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

September 8, 2016

Q & A – 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").

1. What cybersecurity tests are addressed by the Final Rules?

As discussed more fully in the Final Rules, a comprehensive cybersecurity testing program is crucial to efforts by derivatives clearing organizations, designated contract markets, swap execution facilities, and swap data repositories to strengthen cyber defenses, mitigate operational, reputational, and financial risk, and maintain cyber resilience and the ability to recover from cyber attack. Accordingly, the Final Rules seek to enhance and clarify existing requirements relating to system safeguards risk analysis and cybersecurity testing by, among other things, specifying and defining five types of cybersecurity testing essential to a sound system safeguards program.

Under the Final Rules, 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.

2. How often do derivatives clearing organizations, designated contract markets, swap execution facilities, and swap data repositories have to conduct cybersecurity testing?

The Final Rules call for all derivatives clearing organizations, designated contract markets, swap execution facilities, and swap data repositories to conduct cybersecurity testing at a frequency determined by an appropriate risk analysis. In addition, the Final Rules specify the following minimum frequency requirements for testing by derivatives clearing organizations, covered designated contract markets (as defined in the Exchange Final Rules), and swap data repositories:

1. Vulnerability testing should be conducted no less frequently than quarterly;
2. Internal penetration testing, external penetration testing, security incident response plan testing, and enterprise technology risk assessments should be conducted no less frequently than annually; and
3. Controls testing may be conducted on a rolling basis but each key control must be tested no less frequently than every three years.

3. Who should conduct cybersecurity testing?

Certain tests may be conducted using employees of the derivatives clearing organization, designated contract market, swap execution facility, or swap data repository who are not responsible for development or operation of the systems or capabilities being tested. The Final Rules require derivatives clearing organizations, covered designated contract markets, and swap data repositories to engage independent contractors to conduct some

of the required tests. For example, the Final Rules require that independent contractors conduct the required annual external penetration test. With respect to controls testing, the Final Rules require that independent contractors test each of the organization's key controls at least once every three years.

4. What are the other requirements in the Final Rules?

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. Specifically, the Final Rules require that reports on testing protocols and results be communicated to, and reviewed by, the registrant's senior management and board of directors. Derivatives clearing organizations, designated contract markets, swap execution facilities, and swap data repositories are also required to establish and follow appropriate procedures for the remediation of issues identified through such testing and review, and for evaluation of the effectiveness of testing and assessment protocols. Accordingly, the derivatives clearing organizations, designated contract markets, swap data repositories, and swap execution facilities are required to identify and document the vulnerabilities and deficiencies in their systems 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.

5. Are there substantive differences between the Exchange Final Rules and the Clearing Final Rules?

The Exchange Final Rules and the Clearing Final Rules are parallel rulemakings, although there are a few differences. The Clearing Final Rules apply to all derivatives clearing organizations. Most of the requirements in the Exchange Final Rules apply to all designated contract markets, swap execution facilities, and swap data repositories, although the new minimum testing frequency and independent contractor testing requirements apply only to covered designated contract markets and all swap data repositories. The Exchange Final Rules also 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.

6. What is a covered designated contract market?

The Exchange Final Rules define a covered designated contract market as 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 the Exchange Final Rules. 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 three consecutive calendar years ceases to be a covered designated contract market as of March 1 of the calendar year following such three consecutive calendar years.

See also the Fact Sheet regarding the Final Rules, available on the Commission's website.