Rules

As discussed above in Section I.G.3., proposed §§ 38.1051(m), 37.1401(m), and 49.24(n) would require a DCM, SEF, or an SDR to analyze the results of the testing and assessment required by this section to identify all vulnerabilities and deficiencies in the entity's systems. The DCM, SEF, or SDR would also be required to remediate the vulnerabilities and deficiencies revealed by all testing and assessment, to the full extent necessary to enable the entity to fulfill the system safeguards requirements of this chapter, and to meet all statutory and regulatory obligations in connection with its regulated activities. The remediation must be timely in light of appropriate risk analysis with respect to the risks presented by such vulnerabilities and deficiencies.

b. Costs

As discussed in the preamble, the Commission proposes to 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. Remediation of vulnerabilities and deficiencies revealed by cybersecurity testing is a best practice and a fundamental purpose of such testing.[379] The Commission believes, as the generally accepted standards and best practices noted in this NPRM make clear, that it would be essentially impossible for a DCM, SEF, or SDR to

[376] FINRA, *Report on Cybersecurity Practices,* February 2015, at 7, available at *https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf*; FFIEC, *Information Security IT Examination Handbook,* at 5, available at *http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_InformationSecurity.pdf.*; and NIST SP 800–53, Rev. 4, *Program Management Control Family,* available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.*

[377] *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*; NIST SP 800–53A Rev. 4, at 10, available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf;* FFIEC, *Information Security IT Examination Handbook,* at 5, available at *http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_InformationSecurity.pdf*; NIST SP 800–53 Rev. 4, *Program Management control family,* available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf;* FINRA, *Report on Cybersecurity Practices,* February 2015, at 8, available at *https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf;* FFIEC, *Audit IT Examination Handbook,* Objective 6, at 5, available at *http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_Audit.pdf*; ISACA, COBIT 5, APO12, available at *https://cobitonline.isaca.org/.*

[378] *See supra* note 246.

[379] FINRA, *Report on Cybersecurity Practices,* February 2015, at 7, available at *https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf*; FFIEC, *Information Security IT Examination Handbook,* at 5, available at *http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_InformationSecurity.pdf.*; and NIST SP 800–53, Rev. 4, *Program Management Control Family,* available at *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.*

fulfill its existing obligation to conduct testing sufficient to ensure the reliability, security, and capacity of its automated systems without performing remediation.[380] This has been true since before the testing requirements of the Act and the current regulations were adopted.[381] If compliance with the existing testing requirements as clarified by the proposed 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 existing regulations and not to the proposed rules. Accordingly, the Commission believes that this clarification will not impose any new costs for DCMs, SEFs, and SDRs.

c. Benefits

The Commission believes that effective remediation is a critical component of a comprehensive and effective system safeguard program. As discussed above, the Commission believes that the remediation of vulnerabilities and deficiencies revealed by cybersecurity testing is an industry best practice. Moreover, remediation may reduce the frequency and severity of systems disruptions and breaches for the DCMs, SEFs, and SDRs. In addition, remediation helps to ensure that the entities dedicate appropriate resources to timely address system safeguard-related deficiencies and would place an emphasis on mitigating harm to market participants while promoting market integrity. Without a timely remediation requirement, the impact of 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.

d. Request for Comments

As set out in more detail below in the Request for Comments section, the Commission seeks additional information regarding the costs and benefits of the remediation requirement. The Commission particularly solicits comments concerning the need for remediation and the associated costs and benefits, from DCMs, SEFs, and SDRs, from futures and swap market participants, from best practices and standards organizations, from cybersecurity service providers and cybersecurity experts in both the private and public sectors, and from other financial regulators.

17. Required Production of Annual Trading Volume: Section 38.1051(n)

a. Summary of Proposed Rule

Proposed § 38.1051(n) would require all DCMs to provide to the Commission for calendar year 2015, and each calendar year thereafter, its annual total trading volume. This information would be required 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.

b. Costs

As discussed above in the PRA section, 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. Therefore, the Commission believes that any costs incurred by the DCMs as a result of proposed § 38.1051(n) would be minimal. The Commission estimates that each DCM would spend approximately half an hour to prepare and file the trading volume information with Commission at a cost of approximately $22.00 annually.[382]

c. Benefits

As a result of the Commission's proposal to apply the enhanced system safeguard requirements to DCMs whose annual trading volume in a calendar year is five percent or more of the combined annual trading volume of all DCMs regulated by Commission (*i.e.,* covered DCMs), 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 proposal. As stated in the proposed 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. Therefore, all DCMs will receive certainty from the Commission regarding whether they must comply with the enhanced system safeguard requirements. This requirement will support more accurate application of the proposed rules.

18. Section 15(a) Factors

a. Protection of Market Participants and the Public

The Commission believes that the proposed rules should 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. 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 proposed 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 are essential to mitigation of system 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

[380] *See supra* note 377.

[381] *See supra* note 246.

[382] 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 (2014 Report). The hourly rate for a Compliance Officer in the Securities and Commodity Exchanges as published in the 2014 Report was $44.03 per hour.

lost.[383] 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. Additionally, and because SDRs hold data needed by financial regulators from multiple jurisdictions, safeguarding such systems will be essential to mitigation of systemic risk world-wide. Notice to the Commission concerning the results of system safeguard tests performed by the 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 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. Similarly, any interruption in the operations of an SDR will 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 proposed rules will reduce the incidence and severity of automated system security breaches and functional failures. In addition, the Commission views the proposed 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 proposed 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 without interruption will 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.

e. Other Public Interest Considerations

The American economy and the American public depend upon the availability of reliable and secure markets for price discovery, hedging, and speculation. Ensuring the adequate safeguarding and the reliability, security, and capacity of the systems supporting these market functions is a core focus in the Commission's role in monitoring and assessing the level of systemic risk, and is central to its fulfillment of oversight responsibilities. As one CFTC Roundtable panelist explained, ''if the futures system doesn't work many other things don't work, and it's a wholly interconnected system. And the more we can make all the parts more secure the more resilient it's going to be overall.'' [384]

III. Requests for Comment

A. Comments Regarding Notice of Proposed Rulemaking

The Commission requests comments from the public on all aspects of this NPRM. This specifically includes comments on all aspects of the Commission's preliminary consideration of costs and benefits associated with the Proposal, and all aspects of the Commission's preliminary consideration of the five factors that the Commission is required to consider under section 15(a) of the CEA. The Commission particularly solicits comments concerning all aspects of the Proposal and its associated costs and benefits from DCMs, SEFs, and SDRs, from futures and swap market participants, from best practices and standards organizations, from cybersecurity providers and cybersecurity experts in both the private and public sectors, and from other financial regulators.

The questions below relate to areas that the Commission believes may be relevant. In addressing these questions or any other aspects of the Proposal and Commission's assessments, commenters are encouraged to submit any data or other information that they may have quantifying or qualifying the costs and benefits of the Proposal. Comments may be submitted directly to the Office of Information and Regulatory Affairs, by fax at (202) 395–6566 or by email at *OIRAsubmissions@omb.eop.gov*. Please provide the Commission with a copy of submitted comments so that all comments can be summarized and addressed in the final rule preamble. Refer to the **ADDRESSES** section of this NPRM for comment submission instructions to the Commission. A copy of the supporting statements for the collections of information discussed above may be obtained by visiting *http://RegInfo.gov*. OMB is required to make a decision concerning the collection of information between 30 and 60 days after publication of this document in the **Federal Register**. Therefore, a comment is best assured of having its full effect if OMB receives it within 30 days of publication.

1. Do commenters agree with the Commission's analysis of the costs and benefits of each provision in the Proposal? Please explain why or why not.

2. Do commenters believe that there are additional benefits or costs that could be quantified or otherwise estimated? If so, please identify those categories and, if possible, provide specific estimates or data.

3. Do commenters agree that the definitions of the categories of risk analysis and oversight to be addressed by DCM, SEF, and SDR programs of system safeguards-related risk analysis and oversight included in the Proposal are appropriate, sufficiently clear, and

[383] 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.

[384] CFTC Roundtable, at 28.

reflective of generally accepted best practices and standards? Please identify any suggested clarifications or changes respecting these definitions.

4. Do commenters agree that following generally accepted standards and best practices, ensuring tester independence, and coordinating BC–DR plans appropriately are essential to adequate system safeguards and cyber resiliency for DCMs, SEFs, and SDRs, and that the current rule provisions and guidance providing that DCMs, SEFs, and SDRs should comply in these regards should be changed to require mandatory compliance? Please identify, and quantify insofar as possible, any new costs that DCMs, SEFs, or SDRs would incur due to making such compliance mandatory.

5. Do commenters agree that the definitions of terms included in the proposed §§ 38.1051(h)(1), 37.1401(h)(1), and 49.24(j)(1) are appropriate, sufficiently clear, and reflective of generally accepted best practices and standards? Please identify any suggested clarifications or changes respecting these definitions.

6. Do commenters agree that the types of system safeguards testing specified in the Proposal, including vulnerability testing, external and internal penetration testing, controls testing, security incident response plan testing, and enterprise technology risk assessment, are appropriate and necessary in today's cybersecurity environment? Please explain why or why not. Also, do commenters agree that each testing type is appropriately and adequately addressed by the Proposal? Please explain why or why not, and identify any suggested clarifications or changes in this connection.

7. Are the types of cybersecurity and system safeguards testing included in the Proposal sufficient in the aggregate to provide the cybersecurity and system safeguards protections needed by DCMs, SEFs, and SDRs to enable them to fulfill their statutory and regulatory requirements in the current cybersecurity environment? Please explain why or why not. Also, should the Commission consider requiring other types of cybersecurity and system safeguards testing not included in the Proposal? If so, please identify the other types of testing that should be required, and if possible provide information concerning the costs and benefits that would be involved.

8. The existing system safeguards rules for DCMs, SEFs, and SDRs require testing sufficient to ensure automated system reliability, security, and capacity. The Proposal clarifies these testing requirements by specifying and defining five types of system safeguards testing essential to fulfilling these existing requirements. Do commenters agree that this clarification will not impose new costs on DCMs, SEFs, and SDRs? Commenters who disagree are asked to specify which types of testing called for in the Proposal DCMs, SEFs, or SDRs do not currently conduct, and what new costs such entities would incur as the result of the clarification of required testing types.

9. Do commenters agree that the minimum testing frequency requirements included in the Proposal for each of the types of system safeguards testing are appropriate in today's cybersecurity environment? Please explain why or why not. In your response, please be specific with respect to the types of testing that you suggest should be conducted either more or less frequently than specified in the Proposal, and indicate the potential costs and benefits associated with each such modification.

10. Do commenters agree with the requirements included in the Proposal for certain testing to be conducted by independent contractors? Please explain why or why not. If not, please address what testing you believe should be conducted by independent contractors, and the frequency of independent contractor testing that should be required. Please also indicate the potential costs and benefits associated with each such modification.

11. What are the benefits of requiring certain tests to be conducted by independent contractors? In your response, please be specific with respect to which tests should be conducted by independent contractors and, if possible, provide specific estimates or data for the costs of each test.

12. For covered DCMs and SDRs, please identify and explain how any of the proposed testing requirements respecting minimum testing frequency and use of independent contractors differ from the current practice at the entity (*e.g.*, the entity does not currently use independent contractors for vulnerability testing, whereas the proposed rule would require the entity to engage independent contractors to conduct two of the required quarterly tests each year). In cases where the Proposal differs from current practice, please provide specific estimates of any additional costs that the entity would incur to comply with the proposal.

13. Do commenters agree that the testing scope requirements provided in the Proposal are appropriate, sufficiently clear, reflective of generally accepted best practices and standards, and sufficient to enable DCMs, SEFs, and SDRs to fulfill their statutory and regulatory responsibilities? Please identify any suggested clarifications or changes respecting these provisions.

14. Do commenters agree that the internal reporting and review requirements provided in the Proposal are appropriate, sufficiently clear, reflective of generally accepted best practices and standards, and sufficient to enable DCMs, SEFs, and SDRs to fulfill their statutory and regulatory responsibilities? Please identify any suggested clarifications or changes respecting these provisions.

15. Do commenters agree that the remediation requirements provided in the Proposal are appropriate, sufficiently clear, reflective of generally accepted best practices and standards, and sufficient to enable DCMs, SEFs, and SDRs to fulfill their statutory and regulatory responsibilities? Please identify any suggested clarifications or changes respecting these provisions.

16. Do commenters believe that there are any costs or benefits from the Proposal that could be quantified or monetized that are unique to a DCM, SEF, or an SDR? If so, please identify those costs or benefits, and if possible provide specific estimates or data.

17. Are there methods by which the Commission could reduce the costs imposed by the Proposal, while still maintaining the system safeguards for DCMs, SEFs, and SDRs that are required by law and are appropriate to today's cybersecurity threat environment? If so, please explain.

18. Are there any unintended consequences that would result from the Proposal? If so, please describe them, and explain how the unintended consequences would impact any of the costs or benefits associated with the Proposal, or would impact DCM, SEF, or SDR operations.

19. Does the Proposal appropriately describe the potential impacts on the protection of market participants and the public, efficiency and competition, financial integrity of the futures markets and price discovery, sound risk management practices, and other public interest considerations? If not, please provide specific examples.

20. Do commenters believe that there are reasonable alternatives to any aspect of the Proposal? In the response, please specifically describe such alternatives and identify their potential costs and benefits relative to the proposal. Please also describe the potential impacts of the alternatives on protection of market participants and the public, efficiency and competition, financial integrity of the futures markets and price discovery,

sound risk management practices, and other public interest considerations.

B. Comments Regarding Advance Notice of Proposed Rulemaking Concerning Covered SEFs

The Commission requests comments from the public on all aspects of the ANPRM included herein concerning possible future minimum testing frequency requirements and independent contractor testing requirements for covered SEFs. The Commission particularly solicits comments concerning all aspects of the ANPRM from DCMs, SEFs, and SDRs, from futures and swap market participants, from best practices and standards organizations, from cybersecurity providers and cybersecurity experts in both the private and public sectors, and from other financial regulators.

The questions below relate to areas that the Commission believes may be relevant. In addressing these questions or any other aspects of the ANPRM concerning possible future minimum testing frequency requirements and independent contractor testing requirements for covered SEFs, commenters are encouraged to submit any data or other information that they may have quantifying or qualifying costs and benefits that could be related to the ANPRM. Comments may be submitted directly to the Office of Information and Regulatory Affairs, by fax at (202) 395–6566 or by email at *OIRAsubmissions@omb.eop.gov*. Please provide the Commission with a copy of submitted comments so that all comments can be summarized and addressed in the final rule preamble. Refer to the **ADDRESSES** section of this NPRM for comment submission instructions to the Commission.

The Commission is considering whether the minimum testing frequency and independent contractor testing requirements which this NPRM would apply to covered DCMs and SDRs should be applied, via a future NPRM, to the most systemically important SEFs, which such a future NPRM would define as ''covered SEFs.'' The Commission requests comments on all aspects of this question, including possible related costs and benefits. In addition, commenters are asked to address the particular aspects of this subject included in the questions below.

1. Should the minimum testing frequency and independent contractor testing requirements be applied, via a future NPRM, to the most systemically important SEFs, or to all SEFs, or should such requirements not be applied to SEFs at this time?

2. Given the nature of the swap market, would it be more appropriate to define ''covered SEF'' in terms of the annual total notional value of all swaps traded on or pursuant to the rules of a SEF, as compared with the annual total notional value of all swaps traded on or pursuant to the rules of all SEFs regulated by the Commission? Or would it be more appropriate to define ''covered SEF'' in terms of the annual total number of swaps traded on or pursuant to the rules of a SEF, as compared with the annual total number of swaps traded on all SEFs regulated by the Commission?

3. If defining ''covered SEF'' in terms of notional value is more appropriate, how should ''notional value'' be defined?

4. If defining ''covered SEF'' in terms of notional value is more appropriate, what percentage share of the annual total notional value of all swaps traded on all SEFs regulated by the Commission should be used to define ''covered SEF''?

5. If defining ''covered SEF'' in terms of the annual total number of swaps traded is more appropriate, what percentage share of the annual total number of all swaps traded on all SEFs regulated by the Commission should be used to define ''covered SEF''?

6. Would it be more appropriate for the definition to address the notional value or the number of swaps in each asset class separately, or to address the notional value or the number of all swaps combined regardless of asset class?

7. Do commenters agree that overall risk mitigation for the U.S. swap market as a whole would be enhanced if the minimum testing frequency and independent contractor testing requirements were applied to the most systemically important SEFs? Or do commenters believe that the testing requirements for all SEFs proposed in the current NPRM are sufficient for appropriate overall risk mitigation? Or do commenters believe the minimum testing frequency and independent contractor testing requirements should be applied to all SEFs in order to appropriately address the risk to the U.S. swap market?

8. The Commission is considering defining ''covered SEF'' as a SEF for which the annual total notional value of all swaps traded on or pursuant to the rules of the SEF is ten percent (10%) 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. Via a future NPRM, such SEFs would be subject to the minimum testing frequency and independent contractor testing requirements proposed in this current NPRM for covered DCMs and SDRs. Do commenters agree that this percentage share provides the most appropriate means of determining which SEFs would be ''covered SEFs'' subject to these requirements? Would a different percentage share be more appropriate, and if so, what other percentage share should be used? Should the Commission consider a different methodology for defining covered SEFs? If so, please explain.

9. How should the benefits and costs of applying the minimum testing frequency and independent contractor testing requirements to covered SEFs be quantified or estimated? If possible, provide specific estimates or data.

10. For each of the five types of cybersecurity testing addressed in this NPRM, what costs would a covered SEF incur to comply with the minimum testing frequency and independent contractor testing requirements?

11. To what extent are SEFs currently meeting the minimum testing frequency and independent contractor testing requirements proposed in this NPRM? To the extent possible, please provide specific estimates or data.

12. How could a SEF most appropriately report to the Commission its annual total notional value of all swaps traded or its annual total number of swaps traded, in order to enable the Commission to notify it of whether it is a covered SEF?

13. Are there additional alternatives or factors which commenters believe the Commission should consider in determining what, if anything, to propose in connection with the definition of covered SEFs and minimum testing frequency and independent contractor testing requirements for covered SEFs?

List of Subjects

17 CFR Part 37

Commodity futures, Reporting and recordkeeping requirements, System safeguards testing requirements.

17 CFR Part 38

Commodity futures, Reporting and recordkeeping requirements, System safeguards testing requirements.

17 CFR Part 49

Administrative practice and procedure, Reporting and recordkeeping requirements, System safeguards testing requirements.

For the reasons set forth in the preamble, the Commodity Futures Trading Commission proposes to amend 17 CFR chapter I as follows:

PART 37—SWAP EXECUTION FACILITIES

■ 1. The authority citation for part 37 continues to read as follows:

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. 111–203, 124 Stat. 1376.

■ 2. Amend § 37.1401 as follows:
■ a. Revise paragraphs (a) and (b);
■ b. Remove paragraph (f);
■ c. Redesignate paragraphs (c) through (e) as paragraphs (d) through (f);
■ d. Add new paragraph (c);
■ e. Revise paragraph (g);
■ f. Redesignate paragraph (h) as paragraph (j); and
■ g. Add new paragraphs (h), (i), (k), (l), and (m).

The revisions and additions read as follows:

§ 37.1401 Requirements.

(a) A swap execution facility's program of risk analysis and oversight with respect to its operations and automated systems must 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 (*e.g.,* least privilege, separation of duties, account monitoring and control); user and device identification and authentication; security awareness training; audit log maintenance, monitoring, and analysis; media protection; personnel security and screening; automated system and communications protection (*e.g.,* network port control, boundary defenses, encryption); system and information integrity (*e.g.,* malware defenses, software integrity monitoring); vulnerability management; penetration testing; security incident response and management; and any other elements of information security included in generally accepted best practices.

(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 paragraphs (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 (*e.g.,* testing, monitoring, and analysis of current and projected future capacity and performance, and of possible capacity degradation due to planned automated system changes); and any other elements of capacity and performance planning included in generally accepted best practices.

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

(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 must 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. The 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 must 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 § 1.31 of this chapter, Core Principle 10 (Recordkeeping and Reporting), and §§ 37.1000 and 37.1001, a swap execution facility must provide to the Commission the following system safeguards-related books and records, promptly upon the request of any Commission representative:

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

(2) All assessments of its 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 by employees of the swap execution facility; and

(4) All other books and records requested by Commission staff in connection with Commission oversight of system safeguards pursuant to the Act or to part 37 of the Commission's regulations, or in connection with Commission maintenance of a current profile of the swap execution facility's automated systems.

(5) Nothing in paragraph (g) of this section 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 of this chapter, or §§ 37.1000 or 37.1001 of the Commission's regulations.

(h) A swap execution facility must conduct regular, periodic, objective testing and review of its automated systems to ensure that they are reliable, secure, and have adequate scalable capacity. It must 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 paragraph (h) of this section.

(1) *Definitions.* As used in paragraph (h) of this section:

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 system safeguards requirements established by this chapter.

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 or potentially jeopardizes automated system operation, reliability, security, or capacity, or the availability, confidentiality or integrity of data.

Security incident response plan means a written plan documenting the 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 paragraph (k) of this section, at a frequency determined by an appropriate risk analysis.

(i) Such vulnerability testing shall include automated vulnerability scanning. Where indicated by appropriate risk analysis, such scanning must be conducted on an authenticated basis, *e.g.,* using log-in credentials. Where scanning is conducted on an unauthenticated basis, the designated contract market must implement effective compensating controls.

(ii) Vulnerability testing for a swap execution facility shall be conducted by qualified, independent professionals. Such qualified independent professionals may be independent contractors or employees of the swap execution facility, but shall not be persons responsible for development or operation of the systems or capabilities being tested.

(3) *Penetration testing*—(i) *External penetration testing.* A swap execution facility shall conduct external penetration testing of a scope sufficient to satisfy the requirements set forth in paragraph (k) of this section, at a frequency determined by an appropriate risk analysis.

(A) External penetration testing for a swap execution facility shall be conducted by qualified, independent professionals. Such qualified independent professionals may be independent contractors or employees of the swap execution facility, but shall not be persons responsible for development or operation of the systems or capabilities being tested.

(B) [Reserved]

(ii) *Internal penetration testing.* A swap execution facility shall conduct internal penetration testing of a scope sufficient to satisfy the requirements set forth in paragraph (k) of this section, at a frequency determined by an appropriate risk analysis.

(A) A swap execution facility may 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.

(B) [Reserved]

(4) *Controls testing.* A swap execution facility shall conduct controls testing of a scope sufficient to satisfy the requirements set forth in paragraph (k) of this section, at a frequency determined by an appropriate risk analysis. Such controls testing must include testing of each control included in the swap execution facility's program of risk analysis and oversight.

(i) Controls testing for a swap execution facility shall be conducted by qualified, independent professionals. Such qualified independent professionals may be independent contractors or employees of the swap execution facility, but shall not be persons responsible for development or operation of the systems or capabilities being tested.

(ii) [Reserved]

(5) *Security incident response plan testing.* A swap execution facility shall

conduct security incident response plan testing sufficient to satisfy the requirements set forth in paragraph (k) of this section, at a frequency determined by an appropriate risk analysis.

(i) 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.

(ii) 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.

(iii) A swap execution facility may conduct security incident response plan 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) *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 paragraph (k) of this section, at a frequency determined by an appropriate risk analysis.

(i) 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.

(ii) [Reserved]

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

(1) 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;

(2) 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

(3) 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 must 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 or insider to:

(1) Interfere with the swap execution facility's operations or with fulfillment of its statutory and regulatory responsibilities;

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

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

(4) 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 the swap execution facility shall receive and review reports setting forth the results of all testing and assessment required by this section. The swap execution facility shall establish and follow appropriate procedures for the remediation of issues identified through such review, as provided in paragraph (m) of this section, and for evaluation of the effectiveness of testing and assessment protocols.

(m) *Remediation.* A swap execution facility shall analyze the results of the testing and assessment required by this section to identify all vulnerabilities and deficiencies in its systems. The swap execution facility must remediate those vulnerabilities and deficiencies to the extent necessary to enable the swap execution facility to fulfill the system safeguards requirements of this part and meet its statutory and regulatory obligations. Such remediation must be timely in light of appropriate risk analysis with respect to the risks presented by such vulnerabilities and deficiencies.

Appendix B to Part 37—[Removed and Reserved]

■ 3. In Appendix B to Part 37, under the centered section heading *Core Principle 14 of Section 5h of the Act—System Safeguards*, remove and reserve the text.

PART 38—DESIGNATED CONTACT MARKETS

■ 4. The authority citation for part 38 continues to read as follows:

Authority: 7 U.S.C. 1a, 2, 6, 6a, 6c, 6e, 6d, 6f, 6g, 6i, 6j, 6k, 6l, 6m, 6n, 7, 7a–2, 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. 111–203, 124 Stat. 1376.

■ 5. Amend § 38.1051 as follows:

■ a. Revise paragraphs (a), (b), (c), (g), (h), and (i) introductory text; and

■ b. Add new paragraphs (k), (l), (m), and (n).

The revisions and additions read as follows:

§ 38.1051 General requirements.

(a) A designated contract market's program of risk analysis and oversight with respect to its operations and automated systems must 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 (*e.g.,* least privilege, separation of duties, account monitoring and control); user and device identification and authentication; security awareness training; audit log maintenance, monitoring, and analysis; media protection; personnel security and screening; automated system and communications protection (*e.g.,* network port control, boundary defenses, encryption); system and information integrity (*e.g.,* malware defenses, software integrity monitoring); vulnerability management; penetration testing; security incident response and management; and any other elements of information security included in generally accepted best practices.

(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 paragraphs (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 (*e.g.,* testing, monitoring, and analysis of current and projected future capacity and performance, and of possible capacity degradation due to planned automated system changes); and any other elements of capacity and performance planning included in generally accepted best practices.

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

(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 must 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 must 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 of this chapter, Core Principle 18 (Recordkeeping), and §§ 38.950 and 38.951, a designated contract market must provide to the Commission the following system safeguards-related books and records, promptly upon the request of any Commission representative:

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

(2) All assessments of its 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 by employees of the designated contract market; and

(4) All other books and records requested by Commission staff in connection with Commission oversight of system safeguards pursuant to the Act or to part 38 of the Commission's regulations, or in connection with Commission maintenance of a current profile of the designated contract market's automated systems.

(5) Nothing in paragraph (g) of this section 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 of this chapter, or §§ 38.950 or 38.951 of the Commission's regulations.

(h) A designated contract market must conduct regular, periodic, objective testing and review of its automated systems to ensure that they are reliable, secure, and have adequate scalable capacity. It must 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 paragraph (h) of this section. 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 paragraph (h) of this section.

(1) *Definitions.* As used in paragraph (h) of this section:

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 system safeguards requirements established by this chapter.

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 two consecutive calendar years ceases to be a covered designated contract market as of March 1 of the calendar year following such two 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 or potentially jeopardizes automated system operation, reliability, security, or capacity, or the availability, confidentiality or integrity of data.

Security incident response plan means a written plan documenting the 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 in paragraph (k) of this section, at a frequency determined by an appropriate risk analysis.

(i) Such vulnerability testing shall include automated vulnerability scanning. Where indicated by appropriate risk analysis, such scanning must be conducted on an authenticated basis, *e.g.,* using log-in credentials. Where scanning is conducted on an unauthenticated basis, the designated contract market must implement effective compensating controls.

(ii) At a minimum, a covered designated contract market shall conduct such vulnerability testing no less frequently than quarterly.

(iii) A covered designated contract market shall engage independent contractors to conduct two of the required quarterly vulnerability tests each year. The covered designated contract market may conduct other vulnerability 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.

(iv) Vulnerability testing for a designated contract market which is not a covered designated contract market as defined in this section shall be conducted by qualified, independent professionals. Such qualified independent professionals may be independent contractors or employees of the designated contract market, but shall not be persons responsible for development or operation of the systems or capabilities being tested.

(3) *Penetration testing*—(i) *External penetration testing.* A designated contract market shall conduct external penetration testing of a scope sufficient to satisfy the requirements set forth in paragraph (k) of this section, at a frequency determined by an appropriate risk analysis.

(A) At a minimum, a covered designated contract market shall conduct such external penetration testing no less frequently than annually.

(B) 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.

(C) External penetration testing for a designated contract market which is not a covered designated contract market as defined in this section shall be conducted by qualified, independent professionals. Such qualified independent professionals may be independent contractors or employees of the designated contract market, but shall not be persons responsible for development or operation of the systems or capabilities being tested.

(ii) *Internal penetration testing.* A designated contract market shall conduct internal penetration testing of a scope sufficient to satisfy the requirements set forth in paragraph (k) of this section, at a frequency determined by an appropriate risk analysis.

(A) At a minimum, a covered designated contract market shall conduct such internal penetration testing no less frequently than annually.

(B) A designated contract market may 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.

(4) *Controls testing.* A designated contract market shall conduct controls testing of a scope sufficient to satisfy the requirements set forth in paragraph (k) of this section, at a frequency determined by an appropriate risk analysis. Such controls testing must include testing of each control included in the designated contract market's program of risk analysis and oversight.

(i) At a minimum, a covered designated contract market shall such conduct controls testing no less frequently than every two years. The covered designated contract market may conduct such testing on a rolling basis over the course of the minimum two-year period or over a minimum period determined by an appropriate 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 two years. The covered designated contract market may conduct

any other controls testing required by paragraph (h)(4) of 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) Controls testing for a designated contract market which is not a covered designated contract market as defined in this section shall be conducted by qualified, independent professionals. Such qualified independent professionals may be independent contractors or employees of the designated contract market, but shall not be persons responsible for development or operation of the systems or capabilities being tested.

(5) *Security incident response plan testing.* A designated contract market shall conduct security incident response plan testing sufficient to satisfy the requirements set forth in paragraph (k) of this section, at a frequency determined by an appropriate risk analysis.

(i) 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.

(ii) 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.

(iii) At a minimum, a covered designated contract market shall conduct such security incident response plan testing no less frequently than annually.

(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 who are not responsible for development or operation of the systems or capabilities being tested.

(6) *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 paragraph (k) of this section, at a frequency determined by an appropriate risk analysis.

(i) A covered designated contract market shall conduct an enterprise technology risk assessment no less frequently than annually.

(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 must 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 or insider to:

(1) Interfere with the designated contract market's operations or with fulfillment of its statutory and regulatory responsibilities;

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

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

(4) 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 the designated contract market shall receive and review reports setting forth the results of all testing and assessment required by this section. The designated contract market shall establish and follow appropriate procedures for the remediation of issues identified through such review, as provided in paragraph (m) this section, and for evaluation of the effectiveness of testing and assessment protocols.

(m) *Remediation.* A designated contract market shall analyze the results of the testing and assessment required by this section to identify all vulnerabilities and deficiencies in its systems. The designated contract market must remediate those vulnerabilities and deficiencies to the extent necessary to enable the designated contract market to fulfill the system safeguards requirements of this part and meet its statutory and regulatory obligations. Such remediation must be timely in light of appropriate risk analysis with respect to the risks presented by such vulnerabilities and deficiencies.

(n) *Required production of annual total trading volume.* (1) As used in paragraph (n) of this section, *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.

(2) 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—SWAP DATA REPOSITORIES

■ 6. The authority citation for part 49 continues to read as follows:

Authority: 7 U.S.C. 12a and 24a, as amended by Title VII of the Wall Street Reform and Consumer Protection Act, Pub. L. 111–203, 124 Stat. 1376 (2010), unless otherwise noted.

■ 7. Amend § 49.24 as follows:

■ a. Revise paragraphs (b), (c), (d), (i), (j), and (k) introductory text; and

■ b. Add new paragraphs (l), (m), and (n).

The revisions and additions read as follows:

§ 49.24 System Safeguards.

* * * * *

(b) A registered swap data repository's program of risk analysis and oversight with respect to its operations and automated systems must 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 (*e.g.* least privilege, separation of duties, account monitoring and control); user and device identification and authentication; security awareness training; audit log maintenance, monitoring, and analysis; media protection; personnel security and screening; automated system and communications protection (*e.g.*, network port control, boundary defenses, encryption); system and information integrity (*e.g.*, malware defenses, software integrity monitoring); vulnerability management; penetration testing; security incident response and management; and any other elements of information security included in generally accepted best practices.

(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 paragraphs (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 designated contract market's systems to ensure adequate scalable capacity (*e.g.,* testing, monitoring, and analysis of current and projected future capacity and performance, and of possible capacity degradation due to planned automated system changes); and any other elements of capacity and performance planning included in generally accepted best practices.

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

(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 registered 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 registered 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 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 §§ 1.31 and 45.2 of this chapter, and § 49.12, a swap data repository must provide to the Commission the following system safeguards-related books and records, promptly upon the request of any Commission representative:

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

(2) All assessments of its 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 by employees of the swap data repository; 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 regulations, or in connection with Commission maintenance of a current profile of the swap data repository's automated systems.

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

(j) A registered 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 paragraph (j) of this section.

(1) *Definitions.* As used in paragraph (j) of this section:

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 system safeguards requirements established by this chapter.

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 or potentially jeopardizes automated system operation, reliability, security, or capacity, or the availability, confidentiality or integrity of data.

Security incident response plan means a written plan documenting the 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 paragraph (l) of this section.

(i) Such vulnerability testing shall include automated vulnerability scanning. Where indicated by appropriate risk analysis, such scanning must be conducted on an authenticated basis, *e.g.,* using log-in credentials. Where scanning is conducted on an unauthenticated basis, the swap data repository must implement effective compensating controls.

(ii) The swap data repository shall conduct such vulnerability testing at a frequency determined by an appropriate risk analysis, but no less frequently than quarterly.

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

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

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

(B) The 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.

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

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

(B) The swap data repository may 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.

(4) *Controls testing.* A swap data repository shall conduct controls testing of a scope sufficient to satisfy the requirements set forth in paragraph (l) of this section. Such controls testing shall include testing of each control included in the swap data repository's program of system safeguards risk analysis and oversight.

(i) The swap data repository shall conduct controls testing at a frequency determined by an appropriate risk analysis, but no less frequently than every two years. The swap data repository may conduct such testing on a rolling basis over the course of the minimum two-year period or over a minimum period determined by an appropriate risk analysis, whichever is shorter.

(ii) The swap data repository shall engage independent contractors to test and assess the key controls, as determined by appropriate risk analysis, included in the entity's program of risk analysis and oversight no less frequently than every two years. The swap data repository may conduct any other controls testing required by this paragraph (j)(4) of 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.

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

(i) The 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.

(ii) The 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.

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

(iv) The swap data repository may conduct security incident response plan 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.

(6) *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 paragraph (l) of this section.

(i) The 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.

(ii) The 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 registered swap data repository shall:

* * * * *

(l) *Scope of testing and assessment.* The scope for all system safeguards testing and assessment required by this section must 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 or insider to:

(1) Interfere with the swap data repository's operations or with fulfillment of its statutory and regulatory responsibilities;

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

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

(4) 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 the swap data repository shall receive and review reports setting forth the results of all testing and assessment required by this section. The swap data repository shall establish and follow appropriate procedures for the remediation of issues identified through such review, as provided in paragraph (n) of this section, and for evaluation of the effectiveness of testing and assessment protocols.

(n) *Remediation.* A swap data repository shall analyze the results of the testing and assessment required by this section to identify all vulnerabilities and deficiencies in its systems. The swap data repository must remediate those vulnerabilities and deficiencies to the extent necessary to enable the swap data repository to fulfill the system safeguards requirements of this part and meet its statutory and regulatory obligations. Such remediation must be timely in light of appropriate risk analysis with respect to the risks presented by such vulnerabilities and deficiencies.

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

Christopher J. Kirkpatrick,

Secretary of the Commission.

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

Appendices to System Safeguards Testing Requirements—Commission Voting Summary, Chairman's Statement, and Commissioners' Statements Appendix 1—Commission Voting Summary

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

Appendix 2—Statement of Chairman Timothy G. Massad

I strongly support this proposed rule, which would enhance and clarify requirements to protect exchanges, swap execution facilities and swap data repositories from numerous cybersecurity risks.

This proposal, alongside a companion measure released by the Commission's Division of Clearing and Risk, ensures that the private companies that run the core infrastructure under our jurisdiction are doing adequate evaluation of cybersecurity risks and testing of their own cybersecurity and operational risk protections.

I believe this proposed rule will help address a number of concerns, such as information security, physical security, business continuity and disaster recovery. The proposal sets principles-based testing standards which are deeply rooted in industry best practices.

The rule identifies five types of testing as critical to a sound system safeguards program: Vulnerability testing, penetration testing, controls testing, security incident response plan testing and enterprise-wide assessment of technology risk. Such efforts are vital to mitigate risk and preserve the ability to detect, contain, respond to, and recover from a cyberattack or other type of operational problem.

The proposal applies the base standards to swap execution facilities. It also contains an anticipated notice of proposed rulemaking, which notes that the Commission is considering whether to apply minimum testing frequency and independent contractor testing requirements to the most systemically important swap execution facilities. I previously stated that I did not expect our proposal would apply to SEFs—not because cybersecurity isn't just as important for them—but because many SEFs are still in the very early stages of operation.

But my fellow commissioners have expressed concerns about potential vulnerabilities and felt that we should propose that the requirements apply to SEFs at this time. I appreciate their views and am committed to working collaboratively to address these issues.

As always, we welcome public comment on this and its companion proposal, which will be carefully considered before taking any final action.

Appendix 3—Concurring Statement of Commissioner Sharon Y. Bowen

Today, we are considering two rule proposals that address an issue which is right at the heart of systemic risk in our markets—cybersecurity. The question that we face is: With a problem as immense as cybercrime, and the many measures already being employed to combat it, what would today's proposed rules accomplish? In answer to that question, I want to say a few words about our cybercrime challenge, what is currently being done to address it, and what I hope these proposed regulations would add to these efforts.

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

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

Given the magnitude of the problem, it is not at all surprising that a lot is already being done to address it. The Department of Homeland Security and others have been working with private firms to shore up defenses. Regulators have certainly been

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

[2] *Id.*

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

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

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

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

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

I think these rulemakings are a great first step in accomplishing that balance. There are many aspects of these proposals that I like. First, they set up a comprehensive testing regime by: (a) Defining the types of cybersecurity testing essential to fulfilling system safeguards testing obligations, including vulnerability testing, penetration testing, controls testing, security incident response plan testing, and enterprise technology risk assessment; (b) requiring internal reporting and review of testing results; and (c) mandating remediation of vulnerabilities and deficiencies. Further, for certain significant entities, based on trading volume, it requires heightened measures such as minimum frequency requirements for conducting certain testing, and specific requirements for the use of independent contractors.

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

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

Appendix 4—Statement of Commissioner J. Christopher Giancarlo

In one of our very first conversations over a year and a half ago, Chairman Massad and I discussed the many risks that cyber threats pose to trading markets. We agreed that cyber and overall system security is one of the most important issues facing markets today in terms of trading integrity and financial stability.

Earlier this year, I called for a ''bottom-up'' approach to combating cyber threats.[1] This approach involves a close and dynamic relationship between regulators and the marketplace. It also requires the continuous development of best practices, defensive strategies and response tactics through the leadership of market participants, operators and self-regulatory organizations. The job of the Commodity Futures Trading Commission (''CFTC'') as a regulator is to encourage, support, inform and empower this continuous development so that market participants adopt fully optimized and up-to-date cyber defenses.

It is appropriate that we are now taking up the subject of system safeguards. I commend Chairman Massad and CFTC staff for putting forth today's proposal. I believe it generally reflects the ''bottom-up'' approach I have advocated for market participants to follow industry adopted standards and best practices. I support its publication for notice and comment.

I believe it is right that the proposal covers not just designated contract markets (''DCMs''), but also swap execution facilities (''SEFs''). From my experience, SEFs are as concerned with cyber security as are DCMs. Nevertheless, it is true that the proposed rules will impose additional costs on some SEFs at a time when they are struggling to implement the myriad new Dodd-Frank requirements and obligations. Because system and cyber security should be a priority on our registrants' precious time and resources, the CFTC must find ways to alleviate unnecessary regulatory costs.

As I have said many times before, the best way to reduce unnecessary costs for SEFs is to correct the CFTC's flawed swaps trading rules that remain fundamentally mismatched to the distinct liquidity and trading dynamics of global swaps markets.[2] Attempting to

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

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

[1] *See* Guest Lecture of Commissioner J. Christopher Giancarlo, Harvard Law School, Fidelity Guest Lecture Series on International Finance (Dec. 1, 2015), *http://www.cftc.gov/PressRoom/SpeechesTestimony/opagiancarlo-11*; *see also* Keynote Address of CFTC Commissioner J. Christopher Giancarlo before the 2015 ISDA Annual Asia Pacific Conference, Top Down Financial Market Regulation: Disease Mislabeled as Cure (Oct. 26, 2015), *http://www.cftc.gov/PressRoom/SpeechesTestimony/opagiancarlo-10.*

[2] *See* CFTC Commissioner J. Christopher Giancarlo, Pro-Reform Reconsideration of the CFTC Swaps Trading Rules: Return to Dodd-Frank, White Paper (Jan. 29, 2015), *available at http://www.cftc.gov/idc/groups/public/@newsroom/documents/file/sefwhitepaper012915.pdf* (noting that this mismatch—and the application of this framework worldwide—has caused numerous harms, foremost of which is driving global market participants away from transacting with entities subject to CFTC swaps regulation, resulting in fragmented global swaps markets); *see also* Statement of Commissioner J. Christopher Giancarlo, Six Month Progress Report on CFTC Swaps Trading Rules: Incomplete Action and Fragmented Markets (Aug. 4, 2015), *http://www.cftc.gov/PressRoom/SpeechesTestimony/giancarlostatement080415. See also* International Swaps and Derivatives Association, *Cross-Border Fragmentation of Global Interest Rate Derivatives: The New Normal? First Half 2015 Update,* ISDA Research Note (Oct. 28, 2015), *http://www2.isda.org/functional-areas/research/research-notes/* (concluding that the market for euro interest rate swaps continues to remain fragmented in U.S. and non-U.S. liquidity pools ever since the introduction of the U.S. SEF regime in October 2013).

accommodate this misbegotten regulatory framework restricts the SEF industry's ability to deploy adequate resources for cyber defense. I also believe that the CFTC should provide a sufficient implementation period for any final rules so that market operators, especially smaller DCMs and SEFs, have adequate time to meet the new requirements.

Given the constantly morphing nature of cyber risk, the best defenses provide no guarantee of protection. Therefore, it would be a perverse and unfortunate result if any final system safeguards rule were to have a chilling effect on robust cyber security efforts. Market participants who abide by the rule should not be afraid of a ''double whammy'' of a destructive cyber-attack followed shortly thereafter by a CFTC enforcement action. Being hacked, by itself, cannot be considered a rule violation subject to enforcement. The CFTC should offer clear guidance to market participants regarding their obligations under the rule and designate safe harbors for compliance with it.[3] The CFTC should also indicate how it will measure market operators' compliance against industry standards given that the exact requirements of best practices can be open to interpretation.

In October, I called on the CFTC to add value to ongoing industry cyber security initiatives by designating a qualified cyber security information coordinator.[4] This individual would work with our registered entities to help them navigate the maze of Federal national security agencies and access the most up-to-date cyber security information available. I ask market participants to comment on the value and utility of such a designation.

As market regulators, we can have no naïve illusions that cyber belligerents—foreign and domestic—view the world's financial markets as anything other than 21st century battlefields. Cyber-attacks on trading markets will not diminish anytime soon. They will be relentless for years, if not decades, to come. Cyber risk is a threat for which Dodd-Frank provides no guidance whatsoever. Together, market regulators and the regulated community must make cyber and system security our first priority in time and attention. Today's proposal is a constructive step towards that goal. I look forward to reviewing thoughtful comments from market participants and the public.

[FR Doc. 2015–32143 Filed 12–22–15; 8:45 am]

BILLING CODE 6351–01–P

[3] The proposal requires market operators to follow industry adopted standards and best practices. Given the many organizations and U.S. government agencies (such as the U.S. Treasury Department's Financial Crimes Enforcement Network, the Office of Domestic Finance's Financial Sector Cyber Intelligence Group and the Office of Terrorist Financing and Financial Crimes) issuing cyber security procedures and advisories, there may be some question as to which procedures and advisories fall within industry best practices for purposes of complying with this rule proposal. To provide clarity, the CFTC should offer guidance to market participants regarding their obligations under the rule and designate safe harbors for compliance, as needed.

[4] *See supra* note 1.