# Proposed CFTC cybersecurity testing rules for derivatives market infrastructure

Stephen M. Humenik and James Kwok

Stephen M. Humenik (shumenik@cov.com) is of counsel at Covington and Burling LLP, Washington, DC, USA. James Kwok is an associate at Covington and Burling LLP, New York, NY, USA.

**Abstract**

**Purpose** – *To summarize and analyze the CFTC's proposed enhanced cybersecurity testing rules for entities that run the core derivatives market infrastructure.*

**Design/methodology/approach** – *This article discusses the CFTC's proposed rulemaking related to cybersecurity testing, including enhanced cybersecurity testing requirements and guidance on risk analysis and oversight programs, as well as industry commentary on such rulemaking.*

**Findings** – *This article finds that the CFTC's recent proposed rulemaking has been met with approval generally by industry participants, and is part of a broader effort to protect against cybersecurity threats that may affect the functioning of financial markets.*

**Originality/value** – *Practical guidance from experienced futures and derivatives lawyers.*

**Keywords** *Cybersecurity, Commodity Furtures Trading Commission (CFTC), Derivatives clearing organization (DCO), Designated contract market (DCM), Swap data repository (SDR), Swap execution facility (SEF)*

**Paper type** *Technical paper*

The Commodity Futures Trading Commission ("CFTC") has recently proposed enhanced cybersecurity rules for derivatives clearing organizations ("DCOs"), designated contract markets ("DCMs"), swap execution facilities ("SEFs") and swap data repositories ("SDR"), which comprise the core derivatives market infrastructure. The proposed rules appear in two notices of proposed rulemaking issued by the CFTC[1]. Both notices propose enhanced cybersecurity testing requirements for CFTC-registered entities. One of the notices also provides guidance, for DCMs, SEFs and SDRs, on risk analysis and oversight programs.

The proposed rules, which the CFTC voted unanimously to approve, are in response to evolving and increasingly sophisticated cyber threats that financial firms face. Specifically, the CFTC has cited the increase in the number of cyberattacks on financial institutions, the threat of persistent undetected cyberattacks and the interconnectedness of financial firms facing cyberattacks as motivations for the implementation of enhanced cybersecurity testing and risk analysis and oversight rules[2]. The proposed rules were subject to public comment until February 22, 2016.

## 1. Enhanced cybersecurity testing requirements

The proposed rules augment existing CFTC regulations concerning cybersecurity testing for DCOs, DCMs, SEFs and SDRs (each such entity, a "Registrant"). Under current CFTC Regulation 39.18, DCOs are required to establish and maintain risk analysis and oversight programs as part of their systems. Specifically, DCOs must follow "generally accepted standards and industry best practices with respect to the development, operation,

reliability, security, and capacity of automated systems" when implementing risk analysis and oversight programs[3]. DCMs, SEFs and SDRs similarly are not subject to specific testing requirements under current CFTC rules[4]. The proposed rules, if implemented, would supplement the CFTC's current system safeguards rules by requiring Registrants to conduct five types of systems testing and assessment: vulnerability testing, penetration testing, information security controls testing, security incident response plan testing and enterprise technology risk assessment.

Testing generally must be broad in scope such that a Registrant, as a result of the testing, can identify vulnerabilities that could allow a person to: (i) interfere with a Registrant's operations, (ii) impair or degrade the reliability or capacity of the Registrant's automated systems, (iii) add to, delete, modify, exfiltrate or compromise the integrity of any data related to the Registrant's regulated activities or (iv) undertake any other unauthorized action affecting the Registrant's regulated activities or the hardware or software used in connection with those activities[5].

For covered DCMs[6], DCOs and SDRs, the five types of testing are required at a minimum either quarterly, annually or bi-annually. SEFs generally are required to undertake testing at a frequency as determined through its own risk analysis.

The five types of systems testing and assessment specifically set forth in the proposed rules are as follows[7]:

*Vulnerability testing*. The proposed rules require that a Registrant determine what information may be discoverable through a reconnaissance analysis of its automated systems and the vulnerabilities present on those systems.

*Penetration testing*. The proposed rules require internal and external penetration testing to evaluate a Registrant's vulnerabilities from both inside and outside its systems' boundaries.

*Controls testing*. The proposed rules require testing to determine whether a Registrant's controls are implemented correctly and operating as intended. Controls testing includes evaluation of each control included in a Registrant's risk analysis and oversight program.

*Security incident response plan testing*. The proposed rules require the evaluation of security incident response plans to determine the plans' effectiveness. The evaluation may include checklist completion, walkthrough or table-top exercises, simulations and comprehensive exercises. A security incident response plan should include a Registrant's classification of security incidents; 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.

*Enterprise technology risk assessment*. The proposed rules require a Registrant to undertake an assessment analyzing threats and vulnerabilities in the context of mitigating controls. The assessment should identify, estimate and prioritize risks to the Registrant's operations or assets, or to market participants, individuals or other entities resulting from impairment of the Registrant's automated systems.

## 2. Risk analysis and oversight guidance

The proposed rules, if adopted, also would provide additional guidance with respect to current system safeguard rules pertinent to DCMs, SEFs and SDRs. Specifically, the proposed rules require that Registrants' risk analysis and oversight programs address the following categories: enterprise risk management and governance, information security,

business continuity-disaster recovery planning and resources, capacity and performance planning, systems operations, systems development and quality assurance and physical security and environmental controls. In the release to the proposed rules, the CFTC stressed that the types of activities listed in these categories are non-exhaustive, and are therefore meant only to highlight important aspects of the risk analysis and oversight categories. The following are brief descriptions of the categories of risk analysis and oversight programs specifically set forth in the proposed rules[8]:

1. *Enterprise risk management and governance*. This category includes 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 and other elements of enterprise risk management and governance included in generally accepted best practices.
2. *Information security*. This category includes controls relating to access to systems and data; 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; system and information integrity; vulnerability management; penetration testing; security incident response and management and other elements of information security included in generally accepted best practices.
3. *Business continuity-disaster recovery planning and resources*. This category includes regular, periodic testing and review of business continuity-disaster recovery capabilities and other elements of business continuity-disaster recovery planning and resources included in generally accepted best practices.
4. *Capacity and performance planning*. This category includes controls for monitoring the SEF's systems to ensure adequate capacity and other elements of capacity and performance planning *included in generally accepted best practices.*
5. *Systems operations*. This category includes system maintenance, configuration management, event and problem response and management and other elements of system operations included in generally accepted best practices.
6. *Systems development and quality assurance*. This category includes development of requirements, pre-production and regression testing, change management procedures and approvals, outsourcing and vendor management, training in secure coding practices and other elements of systems development and quality assurance included in generally accepted best practices.
7. *Physical security and environmental controls*. This category includes physical access and monitoring; power, telecommunication and environmental controls; fire protection and other elements of physical security and environmental controls included in generally accepted best practices.

## 3. Industry response and CFTC's cybersecurity focus

Industry participants have expressed general approval for the proposed rulemakings. The Chicago Board of Exchange ("CBOE") stressed the importance of such rules being "principles-based and not prescriptive," given that the appropriate level of cybersecurity testing will vary from organization to organization[9]. Certain industry participants have also provided specific suggestions for improving on the cybersecurity testing rules. For example, FireEye, a cybersecurity firm, has suggested that the testing requirements also

address the possibility that attackers may remain undetected in a system to constantly compromise, manipulate and/or steal sensitive data[10]. The North American Derivatives Exchange ("Nadex") echoed one of Commissioner Giancarlo's concerns regarding the proposed rule, encouraging the Commission to consider a "safe harbor" provision so that entities subject to cyberattacks are not also subject to enforcement actions because of such cyberattacks[11].

The proposed cybersecurity testing rules also reflect the growing importance of cybersecurity to the CFTC. In recent testimony to a US House Appropriations Committee, Chairman Timothy Massad called cyberattacks "perhaps the greatest single threat to the orderly functioning of our markets"[12]. In that testimony, Chairman Massad also announced that the CFTC would enhance its examination capabilities in this area, pointing out that "the risk of cyber-attacks is of particular concern with clearinghouses and warrants examinations specifically dedicated to that subject"[13].

The CFTC's recent action follows the issuance of an interpretive notice from the National Futures Association ("NFA") concerning the supervision of information systems security programs for other CFTC-registrants, specifically, swap dealers, futures commission merchants, commodity pool operators, introducing brokers, commodity trading advisors and major swap participants[14]. With these two actions, the new CFTC cybersecurity regulatory landscape is coming into focus.

Market participants should understand and implement any new rules in a manner practical to a market participant's business and respond to a cyberattack, if and when one should occur.

## Notes

1. *System Safeguards Testing Requirements for Derivatives Clearing Organizations*. 80 Fed. Reg. 80113 (December 23, 2015) and *System Safeguards Testing Requirements*. 80 Fed. Reg. 80139 (December 23, 2015).
2. *See* 80 Fed. Reg. at 80114-15 and 80140.
3. CFTC Regulation 39.18(d).
4. *See* CFTC Regulations 38.1051 (for DCMs), 37.1401 (for SEFs) and 49.24 (for SDRs).
5. 80 Fed. Reg. at 80175-76.
6. Covered DCMs are DCMs whose annual total trading volume is five percent or more of the annual total trading volume of all DCMs regulated by the CFTC. Every DCM would be required to report its total trading volume to the CFTC annually if the proposed rules are adopted. *See* 80 Fed. Reg. at 80160-61.
7. 80 Fed. Reg. at 80133-36 and 80186-89.
8. 80 Fed. Reg. 80139.
9. *See, e.g.* Comment Letter from CBOE Futures Exchange, LLC (http://comments.cftc.gov/PublicComments/ViewComment.aspx?id=60658&SearchText=), Comment Letter from Intercontinental Exchange Inc. (http://comments.cftc.gov/PublicComments/ViewComment.aspx?id=60653&SearchText=)
10. Comment Letter from FireEye (http://comments.cftc.gov/PublicComments/ViewComment.aspx?id=60655&SearchText=)
11. Comment Letter from Nadex (http://comments.cftc.gov/PublicComments/ViewComment.aspx?id=60661&SearchText=)

12. Testimony of Chairman Timothy Massad before the U.S. House Appropriations Committee, Subcommittee on Agriculture, Rural Development, Food and Drug Administration and Related Agencies at www.cftc.gov/PressRoom/SpeechesTestimony/opamassad-42.

13. Id.

14. National Futures Association Interpretive Notice 9070 - NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs (effective Mar. 1, 2016), available at: www.nfa.futures.org/nfamanual/NFAManual.aspx?RuleID=9070&Section=9.


## Corresponding author

Stephen M. Humenik can be contacted at: shumenik@cov.com