REPORT

Futures & Derivatives Law

The Journal on the Law of Investment & Risk Management Products

October 2016 ▪ Volume 36 ▪ Issue 9

CFTC ISSUES CYBERSECURITY RULES ON SYSTEM SAFEGUARDS TESTING REQUIREMENTS

By Edward R. McNicholas, Michael Sackheim, Geeta Malhotra and Alison Looman

The authors are attorneys with the law firm Sidley Austin LLP, and may be reached at emcnicholas@sidley.com, msackheim@sidley.com, gmalhotra@sidley.com and alooman@sidley.com, respectively. This article is for informational purposes only and does not constitute legal advice. This information is not intended to create, and the receipt of it does not constitute, a lawyer-client relationship. Readers should not act upon this information without seeking advice from professional advisers. The content therein does not reflect the views of Sidley Austin LLP.

****

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

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

— Excerpt from statement of CFTC Chairman Timothy G. Massad, accompanying the adoption of the Final Rules

****

On September 8, 2016, the Commodity Futures Trading Commission ("**CFTC**") approved amendments ("**Final Rules**")[1] to its "system safeguards rules." The system safeguards rules obligate designated contract markets, swap execution facilities, and swap data repositories (for convenience, collectively referred to as "**Exchanges**") as well as derivatives clearing organizations ("**Clearinghouses**") to have in place cybersecurity programs of risk analysis and oversight. As part of such a program, Exchanges and Clearinghouses (collectively, "**Covered Entities**") must conduct testing and review sufficient to ensure their automated systems are reasonably reliable and secure, and have adequate scalable capacity.

The Final Rules are important because

they define the categories of testing the CFTC considers essential to fulfilling a Covered Entity's system safeguards testing responsibility. Although not expressly prescriptive, the Final Rules set specific standards by which Covered Entities must develop, test, and monitor their system safeguards.

The categories of tests required by the Final Rules are: (1) vulnerability testing, (2) penetration testing, (3) controls testing, (4) security incident response plan testing, and (5) enterprise technology risk assessment.[2] Certain covered entities—specifically, Clearinghouses, swap data repositories, and "covered designated contract markets" (as described below) (collectively, "**Enhanced Covered Entities**")—have additional requirements pertaining to the frequency of testing and the engagement of independent contractors. These tests and the additional requirements are the subject of this alert.

Background

The Final Rules come during a period of heightened focus by the CFTC (and regulators generally) on cybersecurity. Indeed, CFTC Chairman Timothy Massad recently observed, "[t]he risk of cyberattack probably represents the single greatest threat to the stability and integrity of our markets today."[3] Based on proposed rules the CFTC released in December 2015[4] and amended after a comment period, the Final Rules reflect the CFTC's belief that "a comprehensive cybersecurity program is crucial . . . to strengthen cyber defenses, mitigate operational, reputational, and financial risk, and maintain cyber resilience and the ability to recover from cyber attack."[5]

Senior Management and Board of Directors Reporting Required

Significantly, the Final Rules require that a Covered Entity's senior management and board of directors receive and review reports setting forth the results of this testing and assessment regime. A Covered Entity is also required to establish and follow appropriate procedures for the remediation of issues identified through such a review as well as for the evaluation of the effectiveness of the testing and assessment protocols.

The Required Categories of System Safeguards Testing

Vulnerability Testing. All Covered Entities must conduct vulnerability testing to determine what information and vulnerabilities may be discoverable through a reconnaissance of a Covered Entity's automated systems. Enhanced Covered Entities should conduct vulnerability testing no less than quarterly.

All Covered Entities must be in full compliance with the vulnerability testing requirements by March 20, 2017, which is the first business day after 180 days of the publication of the Final Rules in the Federal Register, which occurred on September 19, 2016 (the "**Effective Date**").[6]

Penetration Testing. All Covered Entities must also conduct penetration testing at a frequency determined by an appropriate risk analysis. The aim of penetration testing is to attempt to penetrate the Covered Entity's automated systems in order to identify and exploit vulnerabilities, such as by circumventing the security features of an automated system. Penetration testing is divided into "internal penetration testing" and "external penetration testing." "In-

ternal penetration testing" attempts to penetrate an automated system from inside the systems' boundaries. "External penetration testing" aims to penetrate an automated system from outside the systems' boundaries.

All Covered Entities must be in full compliance with the penetration testing requirements, and must have actually conducted and completed a penetration test, within one year of the Effective Date. Enhanced Covered Entities must conduct external penetration testing no less frequently than annually.

Controls Testing. All Covered Entities must also conduct controls testing at a frequency determined by an appropriate risk analysis. The aim of controls testing is to assess a Covered Entity's controls to determine whether such controls were implemented correctly, are operating as intended, and are enabling the covered entity to meet the requirements established by the system safeguards rule (including the Final Rules). "Controls" for this purpose are the safeguards or countermeasures employed by the Covered Entity 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 Covered Entity to fulfill its statutory and regulatory duties and responsibilities.

Enhanced Covered Entities must conduct testing of "key controls" no less frequently than every three years. "Key controls" are 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.

All Covered Entities may conduct controls testing on a rolling basis over the course of the required period. All Covered Entities must be in full compliance with the controls testing requirements within one year of the Effective Date. Enhanced Covered Entities have three years from the Effective Date to comply with their key control testing obligations.

Security Incident Response Plan Testing. All Covered Entities must also conduct security incident response plan testing at a frequency determined by an appropriate risk analysis. Enhanced Covered Entities must conduct security incident testing no less frequently than annually. The scope of such testing shall be sufficient to satisfy the Covered Entity's scope obligations under the Final Rules.

The aim of security incident response plan testing is to determine a 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 include checklist completion, walk-through or table-top exercises, simulations, and comprehensive exercises. The Covered Entity may coordinate its security incident response plan testing with other testing required by the Final Rules, or with testing of its business continuity-disaster recovery and crisis management plan.

A "security incident" is defined for this purposes as a cyber-security or physical security event that actually jeopardizes or has a significant likelihood of jeopardizing automated system operation, reliability, security or capacity, or the availability, confidentiality or integrity of data.

A "security incident response plan" is a writ-

ten plan documenting the Covered Entity's policies, controls, procedures, and resources for identifying, responding to, mitigating, and recovering from security incidents. The plan should document in writing the roles and responsibilities of its management, staff, and independent contractors in responding to a security incident. The plan should include the Covered 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. A security incident response plan may be a separate document, a business continuity-disaster recovery plan section, or an appendix dedicated to security incident response.

All Covered Entities must be in full compliance with the security incident response plan testing requirements, and must have actually created and completed testing of a security incident response plan, within 180 days of the Effective Date.

Enterprise Technology Risk Assessment. All Covered Entities must develop a written enterprise technology risk assessment, which includes an analysis of threats and vulnerabilities in the context of mitigating controls. The aim of an enterprise technology risk assessment is to identify, estimate, and prioritize risks to the Covered 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.

All Covered Entities must be in full compliance with the enterprise risk assessment requirements, and must have actually completed an assessment, within one year of the Effective Date. All Covered Entities must then conduct such an assessment at a frequency determined by an appropriate risk analysis, although they may do so by updating the previous assessment. Enhanced Covered Entities must conduct the analysis at least annually.

Appropriate Risk Analysis in General and as Applied to Scope

Although the Final Rules specify particular types of testing, for other matters, such as frequency and scope, they defer to a Covered Entity's "appropriate risk analysis," providing Covered Entities with some flexibility as to how they conduct their testing. Appropriate risk analysis does not require a separate, formal risk analysis other than that which is already required by the system safeguards rule's program of risk analysis and oversight.

With respect to scope, the Final Rules require testing that is broad enough to include all automated systems and controls that a Covered Entity's program of risk analysis and oversight indicates are necessary to identify risks and vulnerabilities that could enable an intruder, unauthorized user or insider to:

(a) interfere with operations or fulfillment of the Covered Entity's statutory and regulatory obligations;

(b) impair or degrade the reliability, security or adequate scalable capacity of the Covered Entity's automated systems;

(c) add to, delete, modify, exfiltrate or compromise the integrity of any data related to

such Covered Entity's regulated activities; or

(d) undertake any other unauthorized action affecting the Covered Entity's regulated activities or the hardware or software used in connection with those activities.

Covered Designated Contract Markets

As discussed above, Enhanced Covered Entities have certain testing obligations that do not attach to the other Covered Entities. The "Enhanced Covered Entities" are Clearinghouses, swap data repositories and "covered designated contract markets." A "covered designated contract market" is one that had an annual total trading volume in the previous year of five percent (5%) or more of the combined annual total trading volume of all designated contract markets regulated by the CFTC in the previous year. A covered designated contract market with annual total trading volume of less than five percent (5%) of total trading volume for three consecutive calendar years shall cease to be a covered designated contract market as of March 1 of the calendar year following such three consecutive calendar years.

Each such designated contract market shall provide the CFTC with its annual total trading volume for the previous year: (a) within 30 calendar days of the Effective Date; or (b) thereafter, by January 31 of the following calendar year. The CFTC shall then provide each such designated contract market its percentage of total trading volume for that year: (a) within 60 days of the Effective Date; or (b) thereafter, by February 28 of the following calendar year. For this purpose, "annual total trading volume" is the total number of all contracts traded on or pursuant to the rules of a designated contract market during a calendar year.

Who Can Conduct the Tests

In general, all testing set forth in the Final Rules may be conducted by independent contractors or employees who are not responsible for the development and operation of the systems or operations being tested. For certain categories of testing at certain frequencies, however, Enhanced Covered Entities must engage independent contractors:

(a) External Penetration Testing—Enhanced Covered Entities must annually engage an independent contractor to conduct external penetration testing. Any other external penetration testing may be conducted using an independent contractor or employees who are not responsible for the development or operation of the relevant system.

(b) Controls Testing of Key Controls—Enhanced Covered Entities shall engage an independent contractor to test and assess key controls no less frequently than every three years. Any other controls testing may be conducted using an independent contractor or employees who are not responsible for the development or operation of the relevant system.

Remediation

A Covered Entity must identify and document the vulnerabilities and deficiencies revealed by the tests and assessment. The Covered Entity then must analyze the risks presented by any discovered vulnerabilities and deficiencies to determine

and document whether to remediate or accept the risk. If the decision is made to remediate, the remediation must be done in a timely manner given the nature and magnitude of the risk.

Additional Items For Exchanges

The Final Rules also set in place a handful of additional requirements for Exchanges, including requiring the Exchanges to:

(a) incorporate a category called "enterprise risk management and governance" into the Exchanges' existing programs of risk analysis and oversight of automated systems and operations (see below);

(b) follow best practices, including in the testing of system safeguards and in the coordination of business continuity-disaster recovery plans with market participants and essential service providers (largely making mandatory previously existing guidance applicable to swap execution facilities and previously existing regulations applicable to designated contract merchants and swap data repositories);

(c) update their business-continuity plans at least annually; and

(d) produce books and records relating to system safeguards testing and requirements if so requested by the CFTC.

This category of "enterprise risk management and governance" includes:

(a) assessment, mitigation, and monitoring of security and technology risk;

(b) security and technology capital planning and investment;

(c) board of directors and management oversight of technology and security;

(d) information technology audit and controls assessments;

(e) remediation of deficiencies; and

(f) any other elements of enterprise risk management and governance included in generally accepted best practices.

All Exchanges must be in full compliance with all provisions of the Final Rules applicable to the Exchanges within one year, except that they must comply with their responsibility to produce system safeguards books and records upon CFTC request as of the Effective Date.

Additional Items For Clearinghouses

The Final Rules update the definition of "recovery time objective" applicable to Clearinghouses to make the language consistent with that used elsewhere in the system safeguard rule. The new definition, effective as of the Effective Date, is:

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

As for the "Additional Items for Exchanges," Provision (1)—regarding enterprise risk management and governance—does not extend to Clearinghouses. The CFTC stated that "any parallel requirements for [Clearinghouses] must be addressed in a more comprehensive fashion involving more than the system safeguards con-

text alone." The other Provisions—(2) (best practices), (3) (business continuity plan), and (4) (providing books and records upon CFTC request)— were not made applicable to the Clearinghouses, but only because similar provisions are already applicable to them.

Clearinghouses must be in compliance with all provisions of the Final Rules as of the Effective Date, unless otherwise stated above.

ENDNOTES:

[1]CFTC, System Safeguards Testing Requirements, 17 C.F.R. § 37, 38, 49, *available at* http://www.cftc.gov/idc/groups/public/@newsroom/documents/file/federalregister090816c.pdf (for Exchanges); CFTC, System Safeguards Testing Requirements for Derivatives Clearing Organizations, 17 C.F.R. § 39, *available at* http://www.cftc.gov/idc/groups/public/@newsroom/documents/file/federalregister090816b.pdf (for Clearinghouses).

[2]CFTC, Fact Sheet—Final Rules on System Safeguards Testing Requirements (Sept. 8, 2016), *available at* http://www.cftc.gov/idc/groups/public/@newsroom/documents/file/syssafeguard_factsheet090816.pdf.

[3]CFTC, Statement of Chairman Timothy Massad on the System Safeguards Testing Final Rules (Sept. 8, 2016), *available at* http://www.cftc.gov/PressRoom/SpeechesTestimony/massadstatement090816b.

[4]CFTC, System Safeguards Testing Requirements, 17 C.F.R. § 37, 38, 49, *available at* http://www.cftc.gov/idc/groups/public/@newsroom/documents/file/federalregister121615a.pdf (for Exchanges); CFTC, System Safeguards Testing Requirements for Derivatives Clearing Organizations, 17 C.F.R. § 39, *available at* http://www.cftc.gov/idc/groups/public/@newsroom/documents/file/federalregister121615b.pdf (for Clearinghouses).

[5]CFTC, Q & A—Final Rules on System Safeguards Testing Requirements (Sept. 8, 2016), *available at* http://www.cftc.gov/idc/groups/public/@newsroom/documents/file/syssafeguard_qa090816.pdf.

[6]System Safeguards Testing Requirements, 81 Fed. Reg. 64272 (Sept. 19, 2016), *available at* http://www.cftc.gov/idc/groups/public/@lrfederalregister/documents/file/2016-22174a.pdf (for Exchanges); System Safeguards Testing Requirements for Derivatives Clearing Organizations, 81 Fed. Reg. 64322 (Sept. 19, 2016), *available at* http://www.cftc.gov/idc/groups/public/@lrfederalregister/documents/file/2016-22413a.pdf (for Clearinghouses).