July 30, 2013

Via Electronic Mail (rule-comments@sec.gov)

Elizabeth M. Murphy
Secretary
Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-1090

Re: File No. S7-01-13; Regulation Systems Compliance and Integrity

Dear Ms. Murphy:

The undersigned seventeen registered national securities exchanges (the "Exchanges")[1] and the Financial Industry Regulatory Authority, Inc. ("FINRA," and together with the Exchanges, the "SROs") write to provide our comments to the Securities and Exchange Commission (the "Commission") on the Commission's proposed Regulation Systems Compliance and Integrity under the Securities Exchange Act of 1934 (the "Exchange Act"), commonly known as "Regulation SCI."[2]

The comments herein reflect the product of an open dialogue between and among senior regulatory and legal staff at each of the SROs. As such, the SROs offer these recommendations for your consideration and look forward to a continued dialogue with the Commission on this important proposed regulation. Nothing in the comments below should be construed as contradictory to any of the individual SRO comment letters. Rather, these comments reflect an effort to offer a constructive view of proposed Regulation SCI.

EXECUTIVE SUMMARY

The SROs support the main objectives of Regulation SCI, which are to reduce market-wide risk and promote greater confidence in the operations of the equity and options markets among investors and other market participants. SCI entities should have adequate levels of capacity, integrity, resiliency, availability and security to maintain their operational capability. In an evolving marketplace with greater reliance on technology, these are vital objectives to

---

[1] Specifically, BATS Exchange, Inc.; BATS Y-Exchange, Inc.; BOX Options Exchange, LLC; Chicago Board Options Exchange, Inc.; C2 Options Exchange, Inc.; Chicago Stock Exchange, Inc.; EDGA Exchange, Inc.; EDGX Exchange, Inc.; International Securities Exchange, LLC; Miami International Securities Exchange LLC; The NASDAQ Stock Market LLC; NASDAQ OMX BX, Inc.; NASDAQ OMX PHLX LLC; National Stock Exchange, Inc.; New York Stock Exchange, LLC; NYSE MKT, LLC; and NYSE Arca, Inc.

[2] See Securities Exchange Act Release No. 69077 (March 8, 2013), 78 FR 18083 (March 25, 2013) ("Proposal" or "Proposing Release").

promote the maintenance of fair and orderly markets. The SROs specifically agree with these objectives and encourage the need for policies and procedures in this regard.

Nevertheless, the SROs collectively share concerns over many of the definitions proposed in Regulation SCI and the subsequent effect on reporting and other obligations. We question whether Regulation SCI, as currently proposed, represents the most effective method to achieving the objectives of the proposed rules. In summary, we have the following observations and recommendations:

1) In lieu of the publications and standards identified in Table A, the Commission should characterize the appropriate policies and procedures as reasonably designed if they comply with "generally accepted standards."[3]

2) The definition of the term "SCI systems" should be limited to those systems that operate in real-time to directly support the marketplace.

3) The definition of the term "SCI security systems" should be eliminated from the proposed rule and be replaced with a requirement for policies and procedures that both evaluate the risks of non-SCI systems on SCI systems and demonstrate appropriate steps to protect SCI systems from intrusions.

4) The definition of the term "systems disruption" should be limited to include only those events that have a material impact on the delivery of core services to members or participants, as opposed to routine issues.

5) The definition of the term "systems intrusion" should be limited to include only those intrusions that would in fact cause significant harm or loss to market participants.

6) The Commission should provide more guidance on the meaning of "material systems change" since, based on the examples in the Proposing Release, the definition appears to be overly broad and reporting of such may lead to unnecessary and costly delays for SCI entities.

7) The Commission should adopt a materiality threshold for purposes of triggering the requirement to report systems compliance issues to the Commission and to disseminate information to members or participants.

8) The SROs are concerned with the subjective and vague terminology used in describing the notification requirements of proposed Rule 1000(b)(4), specifically

---

[3] Id. at 18111.

that notification is required upon any responsible SCI personnel becoming "aware" of an SCI event.

9) The trigger for notifying the Commission of an SCI event should be determined based on the immediacy with which the SCI entity requires Commission participation. Such requirement should be tiered based on the criticality of the event.

10) The reference in proposed Rule 1000(b)(3) to "corrective action" should be modified to emphasize policies and procedures that are designed to mitigate risk.

11) The definition of the term "responsible SCI personnel" should be limited to designated senior management within the relevant departments of each entity. The "becomes aware" standard places inappropriate emphasis on reporting immediately, potentially to the detriment of diagnosis, resolution and escalation.

12) The SROs propose an alternative safe harbor, which would provide a more objective and transparent mechanism for SCI entities and their employees.

13) The SROs are concerned that live production testing could compromise the marketplace. The SROs would not support including such a requirement in Regulation SCI.

14) Regarding mandatory testing, the SROs believe that further guidance and discussion is needed to determine means for markets to recover from a wide-scale disruption.

15) Rapid recovery following a widescale disruption may not necessarily be the primary objective in all cases. Facts and circumstances may dictate that attempting to recover trading markets during and immediately following a wide-spread disruption may in fact compromise the public safety and the maintenance of a fair and orderly market, as was evidenced in the aftermath of Superstorm Sandy.

16) The Commission needs to clarify what is meant by "access to systems," as such access may be inconsistent with prudent security measures.

17) The cost-burden analysis in the Proposing Release is significantly underestimated and requires further discussion and analysis.

I. SRO CONCERNS ON DEFINITIONS IN RULE 1000(A) AND IMPACT ON RULE 1000(B) OBLIGATIONS

A. REASONABLE POLICIES AND PROCEDURES

Under proposed Rule 1000(b)(1), an SCI entity would be required to establish, maintain and enforce written policies and procedures reasonably designed to ensure that its SCI systems, and for purposes of security standards, its SCI security systems, have levels of capacity, integrity, resiliency, availability and security adequate to maintain the SCI entity's operational capability and promote the maintenance of fair and orderly markets. The Commission is not proposing to prescribe the specific policies and procedures that an SCI entity must follow to comply with the requirements of proposed Rule 1000(b)(1), but has provided guidance that an SCI entity's policies and procedures would be deemed to be reasonably designed if they are consistent with "SCI industry standards."[4] The Commission has also provided a list of publications with examples of SCI industry standards, including National Institute of Standards and Technology ("NIST") and Federal Financial Institutions Examination Council ("FFIEC") standards, and Commission policy statements covering nine inspection areas or domains.[5]

While the SROs support the Commission's providing SCI entities the flexibility to identify appropriate policies and procedures based on their size, technology, business model and other relevant factors, the SROs are concerned that relying on the publications set forth in Table A of the Proposing Release may lead to unintended consequences. For example, such standards might not keep pace with a constantly evolving technological landscape. Despite this evolution, Commission staff might take a checklist approach to its review of policies and procedures, which may lead to further confusion. The SROs suggest that, in lieu of the publications identified in Table A, the Commission characterize the appropriate policies and procedures as reasonably designed if they comply with "generally accepted standards." The generally accepted standards for policies and procedures in today's fast-paced technological environment will be expected to evolve over time by system and by entity. An SCI entity's policies and procedures that are consistent with generally accepted standards would be deemed to be in compliance with Regulation SCI.

B. SCI SYSTEM

Under proposed Regulation SCI, an "SCI system" would mean all computer, network, electronic, technical, automated or similar systems of, or operated by or on behalf of, an SCI entity, whether in production, development or testing, that directly supports trading, clearance and settlement, order routing, market data, regulation or surveillance.[6]

---

4 See Proposing Release, supra note 2, at 18109.

5 See id. at 18111 (Table A).

6 See Proposed Rule 1000(a).

The SROs believe that the Commission's proposed definition of "SCI system" is vague, overbroad and generally fails to appropriately differentiate between real-time market operation, regulation and data dissemination services and those ancillary systems that do not operate in real-time. Systems that do not directly support "trading, clearance and settlement, order routing, market data, regulation or surveillance" *in real-time* do not warrant the level of oversight and added costs that the regulation imposes.

Further, the SROs oppose the designation of any development or testing systems as SCI systems. These systems are intended, for example, to create new products and test their reliability and vulnerability using novel or unexpected trading activity and events. They are uniquely unsuitable for inclusion in the proposed regulation.

C. SCI SECURITY SYSTEM

Under proposed Regulation SCI, an "SCI security system" would be defined as any system that shares network resources with SCI systems and that, if breached, would be reasonably likely to pose a security threat to SCI systems.[7]

The SROs strongly support the Commission's adoption of the alternative set forth in the Proposing Release that would eliminate references to SCI security systems from the regulation and instead require that SCI entities have reasonable policies and procedures that evaluate the risks posed to SCI systems by non-SCI systems that share common network resources, and that the SCI entities take appropriate steps to protect their SCI systems from such risks.[8] This approach would enable SCI entities, as well as Commission staff, to more appropriately focus their attention and resources on those systems that have the most potential to impact investors. These efficiency benefits would be quickly eliminated, however, should the Commission seek to otherwise impose residual reporting or disclosure requirements on those non-SCI systems as suggested in other questions posed by the Commission in the Proposing Release. Alternatively, should the Commission retain the concept of an SCI security system, the SROs believe that, at a minimum, the Commission should narrow its definition so that systems that are not only physically, but logically, separated from SCI systems would not be covered by the regulation if such separations were appropriately monitored.

D. SYSTEMS DISRUPTION

Under proposed Regulation SCI, reportable SCI events would include systems disruptions. Systems disruptions are defined to include: (1) a failure to maintain service level agreements or constraints; (2) a disruption of normal operations, including a switchover to back-up equipment with near-term recovery of primary hardware unlikely; (3) a loss of use of any SCI

---

7 See Proposed Rule 1000(a).

8 See Proposing Release, supra note 2, at 18100.

system; (4) a loss of transaction or clearance and settlement data; (5) significant back-ups or delays in processing; (6) a significant diminution of an SCI entity's ability to disseminate timely and accurate market data; or (7) a queuing of data between system components or a queuing of messages to or from members or customers of such duration that normal service delivery is affected.[9]

The SROs believe the proposed definition of systems disruption is impracticably broad. In particular, it would presumably include minor and routine systems issues that do not materially affect an SCI entity's performance of its core functions. For example, the Commission included in the definition of systems disruption a queuing of data between system components or queuing of messages to or from customers of such duration that normal service delivery is affected. According to the Proposing Release, the Commission is of the view that the "queuing of data between system components is often a warning signal of significant disruption of normal systems operations."[10] In fact, however, the queuing – or "buffering" – of data between system components is a normal and necessary occurrence as information moves between system components. Any time messages are sent from system component to system component, messages must be queued in several places. It would not be reasonable to expect that an SCI entity should or could report to the Commission every instance in which such queuing occurs, nor is it clear what the Commission would do with such information. The SROs believe the Commission should limit the definition of systems disruptions such that it only includes systems events that materially affect the delivery of core services to members, customers or other market participants.

E. SYSTEMS INTRUSION

Under proposed Regulation SCI, a "systems intrusion" would mean "any unauthorized entry into the SCI systems or SCI security systems of an SCI entity."[11] The Commission states in the Proposing Release that the "definition of systems intrusion would cover the introduction of malware or other attempts to disrupt SCI systems or SCI security systems of SCI entities provided that such systems were actually breached."[12] Any time responsible SCI personnel become aware of a systems intrusion, the SCI entity would be required to notify the Commission immediately, and to notify its members or customers promptly.[13] The Commission makes clear in the Proposing Release that this reporting requirement would apply to both intentional and

---

9 See Proposed Rule 1000(a).

10 See Proposing Release, supra note 2, at 18102.

11 See Proposed Rule 1000(a).

12 See Proposing Release, supra note 2, at 18103.

13 See Proposed Rule 1000(b)(4).

unintentional conduct leading to such unauthorized entry, as well as minor and non-impactful intrusions.[14]

The SROs are concerned that such a broad reporting requirement would unreasonably and unnecessarily burden not only SCI entities, but Commission staff as well, because SCI entities would have to rapidly investigate and report a multitude of minor incidents that regularly occur during the normal course of business. For example, if an employee who has desktop access to SCI systems or SCI security systems mistakenly opens a web link that contains malware, it would appear that the SCI entity could be required to immediately notify the Commission and promptly notify its members or customers, even if the action had no impact on SCI systems. The SROs believe the cost of complying with such a requirement far outweighs any incremental benefit that might result from collecting such information. Instead, the SROs suggest that the Commission modify the definition of "systems intrusion" to include only those that the SCI entity reasonably estimates would result in significant harm or loss to market participants.

F. MATERIAL SYSTEMS CHANGE

Under proposed Regulation SCI, a "material systems change" would mean a change to one or more: (1) SCI systems of an SCI entity that: (i) materially affects the existing capacity, integrity, resiliency, availability or security of such systems; (ii) relies upon materially new or different technology; (iii) provides a new material service or material function; or (iv) otherwise materially affects the operations of the SCI entity; or (2) SCI security systems of an SCI entity that materially affects the existing security of such systems.[15] This definition is substantively similar to the definition of "significant system change," as discussed in the "ARP II Release."[16]

The SROs believe that the Commission needs to provide more guidance as to what would be considered "material" in this context. As written, the definition provides a materiality standard, but the examples provided in the Proposing Release suggest otherwise. The examples imply that any and all systems changes could be considered "material." Further, the SROs are concerned that this requirement, in practice, would far exceed that which is currently reported by SROs under the ARP releases and SRO Systems Compliance Letter. In turn, this would have a serious impact on the reporting obligations under Rule 1000(b)(6). Therefore, the SROs suggest that a simpler standard for material systems changes would alleviate some of the confusion and limit unnecessary, time-consuming and costly notifications to the Commission.

---

[14] See Proposing Release, supra note 2, at 18103.

[15] See Proposed Rule 1000(a).

[16] See Automated Systems of Self-Regulatory Organizations, Securities Exchange Act Release No. 27445 (November 16, 1989), 54 FR 48703 (November 24, 1989) ("ARP I") and Automated Systems of Self-Regulatory Organizations, Securities Exchange Act Release No. 29185 (May 9, 1991), 56 FR 22490 (May 15, 1991) ("ARP II," and together with ARP I,"ARP").

For example, the Commission states in the Proposing Release that "reconfigurations of systems that would cause a variance greater than five percent in throughput or storage" would be considered material.[17] The SROs believe that systems changes amounting to a 5% change to capacity, especially an upward change, are part of the normal course of business operations --and occur with relative frequency. Not only is it unnecessary to report such a change, the 30-day advance reporting requirement would likely, and needlessly, delay a necessary capacity enhancement.

Moreover, the SROs are concerned with the duplicative effects of Rule 1000(b)(6) in light of the fact that SROs have obligations under Section 19(b) of the Exchange Act and Rule 19b-4 thereunder. Where a systems change requires a rule filing, a duplicative notice should not be required under Rule 1000(b)(6). If the change does not require a rule filing, periodic, post-hoc reporting should suffice as it does today under ARP regime. The Commission has given no concrete indication of what it plans to do with systems change notifications, and the SROs are concerned that the Commission will delay or seek to create an approval process comparable to the rule filing approval process, around systems changes. The SROs believe that SCI entities themselves are in the best position to monitor such changes.

II. REPORTING OBLIGATIONS

Under proposed Regulation SCI, the Commission would require notification of SCI events. Proposed Rule 1000(b)(4) provides that, "[u]pon any responsible SCI personnel becoming aware of a systems disruption that the SCI entity reasonable estimates would have a material impact on its operations or on market participants, any systems compliance issue, or any systems intrusion, notify the Commission of such SCI event." The Commission provides a series of requirements that require immediate notification to Commission staff, written notice within 24 hours, written updates as requested by the Commission and the use of a prescribed form, Form SCI.[18]

A. MATERIALITY THRESHOLD FOR IMMEDIATE AND PROMPT REPORTING OF SYSTEMS COMPLIANCE EVENTS

The SROs believe that, in addition to problems with the extensive and vague nature of what constitutes a systems compliance issue, the requirement under proposed Rule 1000(b)(4) for immediate reporting of *any* systems compliance issue to the Commission is too broad to be effective in accomplishing the objectives of Regulation SCI. Similarly, the SROs believe that the prompt dissemination of information regarding systems compliance issues to members or participants, as required under proposed Rule 1000(b)(5), may lead to widespread dissemination of extraneous and potentially inaccurate information that could have the unintended consequence

---

[17] See Proposing Release, supra note 2, at 18105.

[18] See Proposed Rule 1000(b)(4).

of alarming or even harming the markets rather than creating an informed market as intended by the proposed rule.

Instead, the SROs recommend that the Commission adopt a materiality threshold for purposes of triggering the requirement to report systems compliance issues to the Commission and to disseminate information to members or participants. This threshold should resemble or mirror that which would trigger immediate notification and dissemination in the context of systems disruptions. (Specifically, only systems disruptions that "the SCI entity reasonably estimates would have a material impact on its operations or on market participants" are subject to immediate notification under proposed Rule 1000(b)(4)(i), and only systems disruptions "that result in, or the SCI entity reasonably estimates would result, in significant harm or loss to market participants" are subject to dissemination under proposed Rule 1000(b)(5)(i).)

The SROs propose that the materiality threshold for systems compliance issues should be based on factors such as the number of members affected, financial impact and operational impact, and the guidelines for these considerations should be articulated in the SCI entity's written policies and procedures. The SROs recommend further discussion in detailing these thresholds either in the final rule or in subsequent Commission guidance. Thus, any systems compliance issue that meets the materiality threshold as articulated above would be reported to the Commission, and information on such issue would be disseminated to members and participants, as outlined under proposed Rule 1000(b)(4)(i) and proposed Rule 1000(b)(5)(i) and articulated in the SCI entity's written policies and procedures.

B. VAGUE TERMINOLOGY IN TIMING OF NOTIFICATION

The SROs are concerned with the subjective and vague terminology used in describing the notification requirements of proposed Rule 1000(b)(4), specifically that notification is required upon any responsible SCI personnel becoming "aware" of an SCI event. This language does not acknowledge that personnel may become "aware" of an SCI event without knowing what the event effectively entails. For example, responsible SCI personnel may be conscious of a bug in the system because of non-standard behavior exhibited by the system, but may not know the source or the cause of the bug. More importantly, the SROs believe that requiring responsible SCI personnel to focus on immediate reporting as soon as they become "aware" would distract them from what should be the first priorities – containment, diagnosis, resolution and escalation.

Accordingly, the requirement for an immediate notification to the Commission could create a greater incidence of false positives without the benefit of careful consideration and identification of the cause of the problem. The immediate notice requirement will result in a conservative approach where SCI entities notify the Commission every time there may potentially be an SCI event. For example, SCI entities may feel compelled to report whenever there is an exception on a compliance or information security report in order to comply with the "becomes aware" standard. Similarly, SCI entities may feel compelled to characterize and report a greater number of system anomalies as disruptions to comply with the proposed rule. The

SROs believe that, in comparison to a considered notification requirement, this conservative type of notification would be an inefficient deployment of both the SCI entity and Commission resources, with no material benefit derived. The Commission should be focused on ensuring that first and foremost, problems are resolved, and that only material issues are brought to their attention. Otherwise, over-reporting will result and the likelihood of truly material issues getting lost in all the paperwork would increase exponentially.

C. MISPLACED FOCUS ON IMMEDIATE REPORTING

The Commission stated in the Proposing Release that the reason for immediate notification is to enable the Commission and its staff to "quickly assess the nature and scope of an SCI event, and help the SCI entity identify the appropriate response to the SCI event."[19] While the SROs support the need for transparency to the Commission, the SROs believe that providing immediate information for SCI events, as currently proposed, will not effectively achieve the objectives of Regulation SCI and the Commission will burden both the SCI entity's and Commission's resources without any corresponding benefit.

The SROs believe that the Commission should only be immediately informed of issues when there is a compelling need for the Commission to have immediate awareness, but this should be at a much higher materiality threshold than, for example, events that may potentially fall into exceptions of daily compliance oversight of SCI entities. The SROs strongly believe that such considered notifications will be of greater value to the Commission, members and participants.

The SROs also believe that the focus in Regulation SCI on immediate reporting to the Commission, followed by further detailed reporting within 24 hours of any SCI event, represents the wrong order of priorities for SCI entities. Following an SCI event, the main priority for the SCI entity should be taking corrective action to avoid or mitigate potential harm to investors and market integrity resulting from the SCI event. As it is important for the personnel involved in the SCI event to be participating in the containment and resolution of the SCI event, their required involvement in the immediate reporting may not be practical. The focus and purpose of any notification to the Commission on an immediate basis should not be to catalogue all "material" events for the Commission. Rather, the trigger for notifying the Commission should be determined based on the immediacy with which the SCI entity requires Commission participation. The SROs suggest a tiered method that ensures that SCI entities have written policies and procedures that focus the SCI entity's attention primarily on taking corrective measures during an SCI event, maintaining records to provide information to the Commission and members and participants, as necessary and appropriate, and reserving immediate notification to the Commission for truly critical events where the Commission's perspective on the instant issue would likely contribute to a more expedient resolution.

---

[19] See Proposing Release, supra note 2, at 18119.

D. MITIGATION OF POTENTIAL HARM

The SROs consider proposed Rule 1000(b)(3) to be vague in requiring corrective action that includes "at a minimum, mitigating potential harm to investors and market integrity,"[20] and requests that the Commission provide further clarity. Further, focus of this proposed rule should be on SCI entities and their policies and procedures with reference to the requirements under proposed Rules 1000(b)(1) and 1000(b)(2).

To that end, the SROs propose the following changes to proposed Rule 1000(b)(3):

> (3) Corrective Action. [Upon any responsible SCI personnel becoming aware of an SCI event, begin to take appropriate corrective action]<u>If any responsible SCI personnel at an SCI entity has a reasonable basis to conclude that an SCI event has occurred, the SCI entity shall invoke its policies and procedures promulgated pursuant to Rules 1000(b)(1) and 1000(b)(2) to take corrective action</u> which shall include, at a minimum, [mitigating potential harm to investors and market integrity resulting from the SCI event and]<u>communicating the potential existence of an SCI event to responsible parties, diagnosing the scope of the potential SCI event and its root cause,</u> devoting adequate resources to remedy the SCI event as soon as reasonably practicable <u>and mitigating potential harm to investors and market integrity resulting from the SCI event by following said procedures and, where required under Rule 1000(b)(5), notifying members and the public.</u>

Also, the SROs believe that the requirement of prompt dissemination and disclosure to members and participants of dissemination SCI events places a disproportionate focus on disclosure as the appropriate mitigation of potential harm for all SCI events. The SROs believe that there should be a balanced approach to making such disclosure, as there may be more effective means to mitigate potential harm. For example, prompt disclosure of an SCI event to members or participants that is not fully understood may result in unsettling the markets rather than promoting market integrity.

E. UNDULY BROAD INCLUSION OF DISSEMINATED COMMUNICATION

The SROs support the requirement that information disseminated in order to comply with proposed Rule 1000(b) should be attached to Form SCI; however, the SROs question the need to include a copy of *any* information disseminated to members or participants regarding an event as required under proposed Rule 1000(b)(4)(iv)(C). Given the flood of member requests for information during an incident and the disparate manner by which information could be disseminated, this is an overly broad inclusion of communications. Indeed, the SROs believe that this requirement would likely have a chilling effect on communications between the SCI entities and their members and participants.

---

[20] <u>See id.</u> at 18117.

F. CONFIDENTIALITY OF REPORTING

The current proposal is silent as to whether the disclosures made pursuant to Regulation SCI, and Form SCI in particular, will be maintained as confidential and non-public and protected from FOIA disclosure requests. The proposed disclosure and reporting requirements in the proposal encompass a wide variety of information (including, for example, proprietary systems design information, network and exchange system security controls, and market surveillance programs) that are currently maintained on a confidential, non-public basis. If such information is provided to the Commission under the current ARP program, it is strictly on a confidential, non-public basis. The public disclosure of such information could potentially expose individual SROs and the entire market system to additional risks of more frequent SCI events. The SROs support a requirement that any information provided to the Commission pursuant to the proposal should be done on a confidential, non-public basis and explicitly protected from FOIA disclosure requests.

III. RESPONSIBLE SCI PERSONNEL

The SROs are concerned about the scope of employees who could be considered "responsible SCI personnel." As defined, responsible SCI personnel would include any personnel, whether an employee or an agent, of an SCI entity having responsibility for an SCI system or SCI security system. Obligations for such personnel are contained in Rules 1000(b)(3) (Corrective Action), (b)(4) (Commission Notification), and (b)(5) (Dissemination of Information to Members or Participants). The guidance from the Commission in the Proposing Release specifies that individuals who have no responsibility for an SCI system are not responsible SCI personnel and makes clear the Commission's intent that both senior and junior level employees would be included. As a practical matter, this would appear to cover any employee who works in a technology or operations capacity for a department that maintains an SCI system or SCI security system. This imposition of regulatory liability on all such employees is overreaching and would likely have an adverse effect on an SCI entity's ability to hire skilled technology personnel. The SROs, therefore, recommend that the Commission consider limiting the definition of SCI personnel to senior technology or operational management or allow entities the ability to identify such responsible parties.

Similarly, the SROs are concerned about the "becomes aware" standard underlying the reporting requirements that would apply to responsible SCI personnel. In the SROs' experience, it is often not clearly apparent when personnel have in fact become aware that an SCI event has occurred or whether the event is significant. For example, in the case of systems compliance issues, a junior employee may identify a particular occurrence or a member may report some perceived problem to operations personnel, and it may then take several hours or days of research and analysis before personnel can determine whether the event in question was actually a systems compliance issue. In such cases, the exact moment responsible SCI personnel became aware that a potential issue or problem is also an SCI event may not be clear. The SROs are concerned that, in the inevitable instance of an SCI event, Commission staff may, as a matter of

course, second guess the timing of an SCI entity's reporting of SCI events based on its own interpretation of which particular employees are "responsible SCI personnel" and when they became "aware" of the SCI event.

Importantly, the SROs are concerned that these standards may lead such employees to be legitimately concerned about undue personal liability associated with their employment, which could impact the ability of SROs to attract and retain experienced personnel in information technology. Given the importance of human capital in creating, administering and evolving risk-management systems, striking an appropriate balance between individual and organizational responsibility should be an important consideration. The SROs believe a more prudent and balanced approach would be to trigger the mandatory reporting obligations when a designated senior officer or the SCI entity generally becomes aware of accurate and actionable information.

IV. SAFE HARBOR AND AN ALTERNATIVE

Proposed Regulation SCI contains a "safe harbor" provision which purports to limit liability for SCI entities and their staff who, despite good faith efforts to comply with the rules, fail to meet all of the requirements of proposed Rule 1000(b)(2)(i). However, given the numerous and different systems and structures of each SCI entity, the SROs believe that listing subjective criteria under proposed Rules 1000(b)(2)(ii) and (iii) is not an effective safe harbor insofar as it does not provide an objective and transparent mechanism to protect SCI entities and their personnel from liability. Given the complexity of proposed Regulation SCI, this protection is critically important to provide clear and transparent guidelines that enable SCI entities and individuals to discharge their Regulation SCI responsibilities, including open communication and collaboration with Commission staff, in a manner that supports fair and orderly markets.

The safe harbor proposed in Regulation SCI would be the first and only safe harbor adopted by the Commission related to policies and procedures.[21] The SROs believe that the proposed safe harbor should provide a more objective and transparent approach, giving SCI entities a clear, affirmative defense from allegations of having violated Regulation SCI. On the contrary, however, the provisions in the proposed safe harbor, as set forth in proposed Rules 1000(b)(2)(ii) and (iii), are vague, subjective and merely duplicate elements that would exist within a logical interpretation of Rule 1000(b)(1). In fact, this duplication offers no safe harbor protection at all.

Minor mistakes and unintentional errors do occur in the daily operations of running a business, and the SROs believe that a safe harbor should provide protection to SCI entities that follow the policies and procedures as intended, including in the resolution and containment of such mistakes and errors. Policies and procedures should be *reasonably designed* to ensure

---

[21] Commissioner Luis A. Aguilar, Developing Solutions to Ensure that the Automated Systems of Our Marketplace are Secure, Robust, and Reliable (Mar. 7, 2013) (available at https://www.sec.gov/news/speech/2013/spch030713laa.htm).

compliance; they are not, however, a failsafe against issues occurring notwithstanding. Accordingly, the SROs recommend that the safe harbor offer protection when the SCI entity maintains reasonable policies and procedures under proposed Rule 1000(b)(1) and proposed 1000(b)(2) and timely reports SCI events. There should be no entity or individual liability absent having knowingly violated Regulation SCI or the policies and procedures implemented by an SCI entity. Further, the safe harbor should apply to all of Regulation SCI, not just proposed Rule 1000(b)(2)(i).

To that end, the SROs propose that the Commission replace proposed Rule 1000(b)(2)(ii) and (iii) with the following:

(ii) Safe harbor from liability for SCI entities. An SCI entity shall be deemed not to have violated Regulation SCI if:

a) the SCI entity established and maintained written policies and procedures reasonably designed to comply with Regulation SCI; and
b) The SCI entity did not knowingly violate such policies and procedures.

(iii) Safe harbor from liability for individuals. A person employed by an SCI entity shall not be liable if:

a) The SCI entity established and maintained written policies and procedures reasonably designed to comply with Regulation SCI; and
b) The individual did not knowingly violate relevant policies and procedures.

While the above modification reflects the current limited scope of the proposed safe harbor, the SROs also request that the Commission specifically clarify its views on the protections provided by the safe harbor for inadvertent violations of other Commission laws, rules and regulations that arise, despite compliance with the regulation, from unintentional technological failures of SCI systems, and explicitly expand the safe harbor to cover such instances. In short, it is no comfort to SCI entities and their employees if their large investments in time, money and effort in adopting, implementing, overseeing and meeting the requirements of the regulation and safe harbor would nevertheless put them at risk of a discretionary enforcement action, not based on violation of the regulation itself, but on resulting violations of another law, rule or regulation enforced by the Commission.

V. DISASTER RECOVERY AND BUSINESS CONTINUITY PLAN TESTING

A. TESTING IN LIVE PRODUCTION

The Commission requested comment on the possibility of requiring business continuity and disaster recovery plan testing in a "live 'production' environment on a periodic basis."[22] The SROs do not support such a requirement. The SROs believe that a "live production" business continuity and disaster recovery test could compromise "normal" trading during this test period, while providing limited if any incremental benefit over the current industry weekend tests. Moreover, it would be impossible to create a real-life disaster situation since the test would not be conducted during a true wide-spread disruption, in which transportation and other services would likely be unavailable. The SROs agree with the Commission that SCI entities and their members should coordinate business continuity and disaster recovery plan tests as proposed in Rule 1000(b)(9)(ii). The Commission can either participate in the planning of such tests or be kept informed in the event it has suggestions for particular types of coordinated tests.

B. COORDINATION AND SCOPE OF TESTING

1. MANDATORY TESTING

Proposed Rule 1000(b)(9) would require an SCI entity, among other things, to perform, at least every 12 months, a functional and operational test of its business continuity and disaster recovery plans, including its back-up systems, with designated members or participants. Each SCI entity must notify the Commission of such designations and its standard for designation, and promptly update such notification after any changes to its designations or standards. The testing must also be performed in coordination with other SCI entities on an industry-wide or sector-wide basis.

The SROs are concerned that the broad language contained in proposed Rule 1000(b)(9) would result in complex and costly testing requirements that may not be effective or meaningful. The SROs request that the Commission narrow the scope of the proposed rule to only require an SCI entity to perform coordinated functional and operational testing of its disaster recovery plan. In addition, it is not clear what type of testing the SROs must perform in order to comply with the stated requirements. Accordingly, the SROs request additional guidance on the level and type of testing that is required under the proposed rule.

The requirements contained in proposed Rule 1000(b)(9) are similar to those contained in the Commission's Policy Statement on Business Continuity Planning for Trading Markets ("BCP Policy Statement").[23] The Commission outlined certain principles in the BCP Policy Statement

---

22 See Proposing Release, supra note 2, at 18113, 18127.

23 See Securities Exchange Act Release No. 48545 (September 25, 2003), 68 FR 56656 (October 1, 2003) (the "BCP Policy Statement").

that it expected each SRO operating a trading market and electronic communication network to incorporate in its business continuity planning, including: (i) "anticipating" the resumption of trading on the day following a wide-scale disruption; (ii) providing for geographic diversity between primary and back up sites; (iii) assuring full resilience of important shared information systems; and (iv) testing the effectiveness of back-up arrangements in recovering from a wide-scale disruption.[24]

The Commission notes in the Proposing Release that by requiring certain exchange members to participate in the testing of an SCI entity's business continuity and disaster recovery plans, it is fulfilling the objective of "ensuring resilient and available markets…."[25] The SROs are concerned that the Commission's approach as set forth in proposed Rule 1000(b)(9) imposes a significant cost burden on the SCI entities through its broad, one-size-fits-all approach, and it may not be an effective or efficient means of ensuring that markets can rapidly recover from a wide-scale disruption.

The SROs request that the Commission provide additional guidance with regard to the scope of functional and operational testing required to establish the effectiveness of an SCI entity's disaster recovery plans. The complexity and cost associated with establishing an effective coordinated test script that captures the significant number of possibilities that may occur to each significant market participant or SCI entity may outweigh the benefits to the industry associated with simulating real-life market conditions. A market participant may have enacted its business continuity plan but can still access an SCI entity through the primary facility. Other market participants may have initiated their disaster recovery plans and must access an SCI entity through back-up facilities. It is unclear what combination of testing would be required under the proposed rule.

The SROs recommend that the scope of the coordinated functional and operational testing requirements be narrowed to cover those instances in which an SCI entity determines to enact its disaster recovery plan. The SROs would suggest that the Commission avoid creating a one-size-fits-all approach to disaster recovery requirements and functional and operational testing of disaster recovery plans.

2. RAPID RECOVERY

The SROs believe that a rapid recovery, as demonstrated by the resumption of trading the day following a wide-scale disruption, is not necessarily the overriding goal in all cases. The SROs believe that trading markets may, in fact, compromise public safety and the maintenance of fair and orderly markets if trading is resumed the day after any wide-scale disruption without due regard to the facts and circumstances. As was the case during and immediately after

---

[24] See id. at 56658.

[25] See Proposing Release, supra note 2, at 18125, fn 266.

Superstorm Sandy, even if exchange members had the ability to trade on an SCI entity's primary or back-up facility, considerations of the public interest and the protection of investors, and the maintenance of fair and orderly markets, could properly result in a decision that the markets remain closed.

Furthermore, the Commission's current objective appears to contradict the BCP Policy Statement, which provides that rapid recovery "should not be regarded as a hard and fast deadline that must be met in every emergency situation. Various external factors, such as time of day, scope of disruption and status of critical infrastructure – particularly communications – can affect actual recovery times."[26] The SROs believe that the Commission and SCI entities must continue to evaluate each wide-scale disruption on a case-by-case basis to determine whether rapid recovery would be in the public interest and consistent with the Commission's core mission of investor protection and the maintenance of fair and orderly markets.

The Commission also indicated in the BCP Policy Statement that the resilience of a market's business continuity plan to resume trading should reflect "the extent of alternative trading venues for the securities traded by that market, including the number of sole listings on the market, the market share of the market, and the number of sole members or subscribers of the market."[27] The SROs believe that each SCI entity should be able to continue to consider these factors when determining the resilience required for its business continuity plan as well as other written policies and procedures under proposed Rule 1000(b)(1).

The reasonableness of this approach is supported by Commission statements relating to the level of systemic risk posed by individual trading markets in the BCP Policy Statement. The Commission believed that individual markets posed less systemic risk than the clearance and settlement system due to the fungible nature of trading activity, and that few securities were only traded on one market. Ten years later, trading activity has become even more diffuse and fungible as the number of trading venues increased and self-regulatory organizations operate more than one national securities exchange. Routing broker-dealers accelerate the portability of trading activity by providing non-members and customers with the ability to direct orders to numerous market venues. Given these important factors in the operation of today's securities markets, the SROs believe that the Commission should not require SCI entities to adhere to a single rigid standard.

VI. ACCESS TO LIVE OR PRODUCTION SYSTEMS BY COMMISSION

Proposed Rule 1000(f) would require an SCI entity to provide Commission staff with reasonable access to its SCI systems and SCI security systems for purposes of assessing the SCI entity's compliance with Regulation SCI. While "reasonable access" is not defined, the

---

[26] See BCP Policy Statement, supra note 23, at 56658, fn 6.

[27] See BCP Policy Statement, supra note 23, at 56658, fn 20.

Commission notes in the Proposing Release that this provision would facilitate either remote or on-site access and, for example, would enable Commission staff to test an SCI entity's firewalls and vulnerability to intrusion.

The SROs are concerned about the potential risks that such access could pose, including risks to the systems themselves, the security of the systems and confidential data stored in the systems. In a worst case scenario, there could potentially be market impact if, for example, information is inadvertently disseminated to the market or systems functionality is inadvertently disabled. The SROs believe that the risks (which exist when any third party has direct access to a system with which they are not familiar) would far outweigh any potential benefits. While the SROs understand the importance of Commission staff having the ability to assess an SCI entity's systems operations and protocols, we believe that the goals of Regulation SCI can be achieved with more limited access to an SCI entity's systems. Among other things, SCI entities can conduct systems demonstrations for Commission staff and conduct tests with Commission staff on-site to observe.

Accordingly, the SROs request that the Commission clarify that access under the proposed rule would be on-site only and supervised by the SCI entity's staff and would not include direct access by Commission staff to any production system.

VII. THE COMMISSION'S ECONOMIC/COST ANALYSIS

With respect to the Commission's cost estimates for proposed Regulation SCI, the SROs question whether the Commission has undertaken its analysis on the basis of a faulty premise. Specifically, the SROs question the Commission's assumption that the cost of compliance with Regulation SCI would merely be incremental as compared with the current baseline cost of voluntary compliance with the ARP regime. While entities covered by the ARP regime today strive to voluntarily observe the ARP guidance, particularly with respect to notification of system outages and related system compliance issues, it is possible that the mere codification of ARP guidelines as rules (and indeed is likely when considering the scope of the proposed new rules) would lead to an increase in notifications. This increase would simply reflect the desire of SCI entities to be conservative in compliance with the new rules. Based on the Commission's own estimates, it expects a ten-fold increase just for notifications of SCI events under proposed Rule 1000(b)(4). Some of the SROs perceive this to be a gross underestimate. It is unclear whether this increase would be due to the conversion of ARP from a voluntary to a mandatory regime, the addition of systems intrusions to the scope of reportable events, or other factors–but the concern remains that there would likely be a dramatic increase in notifications, which alone would bring a significant cost burden that requires further discussion and analysis.

Further, the SROs believe the Commission makes a number of other faulty assumptions in determining the cost-burdens for specific components of the proposed rules. For example, regarding Rule 1000(b)(4)(ii), no provision is made for the time burden that would be placed on technology personnel in connection with the notification process. In other sections, the

Commission either incorrectly assumes that no legal or outside counsel would be used or significantly underestimates the amount of legal or outside counsel expenses. The Commission also significantly underestimates the number of updates that would be required under Rule 1000(b)(4)(iii).

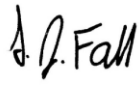
The SROs believe many of the economic and cost assumptions suggested by the Commission would benefit greatly from further discussion and analysis with the SROs, including on the overall time and cost burdens for each component of the proposed rules. As proposed, the rules run the risk of misallocating resources at both the Commission and at SCI entities.

* * * * *

The SROs appreciate the Commission's consideration of this comment letter. If you have any questions, please contact the undersigned.

Sincerely,

Eric Swanson
SVP, General Counsel and Secretary
BATS Global Markets, Inc.



Lisa J. Fall
President
BOX Options Exchange LLC

Joanne Moffic-Silver
Executive Vice President
General Counsel &
Corporate Secretary
Chicago Board Options Exchange, Inc.
C2 Options Exchange, Inc.

Peter D. Santori
Executive Vice President
Chief Compliance Officer
Chief Regulatory Officer
Chicago Stock Exchange, Inc.

Thomas N. McManus
Chief Compliance and Regulatory Officer
EDGA Exchange, Inc.
EDGX Exchange, Inc.

Marcia E. Asquith
Senior Vice President
and Corporate Secretary
Financial Industry Regulatory Authority

Michael J. Simon
General Counsel
Chief Regulatory Officer and Secretary
International Securities Exchange, LLC

Barbara J. Comly
EVP, General Counsel and
Corporate Secretary
Miami International Securities
Exchange, LLC

Joan Conley
Senior Vice President and
Corporate Secretary
The NASDAQ Stock Market LLC,
NASDAQ OMX PHLX LLC and
NASDAQ OMX BX, Inc.

Susan Ameel
Chief Regulatory Officer
National Stock Exchange, Inc.

Janet McGinness
EVP, Corporate Secretary and
GC – US Markets
New York Stock Exchange LLC
NYSE MKT LLC
NYSE Arca, Inc.

cc: Honorable Mary Jo White, Chair
Honorable Elisse B. Walter, Commissioner
Honorable Luis A. Aguilar, Commissioner
Honorable Troy A. Paredes, Commissioner
Honorable Daniel J. Gallagher, Commissioner

John Ramsay, Acting Director, Division of Trading and Markets
James R. Burns, Deputy Director, Division of Trading and Markets
David S. Shillman, Associate Director, Division of Trading and Markets
David Liu, Senior Special Counsel, Division of Trading and Markets