Hope M. Jarkowski
General Counsel
New York Stock Exchange
11 Wall Street
New York, NY 10005
T: 202.661.8946
Hope.Jarkowski@nyse.com

NYSE
AN ICE EXCHANGE

June 13, 2023

Via Email

Ms. Vanessa Countryman
Secretary
U.S. Securities and Exchange Commission
100 F Street NE
Washington, D.C. 20549

Re: File Number S7–07–23; Release No. 34–97143; Regulation Systems Compliance and Integrity

Dear Ms. Countryman:

Intercontinental Exchange, Inc. and its affiliates (collectively, "ICE") appreciate the opportunity to comment on the U.S. Securities and Exchange Commission's (the "Commission") proposed amendments to Regulation Systems Compliance and Integrity ("Regulation SCI").[1] ICE is a leading provider of market infrastructure, data services, and technology solutions to a broad range of customers including financial institutions, corporations, and government entities. ICE operates 13 regulated exchanges, six clearing houses, and four SEC-registered broker-dealers. Numerous ICE entities are impacted by the proposed amendments, as many ICE entities are currently subject to Regulation SCI and additional ICE entities would be newly subject to Regulation SCI if the proposed amendments are adopted.

ICE well understands the challenges of ensuring the capacity, integrity, resiliency, availability, and security of the technology infrastructure underlying the securities markets and supports the Commission's intent in seeking to update Regulation SCI to better reflect and respond to the current state of those markets. Particularly in an evolving marketplace with greater reliance on technology, ICE believes reducing market-wide risk and promoting greater confidence in the operations of the securities markets among investors and other market participants are vital to the maintenance of fair and orderly markets.

In this letter, ICE provides the Commission with comments on the proposed amendments, including certain alternative proposals that we believe would more efficiently accomplish the Commission's objectives in amending Regulation SCI. While ICE supports the revision of Regulation SCI to better meet the needs of today's securities markets, we believe there are ways to achieve those goals that are less costly, more consistent with industry practice, and yield fewer unintended consequences, as discussed below.

[1] 88 FR 23146 (April 14, 2023) ("Regulation SCI Amendments").

Third-Party Provider Management

ICE agrees with the Commission that SCI entities should actively manage relationships with third-party providers that operate those SCI entities' SCI systems, or for the purposes of security, indirect SCI systems. That is consistent with the definition of "SCI systems" under Rule 1000, which is limited to those systems "of, *or operated* by or *on behalf of*, an SCI entity *that*, with respect to securities, *directly* support [the six SCI functions of] trading, clearance and settlement, order routing, market data, market regulation, or market surveillance" (emphasis added). The definition of "indirect SCI systems" in Rule 1000 is similarly limited to those systems "of*, or operated* by or *on behalf of*, an SCI entity that, if breached would be reasonably likely to pose a security threat to SCI systems" (emphasis added). Proposed Rule 1002(a)(2)(ix), however, refers broadly to "third-party providers that provide functionality, support or service, directly or indirectly" to an SCI entity's SCI systems or, for purposes of security standards, indirect SCI systems. While ICE is supportive of the intent of proposed Rule 1002(a)(2)(ix), we recommend that the Commission refine the text of the proposed language to instead require a "program to manage and oversee third-party providers that operate SCI systems or indirect SCI systems on behalf of an SCI entity."

ICE believes that this alternative proposed language would more precisely define the third-party providers to which Rule 1002(a)(2)(ix) would apply and better reflect the Commission's explanation of third-party SCI systems in connection with its adoption of Regulation SCI[2] and support the intent of the Regulation SCI Amendments. ICE believes that those purposes would be best served by limiting this provision to systems operated by third parties that *directly* support one of the six SCI functions. The Commission's proposed language could be read to extend to any third-party provider with even a tangential role in relation to an SCI entity's SCI systems or indirect SCI systems. Aside from the burden and cost to an SCI entity to assess such a broad swath of third-party providers for purposes of Regulation SCI compliance, this proposal would hinder SCI entities' ability to rely on third-party providers for important services or efficiencies -- fewer third-party providers may be willing to contract with SCI entities because of the additional burdens that would accompany those relationships, such as the added cost for such third-party providers to facilitate SCI entities' compliance with Regulation SCI. The effect of the Commission's proposed rule may be that SCI entities will handle in-house services they would have otherwise outsourced to a third-party provider, at the expense of the expertise a third-party provider would have offered. ICE believes that, with its suggested language, proposed Rule 1002(a)(2)(ix) would avoid this outcome and would set forth reasonable requirements for SCI entities to implement policies and procedures that include, among other things, a program to manage and oversee third-party providers, periodic review of third-party provider contracts, and a risk-based assessment of third-party providers.

Because an SCI entity may rely on third-party providers for a variety of purposes that do not "directly support" any of the six SCI functions, because those third-party providers do not operate any SCI systems, ICE believes that its proposed revision to Rule 1002(a(2)(ix) would appropriately bound the applicability of the rule to those vendors that in fact do operate SCI

---

[2] The Commission previously articulated that "a system [that is] operated on behalf of an SCI entity directly supports one of the six key functions listed within the definition of SCI system…should be included as an SCI system subject to the requirements of Regulation SCI…regardless of whether it is operated by the SCI entity directly or by a third party." 79 FR 72252 (December 5, 2014) at 72276 (emphasis omitted).

systems, or, for the purposes of security standards, indirect SCI systems. While SCI entities should likewise carefully manage their relationships with those third-party providers that do not operate an SCI system (or indirect SCI system) on their behalf, the management of those relationships would more properly fall under a separate vendor management program that assesses those third parties in the context of the specific functionality, support, or service they provide to the SCI entity (which are not subject to Regulation SCI). ICE's proposed alternative rule text thus seeks to add specificity to Rule 1002(a)(2)(ix) and ensure that its scope remains focused on the objectives of Regulation SCI and is consistent with the definitions of SCI systems and indirect SCI systems.

Systems Intrusion Event Framework

We agree, in principle, with the intent of the proposed amendments to the systems intrusion events framework to ensure that SCI entities continue to adequately safeguard the security of SCI systems and are prepared to respond to cybersecurity issues swiftly and effectively. However, ICE cannot support the proposed restructuring of the systems intrusion events framework to, among other things, expand the definition of a systems intrusion event.

ICE believes the existing framework under Regulation SCI has been successful in supporting regulatory objectives and reinforces the commercial interests of SCI entities to prevent systems intrusions. Further, the current reporting framework under Regulation SCI has fostered a level of reporting to the Commission of systems intrusion events that permits SCI entities, the Commission and its staff, and market participants to effectively respond to cybersecurity threats. We are concerned that the expanded scope and frequency of reporting of systems intrusion events would, rather than improve the protection of the securities markets, lead to undesirable outcomes. The proposed amendments to Rules 1000, 1002(b), and 1002(c)(4)(iii) would impose burdensome and time-consuming requirements on SCI entities and result in information overload for both the Commission and market participants, without providing any benefits.

From the perspective of an SCI entity, the new reporting requirements would divert resources and attention from what should be its primary focus when a potential or actual cybersecurity event occurs -- to identify and forestall the potential attack or vulnerability and ensure the security of its systems as quickly as possible. An expansion of the definition of, and the resultant substantial increase in the reporting of, systems intrusion events, which would include public dissemination of information relating to the event in certain cases, could cause confusion and panic among market participants (including investors), even when such events pose no security threat to the securities markets. Even worse, a proliferation of reporting of systems intrusion events -- most of which would not impact the securities markets -- would lead market participants to disregard notices of systems intrusion events altogether, which would run counter to the intent of the proposed amendments to improve the ability of SCI entities, the Commission, and market participants to respond to cybersecurity threats. In addition, the public dissemination of information relating to systems intrusion events poses further risk to SCI entities and the securities markets by disclosing details of cybersecurity events that could be leveraged by bad actors to cause additional harm, including by potentially alerting them to the extent to which a targeted entity is aware of a past or ongoing attack. ICE notes that SCI entities are not only subject to Commission oversight pursuant to Regulation SCI, and may also be active members of groups established by other governmental agencies focused on cybersecurity issues. ICE believes that the Commission's proposed expansion of SCI entities' obligations to publicly report systems intrusion events (the definition of which would also be expanded) is inconsistent with the principles applied by other agencies similarly charged with

evaluating and managing cybersecurity risk in the securities markets, and the Commission's proposed disclosure framework would detract from core strategies for cyber risk management employed by many SCI entities. ICE does not believe that the proposed changes to the systems intrusion framework are practical or supportable and strongly urges the Commission to retain the existing reporting regime for systems intrusion events.

While ICE does not believe that any changes to the systems intrusion event framework are necessary, we believe that the proposed third prong of the proposed defintiion is particularly problematic in that it now ambiguously defines a new kind of systems intrusion as "any significant attempted unauthorized entry into the SCI systems or indirect SCI systems of an SCI entity." ICE opposes this substantial and unsupported expansion of the definition. The modifier "significant" would not limit the types of attempted (i.e., unsuccessful) unauthorized entries into SCI systems that would be reported because the Commission's guidance on "significant" includes almost all attempted intrusions. ICE believes this proposed expanded definition of systems intrusion event would not improve market-wide responses to cybersecurity events because it would require reporting of events that are not impactful. Yet the costs associated with the proposed expanded definition of systems intrusion event, including the burdensome reporting obligations for unsuccessful entries into an SCI system, would far outweigh any benefit to SCI entities, the Commission, or market participants derived from reporting incidents that do not represent actual, actionable cybersecurity risks.

The Commission notes that this third prong is intended to include "unsuccessful, but significant, attempts" to access an SCI entity's SCI systems or indirect SCI systems. However, the proposed rule would not define what constitutes a "significant attempted unauthorized entry" and would instead require each SCI entity to establish reasonable written criteria to determine whether such an event has occurred.[3] The Commission identified the following as "characteristics of attempted unauthorized entries" that would generally be considered "significant":

> when an SCI entity becomes aware of reconnaissance that may be leveraged by a threat actor; a targeted campaign that is customized to the SCI entity's system; an attempted cybersecurity event that required the SCI entity's personnel to triage, even if it was ultimately determined to have no impact; an attempted attack from a known sophisticated advanced threat actor; the depth of the breach in terms of

[3] ICE also does not believe, as a threshold matter, that unsuccessful attempts to access an SCI entity's SCI systems or indirect SCI systems are properly considered systems intrusion events and notes that this interpretation is consistent with the definition offered by the Cybersecurity and Infrastructure Security Agency ("CISA"), a U.S. governmental agency that provides industry guidance on cybersecurity and infrastructure security and resilience. CISA defines a cyber intrusion as an event that "compromise[s] a computer system by breaking the security of such system or causing it to enter into an insecure state." See https://niccs.cisa.gov/education-training/catalog/accountinged/cyber-intrusions. Under Regulation SCI as it currently stands, SCI entities must have comprehensive cybersecurity programs that would include, among other things, controls designed to thwart attempts to access SCI systems and indirect SCI systems; an unsuccessful attempt to gain access to such systems would generally indicate that those controls are functioning effectively, making the majority of unsuccessful attempts largely meaningless.

> proximity to SCI systems and critical SCI systems; and a cybersecurity event that, if successful, had meaningful potential to result in widespread damage and/or loss of confidential data or information.[4]

The Commission also noted in proposing the third prong of the systems intrusion event definition that it would be "inefficient, inappropriate, and undesirable (for both SCI entities as well as the Commission and its staff) to require that all attempted entries be considered systems intrusions."[5] However, given the breadth and lack of specificity in the sample characteristics of the attempted unauthorized entries identified by the Commission as generally indicating that such attempt is "significant" and reportable under the requirements of Regulation SCI, these examples would suggest that the Commission views the great majority of attempted, yet unsuccessful, unauthorized entries to be reportable events under Regulation SCI. ICE does not believe that the reporting of every such event meeting the characteristics identified in the Regulation SCI Amendments would serve the objectives of Regulation SCI or further the Commission's goal of enhancing cybersecurity risk management and response. Indeed, ICE believes the Commission's enumerated criteria would require SCI entities to report many more systems intrusion events than currently -- far more than the additional three SCI events the Commission has grossly under-estimated would result from these proposed amendments.[6] ICE also notes that an SCI entity cannot prevent threat actors from *attempting* to gain unauthorized entry, regardless of the quality of its policies and procedures, further weakening the case that there is any benefit to reporting such events to the Commission.

ICE is particularly concerned about certain of the characteristics identified by the Commission in the Regulation SCI Amendments as indicative of a "significant" attempted unauthorized entry and strongly urges the Commission to reconsider whether such characteristics truly describe events that need to be reported pursuant to Regulation SCI, if the Commission proceeds to adopt the third prong definition in a final rule. First, the Commission's suggestion that "an attempted cybersecurity event that required the SCI entity's personnel to triage, even if it was ultimately determined to have no impact" would represent a "significant unauthorized entry" would render nearly all attempted cybersecurity events immediately reportable systems intrusion events, given that most if not all, cybersecurity events require some degree of triaging. ICE understands "triaging" to generally refer to a preliminary assessment to assist in understanding the nature of the issue, determining the severity of the issue, and formulating a course of action to address the issue. If any issue that requires triaging would trigger reporting obligations under Regulation SCI, SCI entities would be constantly reporting events. The result of this requirement would be reports to the Commission of daily triaging activities of information

---

4 Regulation SCI Amendments, 88 FR at 23185.

5 Id.

6 See Regulation SCI Amendments, 88 FR at 23210-11. For example, ICE estimates that it "triages" tens of thousands of cyber-related events each year, the vast majority of which do not require any action other than triage itself (but nonetheless were detected and blocked by ICE's comprehensive cybersecurity program) and would not otherwise be considered "significant" if not for the Commission's suggestion that "an attempted cybersecurity event that required the SCI entity's personnel to triage, even if it was ultimately determined to have no impact" is likely to be significant. See id. at 23185.

security staff at SCI entities, regardless of the quality of the SCI entities' policies and procedures in preventing successful intrusions.

Second, ICE believes that several other examples offered by the Commission to describe characteristics of significant unauthorized entries lack the clarity and specificity necessary to enable SCI entities to establish their own criteria to determine whether such entries constitute systems intrusion events, or otherwise assume facts and circumstances that would not be knowable to an SCI entity without first conducting an investigation into the nature and scope of an incident. For example, the Commission states that instances in which an SCI entity becomes aware of "reconnaissance that may be leveraged by a threat actor" or "a targeted campaign that is customized to the SCI entity's system" would be indicative of a significant attempted unauthorized entry. However, without taking into account any thresholds for materiality, certainty, or legitimacy, these scenarios could encompass incidents ranging from trivial to those that actually pose a significant threat to the security of an SCI entity and do not provide meaningful guidance to SCI entities in assessing the significance of attempted unauthorized entries. The Commission's suggestion that any "cybersecurity event that, if successful, had meaningful potential to result in widespread damage and/or loss of confidential data or information" is likely to be a significant unauthorized entry is likewise too vague to offer effective guidance to inform SCI entities' policies. In fact, because, if successful, many cybersecurity events could lead to such a result, this guidance only expands the types of unsuccessful intrusions that would be reportable. Moreover, SCI entities could not reasonably ascertain whether a campaign has been targeted to its systems, if "an attempted attack [originates] from a known sophisticated threat actor," or the "depth of [a] breach in terms of proximity to SCI systems and critical SCI systems"[7] without triaging (or otherwise investigating) such incidents. Taken together, these criteria effectively suggest that SCI entities could not complete any meaningful investigation into a potential cyber-related event without triggering an obligation to report such event to the Commission; in other words, the Commission appears to be suggesting that any potential cyber-related event would require immediate reporting regardless of its significance, which would seem to nullify the purpose of the proposed third prong of the systems intrusion event definition. ICE does not believe this outcome is consistent with the Commission's stated goal of strengthening the reporting process for systems intrusion events.

In short, the third definitional prong sweeping in "significant attempted unauthorized entr[ies]" -- even those "determined by the SCI entity pursuant to established reasonable written criteria" -- would seem to set up an unworkable standard, where any rational SCI entity would be required to be tying up resources reporting matters to the Commission that, by definition, had no impact whatsoever on the SCI entity's operations or on market participants. Indeed, it is easy to imagine a regime where the Commission's staff could seek to second guess an SCI entity's triage of whether an "attempted unauthorized entry" was "significant" or "insignificant" and/or whether the "written criteria" guiding such triage were "established" and/or "reasonable." If the Commission is concerned that cyber-events are not being timely reported by SCI entities, the Commission's proposed erasure of the eligibility of de minimis SCI intrusions for quarterly reporting (under the proposed amendments to Rule 1002(b)(5)) will be more than sufficient to

[7] ICE also notes that the Commission's use of the term "proximity" in this example needs further clarification in order for SCI entities to understand the types of events that the Commission intends to capture.

achieve the Commission's objectives, without creating an entire new amorphous standard of reportable "attempted" intrusions to create a deluge of new reports.

SCI Review

The Commission has proposed a number of changes to the annual SCI review that SCI entities are required to conduct of their compliance with Regulation SCI. While ICE is supportive of a rigorous and comprehensive SCI review process and the value it provides to both SCI entities and the Commission, ICE strongly urges the Commission to reconsider certain of the proposed amendments relating to the definition of SCI review set forth in Rule 1000.

First, ICE believes the proposed requirement that the SCI review include three specific assessments to be performed by objective personnel would be inconsistent with accepted audit practices, including the Institute of Internal Auditors' widely employed "Three Lines Model."[8] Limiting SCI entities' ability to draw on risk assessments already performed in the ordinary course by qualified personnel of the SCI entity would effectively collapse risk assessment from the second line into the third line and unnecessarily restrict SCI entities' ability to leverage such work to support the SCI review process.

ICE also strongly urges the Commission not to expand the SCI review to encompass testing of every SCI system and indirect SCI system every year, as dictating that the SCI review be conducted in this manner would directly contradict the risk-based approach that underpins sound audit practices. Established auditing principles instead support rotating control testing over a period of years based on a risk assessment, including a sampling of the test population (in this case, SCI systems and indirect SCI systems), to reach a reasonable level of assurance that the controls are functioning as expected. ICE believes this approach is particularly appropriate with respect to process verification, as a sampling of a test population in such cases would be sufficient to gain reasonable assurance that the underlying process is functioning as intended (and testing the entire test population would not provide any further assurances). ICE further believes such an approach would be consistent with industry best practices to ensure the audit gives due focus to areas requiring attention from a risk perspective.[9] ICE is also concerned that prescribing that the SCI review test all systems and controls every year would detract from the efficacy of the review -- for example, time and resources would be expended to assess low-risk areas when they could be better allocated to high-risk areas.

Furthermore, despite the Commission's recognition of the importance of "provid[ing] flexibility to those conducting the SCI review to choose the methodology they believe to be most appropriate

---

8 See https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf.

9 See, e.g., Federal Financial Institutions Examination Council IT Examination Handbook, Audit Booklet, Risk Assessment and Risk-Based Auditing, available at https://ithandbook.ffiec.gov/it-booklets/audit/risk-assessment-and-risk-based-auditing/ ("An effective risk-based auditing program will cover all of an institution's major activities. The frequency and depth of each area's audit will vary according to the risk assessment of that area.")

given the particular characteristics and risks of the SCI entity's systems being assessed,"[10] the proposed framework for the SCI review going forward would not afford SCI entities any flexibility to adapt to the evolving landscape and properly target and assess emerging risks. Given the number of SCI systems and indirect SCI systems that an SCI entity may have, together with the accompanying controls for each such system, this proposed requirement could drastically expand the scope of the SCI review for many SCI entities. The SCI review would likely become an unwieldy and time-consuming undertaking for SCI entities, without conferring meaningful benefits to SCI entities, the Commission and its staff, or market participants. ICE also notes that this proposed reinterpretation of the SCI review appears to be inconsistent with the requirement that SCI entities frame their SCI review around risk assessments conducted by objective personnel; if SCI entities are required to test each and every SCI system and indirect SCI system every year, it is unclear what purpose any risk assessments conducted in support of the SCI review would serve. The definition of "SCI review" in Rule 1000 acknowledges the importance of adhering to industry standards for audit practices,[11] and ICE strongly urges the Commission not to modify the rule in a way that would impede SCI entities' ability to conduct audits pursuant to accepted best practices.

Finally, ICE recommends that the Commission reconsider the addition of the proposed requirement in Rule 1003(b)(1) that SCI entities that are only classified as such for a portion of a given calendar year must still conduct and submit an SCI review for that year. ICE believes that compliance with this requirement would be particularly challenging taken together with the Commission's proposal to expand the scope of the SCI review, and it would be difficult for an SCI entity that is only subject to Regulation SCI for a portion of a calendar year to accomplish the SCI review, as proposed, on a compressed timeframe. We also believe the requirement does not make sense with respect to entities that cease to be SCI entities during a calendar year, as an SCI review of such an entity would impose an unnecessary burden on the entity without providing meaningful benefit to either the entity or to the Commission.

Penetration Testing

ICE supports penetration testing requirements for SCI entities and believes such testing is important to assist SCI entities in assessing the effectiveness of their security policies and controls. Accordingly, ICE does not object to the proposed requirement that SCI entities conduct penetration testing on an annual basis, rather than every three years.[12] However, ICE

---

10 Regulation SCI Amendments, 88 FR at 23188.

11 Rule 1000 currently provides that the SCI review should include an assessment of an SCI entity's "[i]nternal control design and operating effectiveness, to include logical and physical security controls, developmental process, systems capacity and availability, information technology service continuity, and information technology governance, *consistent with industry standards*" (emphasis added).

12 ICE also requests that the Commission clarify in connection with these proposed changes that SCI entities may submit the results of penetration testing, at least for a certain period following the implementation of any final rule incorporating this requirement, separate from the report of the SCI review that is already conducted annually. SCI entities may rely on different teams and processes to conduct the annual SCI review on one hand and penetration testing on the other, and these workflows may not be aligned in a way that would permit the results of the SCI review and penetration

does not agree with the proposed requirement that penetration testing include all "vulnerabilities identified pursuant to [an SCI entity's] regular review and testing requirement in designing its penetration testing" and believes such a requirement would negatively impact the effectiveness of penetration testing. The penetration tests that ICE entities (and likely other SCI entities) currently perform instead focus on vulnerabilities identified through a risk-based prioritization, thereby tailoring penetration testing to those that present a realistic residual risk; those vulnerabilities are the ones that are assessed through penetration testing. ICE believes that this type of penetration testing is more effective than testing all vulnerabilities an SCI entity may be aware of, because it focuses on the most significant risks to an entity rather than testing vectors where the entity has already implemented effective controls that reduce the risk posed by previously identified vulnerabilities.

Current SCI Industry Standards

As the Commission has acknowledged, many SCI entities rely on prevailing industry standards to guide the formulation of their policies and procedures as required by Regulation SCI Rule 1001(a). ICE does not object to the intent of proposed Rule 1001(a)(2)(xi), which would require that SCI entities choosing to avail themselves of the "safe harbor" provision set forth in Rule 1001(a)(4) identify in their policies and procedures any industry standards with which they are aligned, and recognizes that including such information in an SCI entity's policies and procedures could improve their clarity.

However, ICE recommends that any final version of proposed Rule 1010(a)(2)(xi) further provide that SCI entities may comply with this proposed requirement by identifying relevant industry standard(s) only in the top-level policy for a given area, rather than in the policy and also in each subordinate procedure related to such area, provided that the policy and any related procedures are clearly identified as such. We believe that such a requirement would accomplish the Commission's goals in ensuring that an SCI entity's policies and procedures clearly cite to any relevant SCI industry standards when the entity seeks to rely on Rule 1001(a)(4), without imposing an additional burden on SCI entities to include redundant information when the policies and procedures are explicitly identified as related, such that it would be clear that any relevant industry standard(s) are applicable both to a given policy and the procedures that fall under it.

Coordination with Other Regulatory Agencies

Finally, ICE notes that many SEC-registered Clearing Agencies, including ICE Clear Credit and ICE Clear Europe, are also registered as Derivative Clearing Organizations ("DCO") with the Commodity Futures Trading Commission ("CFTC"). In addition, several security-based swap data repositories, including ICE Trade Vault, are also registered with the CFTC. ICE notes that

testing to be reported in tandem. If the Commission believes that the results of both efforts should be submitted to the Commission in the same report, ICE believes that a transition period following adoption of any final rule relating to the reporting of penetration testing results would allow SCI entities the opportunity to coordinate these separate processes to enable such reporting.

there is overlap between the existing CFTC system safeguard regulations,[13] as well as the CFTC's pending proposed rulemaking relating to Reporting and Information Requirements for DCOs,[14] and the proposed amendments, and urges coordination between the Commission and the CFTC to ensure that any final rules are structured so that dual-registered entities can efficiently comply with both agencies' rules.

Conclusion

ICE is supportive of the Commission's intent in updating Regulation SCI to adapt to the evolving securities markets and ensure the continued capacity, integrity, resiliency, availability, and security of the technology infrastructure supporting those markets. The comments provided herein offer suggestions for alternative approaches that ICE believes would more effectively incorporate cost-benefit considerations and industry practice and avoid unintended downstream effects, while still accomplishing the Commission's objectives in strengthening Regulation SCI.

Respectfully submitted,

Hope M. Jarkowski
General Counsel
NYSE Group, Inc.

cc: Honorable Gary Gensler, Chair
Honorable Hester M. Peirce, Commissioner
Honorable Caroline A. Crenshaw, Commissioner
Honorable Mark T. Uyeda, Commissioner
Honorable Jaime Lizárraga, Commissioner
Haoxiang Zhu, Director of the Division of Trading and Markets

---

13 System Safeguard Testing Requirements (RIN 3038–AE30), 81 FR 64271 at 64272 (September 19, 2016). See also System Safeguard Testing Requirements (RIN 3038-AE29), 81 FR 64321 at 64321-64340 (September 19, 2016).

14 Reporting and Information Requirements for Derivatives Clearing Organizations (RIN 3038-AF12), 87 FR 76698 (December 15, 2022).