COVINGTON

Cybersecurity: CFTC Proposes New Cybersecurity Testing Rules for Derivatives Market Infrastructure

January 12, 2016

Futures and Derivatives

The Commodity Futures Trading Commission ("CFTC") has recently proposed enhanced cybersecurity rules for entities that run the core derivatives market infrastructure: derivatives clearing organizations ("DCOs"), designated contract markets ("DCMs"), swap execution facilities ("SEFs") and swap data repositories ("SDR"). The proposed rules appear in two notices of proposed rulemaking.[1] Both notices propose enhanced cybersecurity testing requirements for CFTC-registered entities. One of the notices also provides guidance, specifically 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 cyber attacks on financial institutions, the threat of persistent undetected cyber attacks and the interconnectedness of financial firms facing cyber attacks as motivations for the implementation of enhanced cybersecurity testing and risk analysis and oversight rules. The proposed rules will be subject to public comment until February 22, 2016.

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.[2] DCMs, SEFs and SDRs similarly are not subject to specific testing requirements under current CFTC rules. 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)

[1] *System Safeguards Testing Requirements for Derivatives Clearing Organizations*. 80 Fed. Reg. 80114 (December 23, 2015) and *System Safeguards Testing Requirements*. 80 Fed. Reg. 80140 (December 23, 2015).
[2] CFTC Regulation 39.18(d).

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.

For covered DCMs,[3] 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 are as follows:

1. *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.
2. *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.
3. *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.
4. *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.
5. *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.

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.[4] 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,

[3] 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 under the proposed rules. *See* 80 Fed. Reg. at 80160-61.
[4] *See* CFTC Regulations 38.1050, 37.1400 and 49.24.

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.[5] The following summarizes the categories of risk analysis and oversight programs:

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.

Conclusion

The CFTC's recent action follows a new interpretive notice from the National Futures Association ("NFA") concerning the supervision of information systems security programs for

[5] 80 Fed. Reg. at 80143.

other CFTC-registrants, specifically, swap dealers, futures commission merchants, commodity pool operators, introducing brokers, commodity trading advisors and major swap participants.[6] With these two actions the new CFTC cybersecurity regulatory landscape is coming into focus.

Covington's expertise with CFTC regulation and cybersecurity prevention, investigation and remediation means we remain well positioned to help market participants 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.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Securities practice group:

Stephen Humenik	+1 202 662 5803	shumenik@cov.com
David Fagan	+1 202 662 5291	dfagan@cov.com
Bruce Bennett	+1 212 841 1060	bbennett@cov.com
Ashden Fein	+1 202 662 5116	afein@cov.com
Ronald Hewitt	+1 212 841 1220	rhewitt@cov.com
James Kwok	+1 212 841 1033	jkwok@cov.com
Jason Grimes	+1 202 662 5846	jgrimes@cov.com

[6] *See* Covington's recent Client Alert on the NFA's interpretive notice: Cybersecurity: Recent CFTC and NFA Activity.