February 22, 2016

Via Electronic Submission

Christopher Kirkpatrick
Secretary of the Commission
U.S. Commodity Futures Trading Commission
Three Lafayette Centre
1155 21st Street NW
Washington, DC 20581

RE: ***Comments on Proposed System Safeguards Testing Requirements for Derivatives Clearing Organizations RIN 3038-AE29 and Proposed System Safeguards Testing Requirements for Designated Contract Markets, Swap Execution Facilities and Swap Data Repositories RIN 3038-AE30***

Dear Mr. Kirkpatrick:

Intercontinental Exchange, Inc. ("ICE") appreciates the opportunity to provide comments and recommendations to the Commodity Futures Trading Commission's ("CFTC" or "Commission") proposed rulemaking amending the system safeguards rules for designated contract markets ("DCMs"), swap execution facilities ("SEFs") and swap data repositories ("SDRs") and its proposed rulemaking amending the system safeguards rules for Derivatives Clearing Organizations (DCOs) (collectively the "Proposal" or "Proposed Rules"). As background, ICE operates ICE Futures US, a DCM; ICE Clear US, ICE Clear Europe and ICE Clear Credit; DCOs, ICE Swap Trade, a SEF; and ICE Trade Vault, a SDR(collectively "Regulated Entities"). As the operator of U.S. and international exchanges, clearing houses, trade repositories and a swap execution facilities (collectively "Regulated Entities"), ICE has a practical perspective of the system safeguards rules and the effects of the proposed modifications to the current system safeguards regime. Considering these factors, ICE and its Regulated Entities respectfully offer the following comments regarding the framework outlined in the Commission's Proposed Rules.

Executive Summary

ICE supports the Commission's efforts to improve and enhance system safeguards requirements and address cybersecurity testing. Cybersecurity and system safeguards are paramount to the functioning of the derivatives markets. We encourage the Commission to take a reasoned approach to these amendments and hope that the resulting structure will promote well-functioning markets that continue to allow the Regulated Entities to effectively manage risk. We believe, however, there are certain areas where further clarification or modification is warranted, particularly as the Proposal is meant to cover a variety of entities that provide diverse

services, operate in different markets and have different risk profiles. We specifically encourage the Commission to consider:

- Allowing internal parties of an organization to conduct vulnerability scanning;
- Removing the controls testing and enterprise risk management assessment requirements;
- Permitting independent internal groups to continue providing testing and monitoring functions.

General Comments

The Commission should take a principal based approach when proposing and implementing amendments to the system safeguards regulations. ICE believes that any final rulemaking should be clearly identified and construed as high level guidance. This would allow the Regulated Entities to retain the flexibility to develop and implement approaches and tools to address cyber security and system safeguards issues (i) in a manner that is appropriate for each Regulated Entity's unique risks and circumstances, and (ii) that comport with, and facilitate the Regulated Entities leveraging relevant industry recognized best practices as they evolve and mature. This is critical both from the perspective of the evolving nature of cyber threats and means of response, as well as to avoid the risk of overly prescriptive regulations that would neither be cost effective nor necessarily achieve the desired level of protection. The Regulated Entities need latitude and flexibility when monitoring business risks and determining compliance with regulations. ICE's Regulated Entities currently have extensive system safeguard and cybersecurity programs pursuant to existing Commission rules. Since these programs are already in effect and CFTC standards in place, the need to codify additional requirements is minimal. Overly prescriptive regulations could hinder existing best practices employed today.

The Commission should also be mindful that the proposed testing requirements do not themselves guarantee identification of any and all vulnerabilities. The Regulated Entities make best efforts to test all systems and controls to identify vulnerabilities; however, it is impossible to predict and test for all scenarios. The Commission must take this into consideration and provide adequate flexibility when drafting and implementing the Proposed Regulations.

In addition, the Commission has proposed two sets of rules reflecting its organization (the Division of Market Oversight drafted the rules for SEFs, DCMs, and SDRs and the Division of Clearing and Risk drafted the rules for DCOs). However, many of the entities affected by the rules operate DCMs and DCOs and likely manage system safeguards and enterprise risk at a companywide level. ICE encourages the Commission to propose consistent requirements across Regulated Entities to avoid varying rules for the same objectives. If the Commission believes that varying approaches are warranted, it should explain why and how the rules vary. Safeguards mandating different standards for enterprise risks and system safeguards are difficult to implement and inherently adds more risk into an organization's operation.

Lastly, it is important for the Commission to consider the potential impact of these Proposed Rules on current system safeguards and information security practices. Specifically, the Commission should be flexible in its definitions of "independent professional" and "employees of the Regulated entity who are not responsible for the development or operation of the systems and capabilities being assessed." The Commission should be mindful to allow a company to retain its independent internal groups, such as internal audit, to monitor and test elements of its business. As proposed, these definitions are broad and the Commission should clarify that certain internal groups are considered "independent professionals" or "employees of the Regulated entity who are not responsible for the development or operation of the systems and capabilities being assessed." Internal auditors, for example, are inherently independent from the business unit they are testing and play an important role in monitoring compliance. Not allowing internal auditors to conduct certain system safeguards or information security testing could disrupt long standing practices in addition to adding substantial costs to the Regulated Entities. ICE suggests the Proposed Rule include language stating that an "independent professional" or "employees of the Regulated entity who are not responsible for the development or operation of the systems and capabilities being assessed" can include persons employed by the firm but not specifically responsible for the testing or documentation in question and as such are considered independent. This will allow the flexibility for internal groups to continue monitoring and observing certain system safeguard and information security exercises.

Specific Comments

1. *Cyber Security Program*

The Commission's aim to clarify and enhance rules in response to escalating and evolving cybersecurity threats is timely and welcome. The emphasis on testing prudently focuses behavior and examination on tasks that can prevent active and observed cybersecurity exploitation. The Proposed Rules should stay true to that theme and focus on the specific testing elements that have been identified as crucial to an effective security program. Deviation from that focus should be minimal, specific, and directly relevant to addressing escalating threats. The Commission should not prescribe additional regulations for areas that the Commission has failed to identify as contributing to increased cybersecurity risk. Regulated Entities currently have extensive system safeguards and cyber security programs pursuant to existing rules both in the U.S. and globally. Since standards are already in place, ICE recommends only implementing additional requirements where the Commission has proven increased risks or in instances not currently covered by the existing rules. The Commission should instead focus on testing requirements which result in behavioral changes and examination activity directly responsive to the identified testing needs.

To that end, ICE supports including vulnerability testing, external penetration testing, internal penetration testing and security incident response plan testing in the Proposed Rules. These testing components are on point with the Commission's intent to drive productive security testing and should be retained, subject to certain corrections and refinements. ICE however believes that the proposed controls testing and enterprise technology risk assessment

requirements are already adequately addressed in existing rules, both in the U.S. and globally, and current examination coverage. Accordingly, the Commission should eliminate the controls testing and enterprise technology risk assessment requirements from the Proposed Rules. Attempting to mandate controls testing and enterprise technology risk assessments will result in inconsistent and confused implementation, distract from useful security activity, and generate a superset of results that are already published in a more focused fashion through vulnerability, external, internal or security response plan testing. In addition, the proposed enterprise technology risk assessment is not cyber-specific and neither voiced around threats and vulnerabilities nor focused on the CIA (Confidentiality, Integrity, Availability) triad. The enterprise technology risk assessment should also be the function of an enterprise risk program separate from the information security groups.

The Commission should also note that the testing required in the Proposed Rules could create thousands of reviewable findings. The Commission has proposed that all findings be elevated to senior management and the board of directors. In order to focus on the highest priority risks and not inundate the board and senior management with volumes of low risk findings, the Commission should only require high-priority test findings of internal reports to be reviewed by senior management. It is appropriate for the Regulated Entities to bundle high-priority findings under risk statements which add context and mitigating controls to evaluate the true impact of any finding presented to senior management. In addition, ICE believes these high-priority findings should be circulated to senior management as the board of directors is not an appropriate audience for even these filtered tactical (as opposed to strategic) risks. The board of directors should instead be apprised of enterprise-level high risk issues including cybersecurity risks identified in testing or other activities only when they cross an identified threshold.

2. *Vulnerability Testing*

The Proposed Rules require the Regulated Entities to conduct vulnerability testing at a frequency determined by the appropriate risk analysis, but no less frequently than quarterly. ICE agrees with the quarterly requirement but proposes that if the Regulated Entities meet the quarterly requirement, the Regulated Entities should not be subject to a formal risk assessment to potentially determine a higher testing frequency as the Commission has not provided evidence that a higher frequency is warranted.

Furthermore, the Commission should remove the authenticated vulnerability scanning requirement from vulnerability testing. Vulnerability scanning is defined and differentiated from penetration testing by its automated nature. The Commission's requirement to conduct vulnerability scanning on an authenticated basis increases the quantity of findings potentially diluting and obscuring important results. Introducing authentication also increases the cost and time of a scan and increases risk by requiring an operating system login to be created and maintained on a new system. In practice, vulnerabilities that are detected via authenticated scans (and not detected otherwise) are those that would allow a valid operating system user with interactive login rights the ability to escalate privileges. This means a vulnerability that would

allow an authorized system administrator to elevate to "root" access. This is appropriate and important for systems that allow interactive login at the operating system level to untrusted sources such as servers used in the military or a university. In a financial infrastructure, however, interactive login is only used by system administrators who usually have the ability to gain root access as needed. In sum, authenticated scans may be useful occasionally for ad hoc tests however authenticated scans should not be mandated as part of the Proposed Rules.

The Commission should also provide the flexibility for vulnerability scanning to be conducted by internal parties of an organization as internal parties have the most accurate knowledge and experience with the systems. The deployment of a vulnerability scanning infrastructure is a complex and sensitive project that requires intimate network knowledge, change control interaction and a high level of care to not jeopardize live systems. Vulnerability scanners can be hazardous to the systems and can cause issues during deployment. As a result, vulnerability scanners are carefully deployed and tested in many environments, often taking years to establish correctly. It would be neither cost-effective nor secure to mandate a third-party handle this work. Vulnerability scanners should be staffed by internal employees working closely with change control and operations staff to schedule, conduct and terminate scans carefully. Requiring Regulated Entities to conduct third-party vulnerability scanning is costly and potentially dangerous without adding substantial value. Accordingly, ICE strongly recommends that the Commission not require third-party vulnerability scanning.

3. External and Internal Penetration Testing

The Proposed Rules require the Regulated Entities to conduct external and internal penetration testing at a frequency determined by appropriate risk analysis, but no less frequently than annually. ICE agrees with the annual requirement but proposes that if the Regulated Entities meet the annual requirement, the entities should not be subject to a formal risk assessment to potentially determine a higher testing frequency as the Commission has not provided evidence that a higher frequency is warranted.

ICE also recommends amending the proposed definitions of external and internal penetration testing to specify scenario or capture-the-flag testing intended to compromise the system holistically via all available means including technical exploit, social engineering, and lateral traversal and to clarify that external and internal penetration testing is not intended to cover application-specific tests. The Commission should be silent on parameters for voluntary internal testing allowing each regulated entity to determine its own methodology for voluntary testing.

4. Controls Testing

Organizations often have thousands of controls; many of which do not require testing. Controls testing is difficult to implement and define because few organizations have a distinct (and static) universe of controls and key controls. Organizations often identify and iterate controls during a risk assessment in the context of a specific attributable risk. The concept of

controls testing should not mean testing each control individually. Furthermore, the concept of a key control is not universally adopted. Risks are evaluated after reviewing vulnerabilities and findings alongside all relevant controls. All controls and findings in concert contribute to a risk scoring. A control identified as "key" would actually constitute a concentration risk if it were truly "critically important for effective system safeguards". The goal is not to test such controls; but to eliminate reliance on them. Even when a control is testable, such as a firewall, the controls testing is already covered by penetration testing. Requiring organizations to formulate and test, "key controls", will most likely result in organizations documenting far fewer controls. The key controls proposal imposes a large burden for little to no practical improvement in security. If a control weakness is a problem, it will come to light in vulnerability and penetration testing. For the aforementioned reasons, ICE recommends the Commission remove the controls testing requirements and definition of key controls.

5. *Production of Books and Records:*

The Commission should only require the Regulated Entities to produce books and records relevant to the Regulated Entity's examination. Overly burdensome production requirements will limit the Regulated Entities from having open and honest conversations around risk and not all information is of interest to the Commission. For example, risk is often discussed at a firm wide level and not by a specific Regulated Entity. Discussion around risks for non-CFTC regulated companies is not of use to the Commission and jeopardizes the confidentiality of those non-CFTC regulated companies. Further, requesting information from non-CFTC regulated companies would likely cause conflicts with other regulators and could violate foreign laws or regulations. As such, the Commission should limit the books and records requirements to be relevant and directly tied to examinations of the Regulated Entities.

Conclusion

ICE appreciates the opportunity to comment on the Proposal. ICE supports the Commission's efforts to enhance and clarify provisions relating to system safeguards and cyber security. As drafted, the Proposal codifies many efforts already in place today. We suggest that the Commission allow flexibility in implementation of the new or codified requirements and give deference to the Regulated Entity's current practices. Again, ICE thanks the Commission for the opportunity to comment on the Proposed Rules.

Sincerely,

Kara Dutta
Intercontinental Exchange, Inc.