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

December 16, 2015

Q & A – Notice of Proposed Rulemakings on System Safeguards Testing Requirements

The Commodity Futures Trading Commission proposed amendments to its system safeguards rules for designated contract markets, swap execution facilities, and swap data repositories (the "Exchange Proposal") and for derivatives clearing organizations (the "Clearing Proposal") (collectively, the "Proposals").

1. What cybersecurity tests are addressed by the Proposals?

As discussed more fully in the Proposals, 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 ability to recover from cyber attack. Accordingly, the Proposals 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 Proposals, derivatives clearing organizations, designated contract markets, swap execution facilities, and swap data repositories would be 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 Proposals 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 Proposals would specify the following minimum frequency requirements for testing by derivatives clearing organizations, covered designated contract markets, 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, including testing of all controls, should be conducted no less frequently than every two 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 Proposals would 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 Proposal would require that independent contractors must conduct two of the required quarterly vulnerability tests each year, as well as the required annual external

penetration test. With respect to controls testing, the Proposals would require that independent contractors test the organization's key controls.

4. What are the other requirements in the Proposals?

The Proposals also would 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 Proposals would require that reports on testing protocols and results be communicated to, and reviewed by, the regulatee's senior management and board of directors. Derivatives clearing organizations, designated contract markets, swap execution facilities, and swap data repositories would also be required to establish and follow appropriate procedures for remediation of issues identified through such testing and review, and for evaluation of the effectiveness of testing and assessment protocols. Accordingly, derivatives clearing organizations, designated contract markets, swap execution facilities, and swap data repositories would be required to analyze the results of the testing and assessment required by the applicable system safeguards rules, in order to identify all vulnerabilities and deficiencies in their systems, and to remediate those vulnerabilities and deficiencies to the extent necessary to enable them to fulfill their statutory and regulatory obligations.

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

The Exchange Proposal and the Clearing Proposal are parallel proposals, although there are a few differences. The Clearing Proposal would apply to all derivatives clearing organizations. Most of the requirements in the Exchange Proposal would apply to all designated contract markets, swap execution facilities, and swap data repositories, although the new minimum testing frequency and independent contractor testing requirements would apply only to covered designated contract markets (as defined in the Exchange Proposal) and all swap data repositories. The Exchange Proposal also adds enterprise risk management and governance to the list of required categories of system safeguards-related risk analysis and oversight. As proposed, 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 would also include 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 Proposal defines 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 that would be provided to the Commission by each designated contract market pursuant to the procedure set forth in the Exchange Proposal. 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 two consecutive calendar years would cease to be a covered designated contract market as of March 1 of the calendar year following such two consecutive calendar years.

7. Does the Exchange Proposal address the concept of "covered SEFs"?

The Exchange Proposal includes an Advance Notice of Proposed Rulemaking, which notes that the Commission is considering whether, in a future Proposal, to apply minimum testing frequency and independent contractor testing requirements to certain SEFs to be defined as "covered SEFs."

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