Commodity Futures Trading Commission
Office of Public Affairs
Three Lafayette Centre
1155 21st Street, NW
Washington, DC 20581
www.cftc.gov

September 8, 2016

Fact Sheet – Final Rules on System Safeguards Testing Requirements

The Commodity Futures Trading Commission ("Commission") is adopting amendments to its system safeguards rules for designated contract markets, swap execution facilities, and swap data repositories (the "Exchange Final Rules") and for derivatives clearing organizations (the "Clearing Final Rules") (collectively, the "Final Rules"). The Final Rules will be published in the Federal Register.

The Final Rules enhance and clarify existing requirements relating to cybersecurity testing and system safeguards risk analysis by, among other things, specifying and defining five types of cybersecurity testing essential to a sound system safeguards program. The five types of testing include (1) vulnerability testing, (2) penetration testing, (3) controls testing, (4) security incident response plan testing, and (5) enterprise technology risk assessment.

For specified registrants, the Final Rules also provide minimum frequency requirements for testing, and requirements for them to engage independent contractors to conduct some of the required testing.

The Final Rules also clarify rule provisions relating to the scope of system safeguards testing, internal reporting and review of testing results, and remediation of identified vulnerabilities and deficiencies.

Definitions Related to Cybersecurity Testing

The Final Rules define terms related to cybersecurity testing, including "controls", "controls testing", "enterprise technology risk assessment", "external penetration testing", "internal penetration testing", "key controls", "security incident", "security incident response plan", "security incident response plan testing", and "vulnerability testing". These defined terms are included in Commission regulations applicable to designated contract markets, swap execution facilities, swap data repositories, and derivatives clearing organizations (the "registrants"), and generally mean the following:

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

"Controls testing" means the assessment of a registrant's controls to determine whether such controls are implemented correctly, are operating as intended, and are enabling the registrant to meet the requirements established by the relevant Commission regulations.

"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 a registrant's 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.

"External penetration testing" means attempts to penetrate a registrant'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 a registrant'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 cybersecurity or physical security event that actually jeopardizes or has a significant likelihood of jeopardizing automated system operation, reliability, security, or capacity, or the availability, confidentiality or integrity of data.

"Security incident response plan" means a written plan documenting a registrant'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 registrant'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 registrant'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.

Key Elements of the Final Rules

Specified Cybersecurity Testing. All derivatives clearing organizations, designated contract markets, swap execution facilities, and swap data repositories are required to conduct the following types of cybersecurity testing: (1) vulnerability testing, (2) penetration testing, (3) controls testing, (4) security incident response plan testing, and (5) enterprise technology risk assessments.

Minimum Testing Frequency. Specified registrants are subject to minimum testing frequencies for the specified types of cybersecurity testing.

Use of Independent Contractors. Specified registrants are required to use independent contractors for certain types of cybersecurity testing.

Testing Scope. The Final Rules require that the scope of all testing and assessment required by Commission regulations be broad enough to include the testing of automated systems and controls that the registrant's program of risk analysis and oversight and its current cybersecurity threat analysis indicate is necessary to identify risks and vulnerabilities that could enable an intruder or unauthorized user or insider to:

a. interfere with the registrant's operations or with fulfillment of its statutory and regulatory responsibilities;

b. impair or degrade the reliability, security, or capacity of the registrant's automated systems;

c. add to, delete, modify, exfiltrate, or compromise the integrity of any data related to the registrant's regulated activities; or

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

Internal Reporting, Review, and Remediation. The Final Rules require reports on testing protocols and results to be communicated to, and reviewed by, the registrant's senior management and board of directors. Registrants are required to establish and follow appropriate procedures for the remediation of issues identified through such review, and for evaluation of the effectiveness of testing and assessment protocols. Accordingly, registrants are required to identify and document the vulnerabilities and deficiencies revealed by the testing and assessment required by the applicable system safeguards rules. The registrants are also required to

conduct and document an appropriate analysis of the risks presented by such vulnerabilities and deficiencies to determine and document whether to remediate or accept each risk.

Enterprise Risk Management and Governance

The Exchange Final Rules add enterprise risk management and governance to the list of required categories of system safeguards-related risk analysis and oversight. As stated in the Exchange Final Rules, enterprise risk management and governance includes, but is not limited to, 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.

Enterprise risk management and governance also includes any other elements of enterprise risk management and governance that are included in generally accepted best practices.