From: Alex Albert [redacted]]
Sent: Monday, September 22, 2014 11:17 AM
To: Aguilar, Luis A. (Commissioner)
Subject: Reg. SCI

Commissioner, understand that the Commission is late in the process with Reg. SCI, and I do not have a clear understanding of where things stand with the expanded coverage issue mention below. Nevertheless, it is important to us to compete on a level playing field and these regulations ultimately need to protect that concept. Therefore, I am raising this as an issue to review before final consideration. The current SEC proposal defines SCI Entities to include all exchanges, clearing houses, securities information processors and some ATSs. Our primary argument, as is noted in the attached comment letter **on pages 8-10**, has been that the definition of SCI Entity should be expanded to include all trading centers, not only large ATSs. While the proposed Reg. SCI estimated that 10 ATSs would be covered, it does not cover any broker-dealer trading centers regardless of their size. Given that non-ATS broker-dealers make up around 18% of CADV, we believe the SEC should focus on a trading centers' potential risk to the stability of the equities market over its regulatory designation.

***NOTE NEW OFFICE PHONE # BELOW. PLEASE UPDATE YOUR RECORDS**

Alex Albert
Intercontinental Exchange
[redacted] (0ffice)
(Cell)
[redacted]

Janet McGinness
EVP & Corporate Secretary

NYSE EURONEXT

July 9, 2013

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

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

Dear Ms. Murphy:

NYSE Euronext, on behalf of its wholly-owned subsidiaries, The New York Stock Exchange LLC, NYSE MKT LLC, and NYSE Arca Inc. (collectively, the "Exchanges"), appreciates the opportunity to comment on proposed Regulation Systems Compliance and Integrity ("Proposed Reg SCI") under the Securities Exchange Act of 1934 ("Exchange Act").[1] The Exchanges offer trading in equities, options, and exchange-traded products. Taken together, our equities markets represent approximately one-third of the world's equities trading and our options markets consistently rank among the top U.S. options markets in terms of market share.

The Exchanges agree with the main underlying principles of Proposed Reg SCI, namely that important market systems should have adequate levels of capacity, integrity, resiliency, availability and security to maintain their operational capability and promote the maintenance of fair and orderly markets, and such systems should operate in their intended manner. Therefore, we concur with the Securities and Exchange Commission ("SEC" or "Commission") that its oversight of this area is important, and that the Automated Review Policy program ("ARP") should be re-evaluated and updated based on the evolution of the marketplace. The Exchanges believe, however, that the SEC must make significant modifications to Proposed Reg SCI to ensure that its focus is on systems and events that are actually critical to the functioning of the securities markets. It would be a lost opportunity for the SEC and the industry if Proposed Reg SCI simply carried forward, mandated, and expanded the practices of the current voluntary ARP program, which, in the Exchanges' experience, has often suffered from a lack of focus on the truly critical market events and systems. Given that the SEC's interpretations of the scope of the ARP program have never been subject to public notice and comment – despite over 20 years of practice thereunder, the Exchanges feel strongly that industry opinions on Proposed Reg SCI should be considered fresh and in light of the realities of today's market

[1] Regulation Systems Compliance and Integrity, Securities Exchange Act Rel. No. 69077 (Mar. 8, 2013), 78 Fed. Reg. 18084 (Mar. 25, 2013) ("Proposing Release").

structure, rather than just in light of the history or scope of the ARP program itself. Such a process would ensure that any ensuing regulation reaches the identified objectives, and does so in the manner most beneficial to investors and the markets as a whole.

I. EXECUTIVE SUMMARY

The Exchanges believe that it is critical for all market participants to effectively implement technology in a way that protects investors and the markets and minimizes market disruptions. The fundamental concepts underlying Proposed Reg SCI go far in ensuring systems that are important to the markets have levels of capacity, integrity, resiliency, availability and security adequate to (i) maintain their operational capabilities, (ii) promote the maintenance of fair and orderly markets, and (iii) facilitate the operation of such systems in the manner intended. The Exchanges, however, are concerned that the proposed detailed, extensive oversight of technology is outside the regulatory authority of the Commission. The Exchanges are equally concerned that Proposed Reg SCI, as constructed, is unlikely to operate in a manner that will result in better SEC oversight to the benefit of investors and the markets, and will cost significantly more than any derived benefit. Indeed, even if Proposed Reg SCI had been previously adopted as proposed, it is arguably unlikely that it would have prevented all, or even many of, the recent significant market disruptions cited by the SEC in the Proposing Release.

Notwithstanding these threshold concerns, if the SEC were to move forward with regulation in this area, the Exchanges recommend that the SEC take this opportunity to engage in a detailed public analysis of the costs and benefits of the existing ARP program as a first step – an analysis that has not occurred to date. As discussed below, although Proposed Reg SCI is much broader than ARP in scope, it is based on ARP. By incorporating the many lessons learned from the implementation and application of ARP over the years, the Exchanges believe that the SEC may craft a more effective and efficient regulatory approach than Proposed Reg SCI. To this end, based on their experience as ARP participants and as electronic markets, the Exchanges recommend a variety of enhancements to the proposal to maximize its benefits, while minimizing the unintended adverse consequences and unnecessary costs to investors and the markets.

First and foremost, any regulation in this area must recognize that, because technology development, implementation and management are inherently complex and ever-changing, there will always be systems issues, regardless of reasonable efforts to the contrary. Moreover, such regulation should be narrowly focused to address the stated goals. To these ends, the Exchanges recommend the following significant modifications to Proposed Reg SCI:

(1) The SEC should expand the definition of SCI entities to cover all entities that may affect the integrity of our markets, including all ATSs and broker-dealers that execute orders internally. By excluding certain ATSs and internalizers, Proposed Reg SCI only covers a limited portion of the trading centers that are important to and have an impact on the national market system.

(2) Proposed Reg SCI should apply only to those systems that are reasonably likely to pose a plausible risk to the markets – that is, systems that route or execute orders, clear and settle trades, or transmit required market data – not regulation and surveillance systems or SCI security systems.

(3) The definition of an "SCI event" should be revised to capture genuinely disruptive events. Therefore the term should be refined by deleting "systems compliance issues" from the definition, and more clearly defining the terms "systems disruption" and "systems intrusion."

(4) To ensure that market participants take appropriate actions in the event of a systems issue, the Exchanges recommend the deletion of the concept of "responsible SCI personnel."

(5) In recognition of current technology practices, reasonable policies and procedures should include policies and procedures that are consistent with generally accepted technology principles, rather than "SCI industry standards," as defined in the proposal.

(6) The SEC should match the Commission notification requirements to the type of SCI event. Specifically, the Exchanges propose an alternative notification paradigm in which immediate Commission notification would be reserved solely for truly major market events; periodic reporting would be required for events of medium-level significance; and no reporting, only recordkeeping, would be required for minor events.

(7) The SEC should limit the scope of material systems changes that need to be reported to major changes, and require only periodic reporting of such changes.

(8) The SEC should only require the public dissemination of information about systems in significant circumstances where such information sharing enhances investor protection, and should only require that such information be shared with those parties affected by the systems issues. It should not be required where the information provided (*e.g.*, regarding systems intrusions or issues with surveillance systems) may be misused to the detriment of the markets.

(9) Proposed Reg SCI should provide a more robust safe harbor that adequately protects the reasonable compliance efforts of SCI entities and their employees.

(10) To ensure uniformity and clarity for all market participants, the SEC, not the SCI entities, should designate the frequency of, and required participants in, business continuity and disaster recovery plan testing.

(11) Consistent with current practice, reasonable security precautions require that SEC staff's access to systems of SCI entities be limited to information about the operation of the

systems; access to the live production systems of SCI entities would raise the very security and other issues Proposed Reg SCI is intended to mitigate.

(12) The Exchanges believe that any requirement for an annual review should incorporate a risk-based approach for determining the scope of the review.

II. SEC'S AUTHORITY TO ADOPT REG SCI

The Exchanges have concerns that the Commission does not have the legal authority to adopt Proposed Reg SCI. The authority the Proposing Release relies on most heavily is Sections 11A(a)(1) and (2) of the Exchange Act, which both concern facilitating the establishment of a national market system for securities. Section 11A(a)(2) of the Exchange Act directs the Commission, having due regard for the public interest, the protection of investors, and the maintenance of fair and orderly markets, to use its authority under the Exchange Act to facilitate the establishment of a national market system for securities in accordance with the Congressional findings and objectives set forth in Section 11A(a)(1) of the Exchange Act. Among the findings and objectives in Section 11A(a)(1) is that "[n]ew data processing and communications techniques create the opportunity for more efficient and effective market operations"[2] and "[i]t is in the public interest and appropriate for the protection of investors and the maintenance of fair and orderly markets to assure . . . the economically efficient execution of securities transactions."[3] Other provisions cited by the Commission, such as portions of Section 6(b) or 15A, do not add materially to the power of the Commission under Section 11A.[4] None of these provisions appear to provide legal authority for the SEC to adopt the Commission notification requirement set forth in Proposed Rule 1000(b)(4), the material systems change requirement set forth in Proposed Rule 1000(b)(6), or the access requirement set forth in Proposed Rule 1000(f). Indeed, the Exchanges' concerns regarding the SEC's legal authority may extend to other provisions in Proposed Reg SCI as well.

Reviewing courts regularly caution federal agencies about the need to stay strictly within the authority granted by Congress and not to extend that authority by overly broad constructions. Recently, the Supreme Court was unequivocal in stating: "No matter how it is framed, the question a court faces when confronted with an agency's interpretation of a statute it administers is always, simply, *whether the agency has stayed within the bounds of its statutory authority*."[5] The power of federal agencies "to act and how they are to act is authoritatively prescribed by Congress, so that when they act improperly, no less than when they act beyond their jurisdiction, what they do is ultra vires."[6]

---

[2] Section 11A(a)(1)(B) of the Exchange Act.

[3] Section 11A(a)(1)(C)(i) of the Exchange Act.

[4] Proposing Release at 18085.

[5] City of Arlington v. FCC, No. 11-1545 (U.S. decided May 20, 2013) (emphasis in original) *available at* http://www.supremecourt.gov/opinions/12pdf/11-1545_1b7d.pdf.

[6] *Id.*

Even broadly or generally worded regulatory authority is limited by the purposes of the statutes and is not endlessly elastic. The D.C. Circuit reached this conclusion specifically in connection with Section 11A of the Exchange Act. It rejected a Commission rule justified in part on Section 11A because the Commission's reading of its authority was overly broad. The court carefully examined the reasons and purposes behind a congressional grant of rulemaking power and confined the agency to reasonably related areas. This was especially necessary when considering Section 11A because Congress intended it to be essentially de-regulatory. The court explained that, in advancing the goal of a national market system, Congress directed the Commission to remove existing burdens on competition and to refrain from imposing, or permitting to be imposed, new regulatory burdens.[7]

These principles raise questions here because Proposed Reg SCI would impose significant obligations in areas that are considerably distant from the power conferred in Section 11A. Authority to facilitate a national market or assure economically efficient execution of securities transactions is remote from close, minute regulation of computer systems and computer security. A congressional recognition that "[n]ew data processing and communications techniques create the opportunity for more efficient and effective market operations" might authorize regulatory steps to promote new data processing and communications techniques but not a new detailed and intrusive regulatory regime applicable to the computer systems. It certainly does not support a series of obligations to provide the Commission with notices about systems issues and systems changes, or a legal duty to permit Commission representatives to gain physical access to exchange systems. In fact, nothing in the relevant statutes gives the Commission explicit power to require a regulated party to give the Commission notice of a systems issue or any other issue. We request that the Commission re-examine its legal authority and reconsider Proposed Reg SCI, with a focus on the proposals requiring SCI entities to provide notifications regarding systems issues and changes and permitting Commission representatives access to SCI systems and SCI security systems.

The concern about rule terms that exceed the SEC's legal authority is more pronounced than normal with Proposed Reg SCI because exchanges are self-regulatory organizations. The Exchanges are subject to frequent informal information requests, examinations, and other forms of extensive oversight by several different parts of the Commission, including ARP, the Office of Compliance Inspections and Examinations ("OCIE") (which already has a broad scope of authority) and the Division of Trading and Markets. Enforcement investigations and proceedings are a further overlay to those types of supervision. Proposed Reg SCI would significantly expand Commission oversight and control of the Exchanges and expose the Exchanges to a broad array of Commission information requests based on incidents covered by the regulation. Those information requests often become duplicative because information gathered by one area within the Commission is commonly provided to other parts of the Commission, which then make further inquiries. The regulation also would increase the risk of Enforcement interrogation and second-guessing, even for good faith compliance efforts,

---

[7] *Business Roundtable v. SEC*, 905 F.2d 406, 415-17 (D.C. Cir. 1990).

because Proposed Reg SCI would demand quick responses and rushed notifications often based on preliminary and incomplete information. For these reasons, it is especially important for the Commission to stay well within its legal bounds when determining the scope of a regulation such as Proposed Reg SCI.

Despite the Exchanges' concerns about the SEC's authority to adopt Proposed Reg SCI, the Exchanges nevertheless describe their recommendations as to how the regulation can be improved in Section IV below. The inclusion of such recommendations, however, is not intended to suggest that the Exchanges do not have concerns about the SEC's authority to adopt the regulation, even if modified as the Exchanges recommend.

III. EXPERIENCE UNDER ARP SHOWS THAT REG SCI SHOULD BE VIEWED ON ITS OWN MERITS, NOT SIMPLY AS A CONTINUATION OF ARP

The Exchanges believe that Proposed Reg SCI provides the SEC and market participants with the opportunity to carefully craft systems-related regulation that protects investors and the markets without unintended consequences and unnecessary costs. In doing so, each aspect of Proposed Reg SCI should be evaluated on its own merits, without any assumptions about its value merely because comparable measures existed under ARP. After all, ARP was originally implemented many years ago in a series of policy statements setting out guidance for voluntary compliance and supplemented with informal SEC staff guidance over the years, in many cases before many of the relevant systems or concepts even existed. As ARP was voluntary and consisted of guidance and not rules, it was never subjected to the thorough SEC rulemaking process with its attendant notice and public comment requirements, including a cost-benefit analysis. In addition, Proposed Reg SCI differs from the ARP program in many ways, calling into question the validity of comparisons between the two in the first instance. Moreover, the Exchanges believe that various aspects of the current ARP program could be improved upon. Therefore, each of the practices under the ARP program should be carefully evaluated for their efficacy and cost-effectiveness before incorporating them into any new and mandatory regulation.

A. AFTER 20+ YEARS OF EXPERIENCE UNDER ARP, THE EXCHANGES BELIEVE MANY PRACTICAL ISSUES NEED TO BE ADDRESSED

In the Exchanges' experience, the ARP program, both in terms of its written requirements and its current practical implementation, could be substantially improved. Such improvements would enhance the efficacy of the intended oversight while minimizing the various costs to the covered entities. Therefore, the Exchanges do not believe that the practices under ARP should be implemented in the context of Proposed Reg SCI without careful analysis.

The Exchanges also believe that Proposed Reg SCI should maintain its intended focus – that is, ensuring that market-related systems have appropriate capacity, integrity, resiliency,

availability and security. In our view, the ARP program has suffered at times from a lack of focus on the truly critical market events and systems and has raised the risk of the misallocation of both Exchange and SEC resources away from collaborative efforts for addressing systems issues.

The Exchanges also urge the SEC to reconsider its internal organizational structure in light of the oversight that will be necessary for Proposed Reg SCI. In the Exchanges' experience, oversight responsibility by both the ARP inspections staff in the Division of Trading and Markets and OCIE seems duplicative and inefficient. For example, the Exchanges often are required to submit to follow-up questions from both ARP and OCIE no matter which group has primary oversight of an event. In many instances, the level of attention for a particular event is disproportionately high when compared to the event's significance. Further, such inquiries from the staff often come during critical periods when the very same personnel at the Exchanges needed to respond to the staff's inquiries are engaged in correcting systems issues. Therefore, the Exchanges recommend that the SEC evaluate how to organize its internal resources for implementing Proposed Reg SCI while also allowing the Exchanges to attend to the most important matter at hand: the integrity of the markets. A more cooperative relationship between SCI entities and the SEC and its staff will be critical to the effective implementation of systems oversight.

B. REG SCI SIGNIFICANTLY EXPANDS ARP'S SCOPE WITHOUT NECESSARILY ADDRESSING ITS SHORTCOMINGS

The Exchanges believe that Proposed Reg SCI is significantly different from ARP, despite the Commission's description of Proposed Reg SCI as a codification and enhancement of ARP. Although Proposed Reg SCI incorporates concepts similar to ARP, Proposed Reg SCI revises ARP requirements, introduces new requirements, and generally expands the reach and scope of the ARP guidance. A comparison of the relevant ARP guidance and Proposed Reg SCI reveals a variety of notable differences. These differences include, but are not limited to, the following:

- Proposed Reg SCI expands the class of entities subject to review, by adding the Municipal Securities Rulemaking Board as well as additional ATSs.

- Proposed Reg SCI expands the types of systems subject to review. Unlike ARP, Proposed Reg SCI would apply to regulatory and surveillance systems and SCI security systems.

- Proposed Reg SCI expands the types of events subject to action and notification to include "systems compliance issues."

- Proposed Reg SCI expands and enhances the requirement to provide advanced notice of certain systems changes.

- Under Proposed Reg SCI, the requirement to notify the SEC of systems issues would apply to more entities, more systems and more types of systems issues. In addition, Proposed Reg SCI would accelerate the timing of notifications regarding systems events, increase the level of detail and analysis required in the notification and multiply the number of notifications required for a single event.

- Proposed Reg SCI introduces an all new requirement to disseminate information to members or participants.

- Proposed Reg SCI would create a new requirement mandating that members or participants of SCI entities take part in testing the SCI entity's business continuity and disaster recovery plans.

- Proposed Reg SCI would create new recordkeeping requirements for all SCI entities that are not self-regulatory organizations that may become subject to Proposed Reg SCI.

Given that ARP and Proposed Reg SCI are similar in concept but very different as a practical matter, the Exchanges believe that it is more accurate to view Proposed Reg SCI as a brand new regulatory regime that requires its own cost-benefit analysis. Indeed, had ARP been subject to public notice and comment at some point in the last 20+ years, this analysis would have taken place already. The Exchanges urge the SEC to not compound that missed opportunity by assuming incorrectly that ARP itself is the appropriate baseline for Proposed Reg SCI.

IV. COMMENTS ON PROPOSED REG SCI

A. PROPOSED REG SCI SHOULD APPLY TO ALL MARKET PARTICIPANTS WHOSE SECURITIES ACTIVITIES MAY IMPACT THE INTEGRITY OF THE MARKETS

The requirements of Proposed Reg SCI would apply to "SCI entities," which include national securities exchanges registered under Section 6(b) of the Exchange Act, registered securities associations, registered clearing agencies, the Municipal Securities Rulemaking Board, SCI ATSs, plan processors, and exempt clearing agencies subject to ARP.[8] This definition reflects the combined historical reach of ARP and Regulation ATS, but does not reflect the realities of today's market. As the SEC notes, "[r]ecent events have highlighted the significance of systems integrity of a broader set of market participants than those proposed to be included within the definition of SCI entity."[9] Therefore, the Exchanges recommend that the term "SCI entity" be extended to the ATS and broker-dealer entities covered by the Regulation NMS definition of a "trading center." Specifically, Section 600(b)(78) of Regulation NMS includes within the definition of a "trading center" "an ATS, an exchange market maker, an OTC market maker, or

[8] Rule 1000(a) of Proposed Reg SCI.

[9] Proposing Release at 18138.

any other broker or dealer that executes orders internally by trading as principal or crossing orders as agent." By virtue of such an extended scope, Proposed Reg SCI would cover all entities whose securities activities may impact the overall markets.[10] Furthermore, a failure to include these additional entities would exacerbate what the Exchanges view as an artificial and uneven application of regulation across trading centers by the Commission. Congress directed the Commission to remove existing burdens on competition and to refrain from imposing, or permitting to be imposed, new regulatory burdens. It is hard to imagine how Proposed Reg SCI would comply with this statement if it would not apply to thirty percent or more of the market.

1. BROKER-DEALERS THAT EXECUTE ORDERS

The goals of Proposed Reg SCI cannot be met without expanding its reach to include exchange market makers, OTC market makers, and any other broker or dealer that executes orders internally by trading as principal or crossing orders as agent. These broker-dealers play critical roles in today's markets, and in doing so, rely heavily on sophisticated automated systems, just as exchanges and ATSs do. For example, OTC market makers, which handle a large portion of order flow in the market, would not be covered by Proposed Reg SCI. Yet, a systems issue at such an OTC market maker not only may affect the many orders being handled by the OTC market maker, but may also pose a significant risk to the market by, for example, creating capacity issues at other venues accepting re-routed orders. Moreover, the Exchanges believe that the volume handled by many such broker-dealers exceeds that of certain ATSs that would be included in Proposed Reg SCI.[11]

Moreover, the Exchanges do not believe that the SEC can rely on Rule 15c3-5 to ensure the integrity of these broker-dealers' systems. Rule 15c3-5 is focused on the implementation of risk management and supervisory controls to limit risk associated with routing orders to exchanges or ATSs. It does <u>not</u> address the reliability or integrity of the systems that implement such controls. Therefore, although such filters and other risk controls may prevent the submission of erroneous or otherwise problematic orders to the market if they are operating properly, erroneous orders will still reach the market if those systems fail. In contrast, Proposed Reg SCI would focus on ensuring that the systems implementing risk controls are operating properly. Indeed, the SEC recognizes in the Proposing Release that Rule 15c3-5 takes "a different and more limited approach" than Proposed Reg SCI, and that Rule 15c3-5 is

---

[10] Such a modification would be consistent with the SEC's approach in recently adopted rules in which the SEC sought to capture all relevant trading activity, rather than limiting its efforts to certain segments of the market. *See, e.g.*, Rule 613 (regarding the consolidated audit trail).

[11] Based on consolidated tape data for May 2013, total off-exchange trading share in NMS securities on the Trade Reporting Facilities was 36.1%. According to Rosenblatt Securities, five ATSs with over 1% market share each were responsible for 6.2% of the 36.1%. These ATSs would appear to satisfy the threshold requirements for Proposed Reg SCI. According to Rosenblatt Securities, there was an additional thirteen ATSs with less than 1% market share. Therefore, we estimate that entities not subject to Proposed Reg SCI would have been responsible for 29.9% of volume in May 2013.

designed to address only "some of the same concerns regarding system integrity discussed in the proposal."[12]

2. ALTERNATIVE TRADING SYSTEMS

The Exchanges believe that the definition of "SCI ATS" should be expanded to include all ATSs. As discussed above with regard to other broker-dealers, all ATSs have the potential to negatively affect the markets in the event of a systems problem. Moreover, the reliance on calculated thresholds, as proposed in the definition of "SCI ATS," draws an artificial line between similar ATSs that cross the threshold and those that do not, and would permit an ATS to avoid the application of the Rule by purposely limiting trading on its system.

B. THE SEC SHOULD FOCUS PROPOSED REG SCI ONLY ON THOSE SYSTEMS THAT POSE A PLAUSIBLE RISK TO THE PUBLIC MARKETS

1. SCI SYSTEMS

The Commission proposes to define the term "SCI systems" to 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 support trading, clearance and settlement, order routing, market data, regulation, or surveillance."[13] The Exchanges believe that this proposed definition is overly broad and vague, and should be revised to focus on those systems that would be reasonably likely to pose a plausible risk to the public markets in the course of routing, executing, clearing and settling orders, or transmitting required market data. [14]

The Exchanges believe that the SEC's proposed definition is overly inclusive, covering a variety of systems that are not components of the critical systems infrastructure of SCI entities. The Exchanges agree that systems that directly enable the routing or execution of orders, and the clearance and settlement of trades, or directly transmit required market data should be included within the definition of an SCI system. The definition, however, does not make clear how to draw the line between systems that do and do not directly support those functions. The Exchanges believe that the key to whether a proposed supporting function should be included in the definition is whether or not it is critical to the proper operation of a core functionality.

The Exchanges also believe that the definition of SCI systems is over-inclusive with regard to market data-related systems. Both Congress and the Commission have emphasized the importance of consolidated market data as a comprehensive, accurate and reliable source

---

12 Proposing Release at 18139.

13 Rule 1000(a) of Proposed Reg SCI.

14 The Exchanges recommend that the SEC clarify that the definition of SCI system is separate and distinct from the definition of a facility, as set forth in Section 3(a)(2) of the Exchange Act.

of information for the prices and volume of NMS stocks, as well as for compliance purposes.[15] Thus, Proposed Reg SCI should be limited to systems that directly support "the transmission of market data as required by the Exchange Act and the rules and regulations thereunder."[16] As such, the definition of SCI systems would not include the transmission of proprietary market data feeds, as they are not required under the Exchange Act.[17]

In addition, the definition of SCI system should not include systems used for regulation or surveillance. Such systems are essential for investor protection and market integrity, but, unlike trading-related systems, regulatory and surveillance systems generally do not operate on a real-time basis or have any real-time impact on trading. Therefore, much of Proposed Reg SCI, with its focus on immediate reporting and other responses to systems issues, would not make sense for regulatory and surveillance systems. Similarly, any public dissemination of information related to problems with regulatory or surveillance systems would be ill-advised as it may provide a roadmap for violative market behavior. The Exchanges believe that an approach that requires periodic reporting to the SEC of material outages or delays in the operation of regulatory and surveillance systems, pursuant to appropriate policies and procedures, would support the goals of Proposed Reg SCI, without imposing undue burdens on SCI entities or raising the risk that market participants would purposefully direct order flow to SCI entities experiencing regulatory or surveillance systems issues.

In addition, the Exchanges believe that the phrase "whether in production, development, or testing" should be eliminated from the definition. Only systems being used in production should be included. Systems that are in development or being tested, and not in production, by definition, would not represent a plausible risk to the markets.

2. SCI SECURITY SYSTEMS

Proposed Reg SCI applies, in part, to "SCI security systems," which are defined as "any systems that share network resources with SCI systems that, if breached, would be reasonably likely to pose a security threat to SCI systems."[18] As discussed below, given the inherently interconnected nature of technology infrastructure today, this definition is vastly overbroad and would create a significant compliance burden for SCI entities without materially augmenting investor protection. Therefore, the term "SCI security systems" should be deleted entirely from Proposed Reg SCI, and Proposed Reg SCI should be revised to focus solely on the core systems of SCI entities.

---

[15] Concept Release on Equity Market Structure, Securities Exchange Act Rel. No. 61358 (Jan. 14, 2010), 75 Fed. Reg. 3594, 3600 (Jan. 21, 2010).

[16] This provision would include the transmission of market data as required by Rules 601through 604 of Regulation NMS, and Rule 301(b)(3) of Regulation ATS, as well as the related joint industry plans – the CTA Plan, the CQ Plan and the UTP Plan.

[17] The Commission's focus with respect to proprietary market data feeds has been on ensuring that such information is made available by exchanges on fair, reasonable and non-discriminatory terms.

[18] Rule 1000(a) of Proposed Reg SCI.

The proposed definition of "SCI security systems," is overly broad, vague and too simplistic in its approach. The Commission provides a window into the breadth of this term in the Proposing Release. The SEC states that this term includes systems that may be accessed by employees, clients, participants, or others that "may, in some instances provide a point of access (and thus share network resources) to an SCI entity's SCI systems."[19] Given the networked nature of today's business functions, almost all systems may provide a point of access to core systems in some manner. For example, the SEC notes in the Proposing Release that SCI security systems may include such corporate functions as email and support services. It is possible that the definition could potentially include end user workstations or Blackberries. Indeed, it is difficult to envision any system that is part of an SCI entity's network that would not meet this definition. Moreover, the breadth of the definition is exacerbated by its reliance on certain undefined terms, including "share" and "network resources," that are subject to broad interpretation.

The SEC's goal with Proposed Reg SCI is "to ensure that SCI systems, as the core systems of an SCI entity, are adequately secure and protected from systems intrusions."[20] The SEC need not extend Proposed Reg SCI beyond SCI systems to achieve this goal; rather, the SEC may achieve its objectives more efficiently by removing SCI security systems from the purview of Proposed Reg SCI and instead focusing on actual intrusions of SCI systems. Therefore, the Exchanges recommend that the SEC limit the scope of the proposed rule to SCI systems, but clarify that policies and procedures reasonably designed to ensure that SCI systems have adequate levels of security necessarily would require an assessment of security vulnerability created by other systems, and appropriate steps to address those vulnerabilities. For example, SCI entities could evaluate the security threat of any SCI system by looking at a variety of factors, including, among other things, directionality of information flow, firewalls, and network architecture, and adopt procedures that address identified security threats. Such an approach would reduce unnecessary compliance burdens for SCI entities, and improve the efficiency of Commission oversight without materially undermining its effectiveness.

C. THE DEFINITION OF "SCI EVENT" SHOULD BE LIMITED TO GENUINELY DISRUPTIVE SYSTEM EVENTS

Proposed Reg SCI would define an "SCI event" to mean "an event at an SCI entity that constitutes: (1) a systems disruption; (2) a systems compliance issue; or (3) a systems intrusion."[21] Proposed Reg SCI then defines each of these three categories in turn. As discussed in detail below, the Exchanges believe that the SEC should eliminate from the definition of "SCI event" "systems compliance issues" entirely, and more clearly and narrowly define the terms "systems disruption" and "systems intrusion."

---

19 Proposing Release at 18099.

20 *Id*. at 18100.

21 Rule 1000(a) of Proposed Reg SCI.

1. SYSTEMS DISRUPTION

The Exchanges recommend that the SEC revise and clarify the definition of "systems disruption." First, each of the elements of the definition, as currently drafted, raises practical and interpretive issues.

- The first element – a failure to maintain service level agreements or constraints – should be eliminated. An SCI entity's regulatory requirements should not depend upon the negotiated language of an agreement between business partners. This is particularly true in cases where service level agreements are more stringent than, or are in addition to, any regulatory requirements. In those cases, the operation of the proposed definition would transform complying with a service level agreement into a new regulatory obligation for the SCI entity, as a failure to comply with the agreement would give rise to the obligation to take corrective action regarding the event as well as reporting obligations. The Exchanges believe that bootstrapping regulatory obligations to privately negotiated agreements exceeds the SEC's rulemaking authority. Moreover, an unintended side effect of such a requirement might be the limitation or elimination of service level agreements.

- The second element – disruption of normal operations, including switchover to back-up equipment with near-term recovery of primary hardware unlikely – needs clarification. The phrase "disruption of normal operations" is vague and over-broad, potentially capturing myriad events that are limited in scope and only narrowly affect the markets or market participants.

  By way of example, the SEC explains that this element is intended to cover, among other things, testing errors.[22] It is unclear what that means (*e.g.*, errors that occurred in production but were the result of poor testing; or errors that occur in the testing phase). At a minimum, it should not cover errors in the testing phase. Similarly, the SEC explains that this element also would cover instances in which a systems release is backed out after it is implemented. Yet, not all "back outs" are the result of a systems problem, and should not give rise to a reportable event.

- In the Proposing Release, the SEC indicates that the third element – a loss of use of any such system – would include a failure of primary trading or clearance and settlement systems, even if immediately replaced by back-up systems without any disruption to normal operations.[23] This element should not include immediate failovers to a back-up system. If a system works as designed and fails over smoothly with no impact or with little impact on the operation of an SCI entity, the failover should not be a reportable

---

22 Proposing Release at 18101.

23 *Id.* at 18101.

event. Indeed, such a failover would be better labeled as normal operations than a disruption of normal operations.

- With regard to the fifth and sixth elements – significant back-ups or delays in processing and significant diminution of ability to disseminate timely and accurate market data, the Exchanges agree with the SEC that these elements would not apply in those cases where message traffic is intentionally throttled, as the Exchanges and other gateways are designed to do. [24] The Exchanges do not agree, however, that customer complaints about slowness or disruption of market data should be a basis for determining whether there has been a systems disruption. Indeed, slowness that is the subject of complaints may be caused by the customer's systems issues.

- Finally, it is imperative that the SEC provide additional guidance regarding relevant queues for the seventh element – queuing of data between system components or queuing of messages to or from customers of such duration that normal service delivery is affected – since all systems have queues to some extent with normal functionality (*e.g.*, peak times), and only certain queues trigger recovery actions.

Second, the definition fails to include a materiality threshold for at least four of the above seven elements. In particular, paragraphs (1), (2), (3) and (4) do not require that the event be material or significant. The Exchanges believe that immaterial and insignificant systems issues should not be included in the definition of a systems disruption.

Third, the definition of a systems disruption needs to be reworked to ensure that the elements make sense for each of the different types of systems at issue, not just trading systems. For example, if, notwithstanding our recommendation to the contrary, an SCI system continues to include regulatory and surveillance systems, the SEC needs to consider a workable definition for when a regulatory or surveillance system is experiencing a systems disruption. Such regulatory systems generally operate on a post-trade basis and minor delays in running a surveillance or other review should not be viewed as a disruption.

Given the vagueness and potential breadth of the language of the definition of "systems disruption," the Exchanges believe that they would need to interpret the provision broadly, thereby capturing far more events than previously covered under ARP. Specifically, not only would the Exchanges report significant loss of functionality (with or without Exchange processes continuing to function), but also more routine functionality concerns. Such a change could easily result in a very significant increase in the number of covered systems disruptions. Therefore, the Exchanges urge the SEC to address the interpretive issues raised by the definition.

---

[24] *Id.* at 18102, n. 150.

2. SYSTEMS INTRUSION

The SEC proposes to define a "systems intrusion" as "any unauthorized entry into the SCI systems or SCI security systems of an SCI entity." Although the Exchanges believe that it is appropriate to include systems intrusions within Proposed Reg SCI, the Exchanges believe that the proposed definition is vague and over-inclusive. The Exchanges have experienced no intrusions to their systems that have caused any disruption to their markets. Because any such activity that was intended to be intrusive was addressed by the Exchanges' intrusion prevention measures, the Exchanges believe that such events should not be captured by the definition of systems intrusion. Given the vagueness of the proposed definition, however, the Exchanges are concerned that the Commission has underestimated the number of security-related incidents that might be reportable under the current definition, most of which are events related to SCI security systems and not SCI systems. Such events could include commonplace activity like anti-virus incidents, proactive measures to block escalated malicious activity, or account access events. Reporting such intrusions makes little sense if, as has been the experiences of the Exchanges, the intrusions cause no disruption to an SCI entity's market. Therefore, the Exchanges would recommend significant modifications to the definition to narrow its breadth and provide greater technical guidance for determining when a covered systems intrusion occurs.

First, the description of a systems intrusion as "any unauthorized entry" into a relevant system provides little guidance regarding the type of intrusions included in or excluded from Proposed Reg SCI. The term "entry" could be interpreted in various ways with regard to systems. By way of an over-simplified layman's example, it is unclear from this definition at what point a computer virus would rise to an intrusion – as soon as it infects the computer, or only if the virus is not caught by anti-virus software? In either scenario, the virus has made an unauthorized entry into a computer. Therefore, the Exchanges recommend that the definition focus on the unauthorized control of the confidentiality, integrity or availability of an SCI system and/or its data. With these changes, a systems intrusion would include the following: (1) keylogger or malware that captures files and sends them to a command and control computer, because it compromises confidentiality; (2) successful unauthorized log in to a system because it compromises integrity; and (3) malware that erases files, because it compromises the availability of data.

Second, like the definition of systems disruption, the definition of systems intrusion is not limited to material intrusions that pose a plausible risk to the core systems. Therefore, the Exchanges believe that the definition should be amended to include only major intrusions that pose a plausible risk to the trading, routing or clearance and settlement operations of the exchange, or to required market data transmission. In this regard, the Exchanges do not believe that inadvertent grants of access to SCI entity personnel should be deemed systems intrusions provided they are promptly addressed upon discovery.

Third, while the Proposing Release clarifies that the definition of a systems intrusion does not cover "unsuccessful attempts at unauthorized entry,"[25] the Exchanges believe that the SEC should revise the definition of "systems intrusion" to explicitly use the term "successful." With this clarification, the Exchanges believe that the following are examples of unsuccessful intrusions that would be outside the proposed definition: (1) downloaded malware quarantined by anti-virus software; (2) downloaded malware that the command and control connection has blocked and manually remediated; (3) failed log in attempts; and (4) portscans.

Fourth, the proposed definition of systems intrusion would apply not only to unauthorized entries into SCI systems, but also to unauthorized entries into SCI security systems. The Exchanges believe that only intrusions of SCI systems should be included, not intrusions of SCI security systems. For purposes of Proposed Reg SCI, an intrusion should only be relevant to the extent that it affected the core systems of an SCI entity. Merely breaching SCI security systems without also breaching the SCI systems should not rise to the level of an SCI event.

3. SYSTEMS COMPLIANCE ISSUE

The SEC proposes to include systems compliance issues in the definition of an SCI event. A systems compliance issue would be defined as "an event at an SCI entity that has caused any SCI system of such entity to operate in a manner that does not comply with the federal securities laws and rules and regulations thereunder or the entity's rules or governing documents, as applicable." The Exchanges believe that a systems compliance issue differs materially from a systems disruption or systems intrusion. Rather than providing a factual description about an operational issue with the system, such as for a systems disruption or systems intrusion, a systems compliance issue describes a legal conclusion about such a systems issue. Indeed, any report regarding a systems compliance issue is, by definition, an admission that the SCI entity has violated a law, rule or one of its governing documents. The Exchanges believe that a reporting obligation specifically focused on legal conclusions creates a substantial risk of an enforcement action or other liability for the SCI entity when, instead, the focus of Proposed Reg SCI should be on promoting the efficacy of the operations of SCI entities and SCI systems. Therefore the Exchanges recommend the deletion of the term "systems compliance issue" from the definition of an SCI event.

The Exchanges do not believe that the exclusion of systems compliance issues from the definition of an SCI event will undermine the SEC's oversight of SCI entities. For example, under paragraph (b)(2), Proposed Reg SCI would still require that SCI entities adopt reasonably designed policies and procedures for ensuring that the SCI systems operate in a manner that complies with the federal securities laws and rules and regulations thereunder and the entity's rules and governing documents. In addition, the SEC remains empowered to take enforcement

[25] Proposing Release at 18103.

action against an SCI entity for violation of the Exchange Act or any rules and regulations thereunder arising from a systems-related issue when the required facts are present. Therefore, the inclusion of systems compliance issues in the definition of an SCI event merely creates a burdensome and redundant layer of regulation.

4. THE NUMBER OF REPORTABLE SCI EVENTS

The Exchanges endeavored to perform an analysis of the potential number of reportable SCI events in order to evaluate the cost analysis provided by the Commission in the Proposing Release. We discuss that analysis below but need to make a few introductory remarks. First, for the reasons given above, the experience of the Exchanges under ARP is not likely to be indicative of what would occur under Proposed Reg SCI. Proposed Reg SCI is more inclusive and broader than ARP, as the Proposing Release acknowledged. Second, ascertaining the scope of Proposed Reg SCI is difficult because of the vagueness of the definitions of a systems disruption, systems intrusion, and systems compliance issue, the ill-defined materiality standard for systems disruptions, and the lack of a materiality standard for systems intrusions. With those qualifications, we now address the potential increased cost burden of Proposed Reg SCI.

As it explained, the SEC expects a significant increase in reportable events under Proposed Reg SCI.

> Because the proposed definition of "SCI event" is broader than the types of events covered by the current ARP Inspection Program, and SCI entities are not currently required by law or rule to report systems issues to the Commission, the Commission preliminarily believes that the number of SCI events that would be reported to the Commission would be significantly more than the number of incidents reported in 2011.[26]

Specifically, the Commission states that each ARP participant reported an average of six incidents in 2011.[27] For Proposed Reg SCI, the Commission anticipates 65 reportable events – a more than ten-fold increase in reportable events. The Commission does not attempt to categorize the number of disruptions, intrusions or compliance issues that make up the forecasted 65 events; the SEC merely states that the estimate is "based on the Commission's experience with the ARP inspection program."[28]

In an attempt to validate the SEC's forecast of 65 events per year, the Exchanges performed an analysis of the number of reportable SCI events the Exchanges could potentially experience using their best guess at the meaning of various definitions in Proposed Reg SCI. The Commission states that 175 events were reported under ARP in 2011 at an average of 6

---

[26] Proposing Release at 18148-149, n. 409 (emphasis added).

[27] *Id.*

[28] *Id.* at 18148.

events per covered entity. Even though the Commission's estimate of 65 events represents a ten-fold increase over reportable events under ARP, the Exchanges believe that this number could be low. Based on their best reading of the more expansive definitions of disruptions and intrusions set forth in Proposed Reg SCI, the Exchanges believe a more accurate estimate could be anywhere from 200 to 500 events per year per Exchange.

The Exchanges estimate that even at 65 notifications per year, a significant number of full-time staff (including legal, compliance, technical and operations staff) would be required to comply with just the Commission notification process under Rule 1000(b)(4). The number of full-time staff dedicated solely to Commission notification would need to increase commensurate to the number of notifications.

Finally, the Commission estimates the total annual ongoing record-keeping burden for Proposed Reg SCI to be $738,000, $528,000 of which is solely to comply with Rule 1000(b)(4). We believe this number does not accurately reflect the on-going costs of the new administrative burdens associated with Proposed Reg SCI. Further, if 70% of the ongoing record-keeping burden relates to notification of SCI events to the SEC, and not to the writing and maintenance of policies and procedures under Rules 1000(b)(1) and (b)(2) and other substantive provisions of Proposed Reg SCI, one must question the objectives and efficiency of the proposed regulation. After all, creating and maintaining reasonable policies and procedures to seek to ensure that important market systems have adequate levels of capacity, integrity, resiliency, availability and security should be the main focus of the regulation, not the reporting provisions.

D. THE CONCEPT OF REG SCI PERSONNEL SHOULD BE ELIMINATED FROM PROPOSED REG SCI

Proposed Reg SCI introduces the phrase "responsible SCI personnel," which is defined to mean "for a particular SCI system or SCI security system impacted by an SCI event, any personnel, whether an employee or agent, of the SCI entity having responsibility for such system."[29] Proposed Reg SCI then imposes certain obligations on responsible SCI personnel under paragraphs (b)(3) (Corrective Action), (b)(4) (Commission Notification), and (b)(5) (Dissemination of Information to Members or Participants). Specifically, under each of these paragraphs, an SCI entity must take certain action upon any responsible SCI personnel becoming aware of certain SCI events. The Exchanges believe that the trigger for the regulatory obligation – that is, when "a responsible SCI personnel" becomes "aware" of the SCI event – is vague and will be difficult to apply in practice. Therefore, the Exchanges believe that the defined phrase "responsible SCI personnel" should be eliminated entirely from Proposed Reg SCI and the proposed trigger should be replaced with an SCI entity having a reasonable basis to conclude that a relevant SCI event has occurred.

[29] Rule 1000(a) of Proposed Reg SCI.

As a practical matter, imposing a requirement to take action upon responsible SCI personnel becoming aware of an event would not be feasible. These provisions inappropriately impose the duty to take regulatory action on too broad a category of personnel. The term "responsible SCI personnel" may include, among others, low level employees and third party agents. Such personnel may gain some knowledge about a system operating other than in its normal fashion in the course of their duties. Such personnel, however, are unlikely to be able to determine whether the event satisfies the definition of an SCI event, and, therefore, would give rise to a reporting obligation under Proposed Reg SCI. Moreover, an SCI entity is unlikely to empower such employees to take regulatory actions without supervision. At best, such personnel will be able to escalate the issue to a supervisor, who can work with decision makers at the SCI entity to determine whether the SCI entity must take action under Proposed Reg SCI. Therefore, this requirement, as currently drafted, disrupts any reasonably-sized organization by intruding into the normal decision making chain of command. Moreover, it interferes with a company's normal management process of information gathering and analysis, consulting with lawyers as necessary, and making an appropriate decision as to whether the systems issue qualifies as one that is subject to Proposed Reg SCI.

In addition, imposing regulatory liability on all responsible SCI personnel is likely to have a chilling effect on the hiring of skilled IT personnel. The SEC should allow each SCI entity the flexibility to identify the appropriate responsible parties for these regulatory obligations under Proposed Reg SCI. In this way, the SCI entity can ensure that the appropriately senior personnel understand their particular responsibilities, and are authorized to take the necessary actions under the rule.

The difficulty of applying the proposed trigger is exacerbated by the reliance on the overly vague "awareness" standard for determining when action is required. It is unclear what level of knowledge is considered "awareness" for the purposes of these provisions. For example, various personnel may have partial knowledge of a systems issue that may or may not give rise to awareness of an SCI event. Or, if a responsible SCI personnel sees some type of exception alert regarding a possible systems issue, it is unclear at what point it gives rise to an awareness of a systems issue.

Moreover, because the regulatory obligation hinges on the employee's awareness, despite the employee's possibly limited ability to make the type of decision required (as discussed above), the regulatory requirement may negatively affect the job performance of relevant personnel. With concerns about regulatory repercussions in mind, the personnel may over-report incidents to ensure compliance, or under-report incidents due to a fear of making an incorrect determination about the severity of the event.

Therefore, to address the above concerns, the Exchanges recommend the deletion of the definition of "responsible SCI personnel" in paragraph (a) of Proposed Reg SCI. Correspondingly, the phrase "[u]pon any responsible SCI personnel becoming aware of" in paragraphs (b)(3)-(5) of Proposed Reg SCI should be replaced with the concept of an "SCI entity

having a reasonable basis to conclude" that a relevant SCI event has occurred. Accordingly, an SCI entity could adopt reasonable policies and procedures for designating personnel responsible for compliance with this provision, and for identifying and escalating possible SCI events to the appropriate decision makers at the SCI entity as well as for analyzing whether events qualify for reporting under paragraphs (b)(3)-(5).

E. REASONABLE POLICIES AND PROCEDURES SHOULD BE CONSISTENT WITH GENERALLY ACCEPTED TECHNOLOGY STANDARDS

Proposed Rule 1000(b)(1)(ii) provides that an SCI entity's policies and procedures would be deemed reasonably designed and thus satisfy the requirements of Proposed Rule 1000(b)(1) if they are consistent with current SCI industry standards. Rule 1000(b)(1)(ii) further states that such SCI industry standards shall be: (A) comprised of information technology practices that are widely available for free to information technology professionals in the financial sector; and (B) issued by an authoritative body that is a U.S. governmental entity or agency, an association of U.S. governmental entities or agencies, or a widely recognized organization. Examples of such SCI industry standards are set forth in Table A in the Proposing Release. Compliance with SCI industry standards would not be the exclusive means for complying with paragraph (b)(1). As discussed below, the Exchanges do not believe that the proposal will provide useful guidance for complying with Proposed Rule 1000(b)(1). Therefore, the Exchanges recommend replacing the reference to "current SCI industry standards" with the phrase "generally accepted technology principles," and deleting paragraphs (A) and (B) of Proposed Rule 1000(b)(1)(ii) as well as Table A from the Proposing Release.

As a practical matter, the Exchanges believe that it is unlikely that SCI entities will comply with all aspects of any particular standard in Table A at any particular time, thereby obviating its usefulness in Proposed Reg SCI. SCI entities, like participants in any industry that relies heavily on technology, commonly review a variety of different standards for frameworks or best practices, and then adopt a derivative of multiple standards, customizing them for the systems at issue. In addition, any reasonable policies and procedures in this area need to be forward-looking, and sufficiently nimble to respond dynamically to changes and threats as they arise. In contrast, by their very nature, standards documents are not forward-looking. Moreover, the SEC's process for updating Table A may add further time lags to the process. Therefore, it is likely that policies and procedures employed by the SCI entities would be more advanced or contain a mixture of different measures than the standards in place at any particular time.

Moreover, the Exchanges are concerned that the reference to SCI industry standards in Proposed Reg SCI paired with the list of standards in Table A in the Proposing Release will create a checklist approach to compliance with the reasonable policies and procedures requirement, notwithstanding the fact that compliance with SCI industry standards is not intended to be the exclusive means for complying with this provision. In other words, the Exchanges fear that the SCI entities will be held to the standards listed in Table A, either by

complying with them or by virtue of the unreasonably high burden likely to be associated with explaining why their practices vary from them, even if the SCI entity has adopted alternative reasonable policies and procedures. Additionally, SCI entities may defer adopting best-in-class standards for fear that they will not be viewed as compliant with Proposed Reg SCI, which could be to the detriment of the market and investors.

Therefore, to ensure that SCI entities have sufficient flexibility in crafting appropriate policies and procedures for the nature, size, technology, business model and other aspects of their business, the Exchanges believe that Proposed Rule 1000(b)(1)(ii) should refer to "generally accepted technology principles" instead of "SCI industry standards." Such an approach will ensure flexibility in devising policies and procedures without compromising their effectiveness.

F. THE COMMISSION NOTIFICATION REQUIREMENT SHOULD BE NARROWLY FOCUSED TO FOSTER THE GOAL OF TRANSPARENCY

The Exchanges have concerns that the Commission notification requirement as set forth in Proposed Rule 1000(b)(4) goes beyond the SEC's authority as a legal matter and would impose excessive costs on SCI entities without concomitant benefits as a practical matter. Therefore, the Exchanges strongly recommend significant amendments to this provision, as detailed below.

1. INSUFFICIENT EXPLANATION OF THE PURPOSE OF IMMEDIATE NOTIFICATION

The Exchanges believe that the SEC has not provided an adequate basis and purpose for the Commission notification requirement.[30] In proposing the Commission notification requirement, the SEC states the following rationale for the rule:

> The Commission preliminarily believes that the proposed notification requirement for immediate notification SCI events, the proposed 24-hour time frame for submission of written notices, and the proposed continuing update requirement, are appropriately tailored to help the Commission and its staff quickly assess the nature and scope of an SCI event, and help the SCI entity identify the appropriate response to the SCI event, including ways to mitigate the impact of the SCI event on investors and promote the maintenance of fair and orderly markets.[31]

---

[30] Section 553(c) of the Administrative Procedures Act ("APA") requires that the SEC incorporate in the rules adopted a concise general statement of their basis and purpose. To satisfy this requirement, a statement should indicate the major issues of policy relevant to the proposal and explain why the SEC decided to respond to these issues as it did. The Exchanges believe that the SEC's stated reasons for proposing paragraph (b)(4) are insufficient to satisfy the requirements of the APA.

[31] Proposing Release at 18119.

The Exchanges believe that this rationale only supports real-time reporting for those very limited circumstances in which the SEC's immediate participation would be valuable in addressing or resolving an event with significant market-wide impact. In particular, the SEC should only require immediate reporting when the SEC's involvement is necessary to provide, for example, a rule interpretation, engage in information sharing with Congress or others at a higher level, orchestrate collaborations among self-regulatory organizations or other regulators (*e.g.*, CFTC), or otherwise address a regional or national crisis. By contrast, the SEC's rationale fails to support immediate reporting and updating requirements, in significant detail on Form SCI, for the vast majority of SCI events (as defined in the proposal). In these other situations, the SEC staff will have no involvement at all during the course of the event other than to gather data. The reported information will simply be recorded, and the SEC may determine to analyze the information at a later date to assist in the general regulation and oversight of SCI entities.[32] Moreover, until the SEC determines that Form SCI is the exclusive means for reporting and that the ARP staff will be the sole point of contact for these events, the Exchanges remain concerned that they will be required to report multiple times to different SEC staff for ostensibly the same reasons – in a manner that will constrain the very Exchange resources needed to address the market disruptions quickly. Therefore, the Exchanges recommend that the notification requirements set forth in paragraph (b)(4) be limited to those circumstances which require the SEC's immediate involvement.

2. INAPPROPRIATE MANAGERIAL/SUPERVISORY ROLE OF SEC STAFF

The Exchanges also believe that the detailed reporting requirements set forth in paragraph (b)(4) of Proposed Reg SCI confuse the roles of the SEC and the SCI entities. The breadth of the SCI events covered, the details requested of the events, and the timeframes for providing a response are more appropriate for reports to a manager or supervisor at the SCI entity tasked with fixing a technical issue than for a prudential regulator. Indeed, the SEC's description of how it would use this information reinforces this concern. The SEC notes that the reports would make sure that the Commission and its staff are "kept apprised of such SCI events, including their causes and their effect on the markets," and are "aware of the steps and resources necessary to correct such SCI events." As discussed above, this may be appropriate in certain limited severe cases, but, in all other cases, the SEC would be imposing costly regulatory notification obligations with no corresponding governmental benefits. The SEC must articulate concrete and specific governmental purposes for collecting the information and the beneficial uses of having the information to meet the Commission's obligation to only promulgate regulations with benefits that outweigh their costs.

---

[32] For example, an SCI entity would be required to notify the SEC in the middle of the night if a relevant SCI event developed at that time. Such a requirement would appear to serve no useful purpose (unless the SEC plans to staff a desk 24 x 7 to receive and respond to such notices).

3. OVERLY BROAD APPLICATION

The Exchanges believe that the Commission notification requirement, as currently drafted, applies to an overly broad and ill-defined category of events. As discussed above, the Exchanges believe that any immediate reporting requirement should only apply to certain significant events.

If the SEC were to continue to apply this provision to SCI events more generally, however, the Exchanges would recommend that the scope of SCI events be limited as described above in Section IV(C). Specifically, the definitions of systems disruptions and intrusions should be redefined for better clarity and focus. In addition, the Exchanges believe that the notification requirement should not extend to systems compliance issues. The reporting should be limited to factual descriptions of systems disruptions or intrusions, not conclusions regarding legal obligations. Moreover, given the expedited timing for the reporting, the focus should be on identifying and correcting systems issues, not necessarily legal ramifications. Finally, no SCI events should be included that do not satisfy a materiality threshold. Clearly, an SCI entity should not be burdened with reporting insignificant events.

4. IMPRACTICAL REPORTING TIMEFRAMES

The proposed 24-hour time limit for the written notice is not practical. Rule 1000(b)(4)(ii) requires an SCI entity to provide written notification regarding any SCI event within 24 hours. Pursuant to Rule 1000(b)(4)(iv)(A)(1), such notification must include:

> All pertinent information known about an SCI event, including: a detailed description of the SCI event; the SCI entity's current assessment of the types and number of market participants potentially affected by the SCI event on the market; and the SCI entity's current assessment of the SCI event, including a discussion of the determination of whether SCI event is a dissemination SCI event or not.

In addition, to the extent available as of the time of notification, the notification (or an update thereto) must include:

> [a] description of the steps the SCI entity is taking, or plans to take, with respect to the SCI event; the time the SCI event was resolved or timeframe within which the SCI event is expected to be resolved; a description of the SCI entity's rule(s) and/or governing documents, as applicable, that relate to the SCI event; and an analysis of parties that may have experienced a loss, whether monetary or otherwise due to the SCI event, the number of such parties, and an estimate of the aggregate amount of such loss.[33]

---

[33] Rule 1000(b)(4)(iv)(A)(2) of Proposed Reg SCI.

Collecting, summarizing, reviewing and approving for submission to the SEC, such detailed, extensive information about an event cannot be appropriately completed in that time frame. At best, a generalized summary of the event may possibly be produced within 24-hours, and we note that such a summary, however, may be incorrect or incomplete, as diagnosing a system issue can be difficult and time-consuming.

To further illustrate this point, we cite the Commission's own cost analysis for reporting under Rule 1000(b)(4)(ii), which includes 10 burden hours for a Compliance Manager and 10 burden hours for an attorney to report each incident. Therefore, each event gives rise to 20 burden hours within 24 hours. Further, no estimate is provided for a technology staff member that would likely be involved in completing Form SCI.

Moreover, Rule 1000(b)(4)(iii) requires an SCI entity to provide updates "at such frequency as reasonably requested by a representative of the Commission." Such a requirement imposes an open-ended obligation on SCI entities to respond to update requests from any SEC representative. At a minimum, the rule must specify the requisite level of seniority the SEC representative must have (*e.g.*, an Associate Director level or higher).

Further, the SEC underestimates the number of updates that will be required. The Commission estimates that for the total of 65 SCI events reportable per year per entity, only five will require such an update under Rule 1000(b)(4)(iii). This suggests that for 60 events, the Commission believes that entities can take corrective action, determine root cause, promulgate a fix, evaluate all affected parties, disseminate notices, prepare Form SCI and do all of this with complete accuracy – within 24 hours. The Commission estimates for the purpose of its cost analysis that in over 90% of SCI events, all required activity is complete and reportable on Form SCI within 24 hours. At best, this is not realistic. At worst, the cost analysis is seriously compromised and underestimates the true cost of reporting. As stated above, we recommend that the Commission reevaluate its estimates and the cost burden for these provisions.

5. PRESERVING CONFIDENTIALITY

Given the confidential nature of the information provided to the SEC pursuant to this requirement, including confidential business, regulatory and security information, Proposed Reg SCI should explicitly state that information will not be made public and will not be available in response to FOIA requests.[34] Moreover, the SEC must provide assurances that sensitive information will be properly safeguarded by the SEC and its agents. There is little point to requiring measures to protect system security at SCI entities if the confidential information is not subject to similar stringent protection when provided to the SEC. Indeed, recent high

[34] The Exchanges support the SEC's statement that information submitted pursuant to Proposed Reg SCI would be kept confidential, subject to provisions of applicable law. Proposing Release at 18155.

profile security lapses at the SEC and other government agencies emphasize that this is not an idle concern.[35]

6. ALTERNATIVE REPORTING PARADIGM: GAR SYSTEM

In light of the concerns with the reporting requirements set forth in paragraph (b)(4) of Proposed Reg SCI, the Exchanges recommend that the SEC consider an alternative reporting paradigm, called the Green, Amber, Red or "GAR" system, which would match the severity of an SCI event to the type of reporting required – the more significant the event, the greater the reporting obligations. The Exchanges believe that such a system would maximize the benefits of reporting while minimizing the costs.

Under the GAR system, each SCI event would be classified in one of three tiers – a Green, Amber or Red event. The first tier – Green events – covers minor events, including situations in which failovers worked as designed, events that have little or no impact on the SCI entities' operations or the markets, and systems issues that require minor patches to correct an error. SCI entities would not be required to notify the SEC regarding Green events. The SCI entity instead would record information about the event in its records, which would be available for inspection.

The second tier, the Amber events, would apply to events with medium impact, including events in which failovers do not operate as designed, there is some impact on market participants and/or the market, self-help is declared for more than ten minutes, events requiring a shut-down of routing/reporting, and public notice is required, other than to a few limited market participants. SCI entities would be required to describe Amber events on a short form version of Form SCI on a semi-annual basis. In addition, the SCI entity would be required to maintain policies and procedures to review such events for compliance issues.

Finally, the Red tier would cover events that have a significant impact on market participants and/or the market. These events would include severe market breakdown, newsworthy events, events with major market impact, and events posing significant financial risk. In all such cases, the SEC's involvement would be necessary. For Red events, SCI entities would be required to provide immediate notice to the SEC, first orally, and then followed by written notice. Within a week, the SCI entity must submit a written report on Form SCI describing the event. The SCI entity would be required to provide updates on Form SCI as events warrant. In addition, the SCI entity would be required to perform an internal compliance/surveillance review of the incident for any compliance issues.

---

[35] *See, e.g.,* Robert Schmidt, *SEC pays $580K to Settle Whistleblower Claims by Ex-Employee*, BLOOMBERG (June 10, 2013), http://www.bloomberg.com/news/2013-06-10/sec-pays-580-000-over-ex-investigator-s-firing-claims.html; Siobhan Gorman & Dion Nissenbaum, *U.S. Relies on Spies for Hire to Sift Deluge of Intelligence*, WALL ST. JOURNAL (June 11, 2013), http://online.wsj.com/article/SB10001424127887324904004578537813599741012.html ; Sarah N. Lynch, *NYSE Hires Ex-Homeland Security Chief After SEC Security Lapse*, REUTERS (Nov. 16, 2012), http://www.reuters.com/article/2012/11/16/sec-cyber-nyse-idUSL1E8MG95K20121116.

G. THE REQUIREMENT TO NOTIFY THE SEC OF MATERIAL SYSTEMS CHANGES SHOULD BE REVISED TO MAXIMIZE ITS BENEFITS WHILE MINIMIZING COSTS

The requirement for SCI entities to give prior notice to the SEC of material systems changes, as set forth in Proposed Rule 1000(b)(6), should be amended to maximize the regulatory benefits while minimizing the cost to SCI entities. The SEC should focus the notice requirement on major systems changes by providing clear and objective guidance regarding the definition of "material" as used in the definition of "material systems change." The current formulation runs the risk of being significantly over-inclusive. In addition, Proposed Reg SCI should require periodic reporting – not prior reporting – of this more limited subset of systems changes. In addition, SCI SROs should not be required to provide notice of systems changes that are otherwise covered by the rule filing requirements of Rule 19b-4. Without these changes, the cost of the notification requirement will place too great a burden on SCI entities.

1. COVERED SYSTEMS CHANGES

The proposed requirement that an SCI entity report all "material system changes," as defined in Rule 1000(a), could be interpreted to encompass too broad a selection of system changes. A "material systems change" is defined to include

> 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 systems.

The reliance on the term "material" throughout this definition raises significant interpretive issues for SCI entities. If "material" were interpreted broadly to cover any functional change to an SCI system, the number of material systems changes could measure in the thousands. In contrast, if "material" were interpreted to mean major or fundamental systems changes, the number of material systems changes would be more manageable for reporting purposes. Therefore, the Exchanges believe that the SEC must provide very specific guidance for drawing the line between material and non-material systems changes, and must draw that line to cover relatively few changes.

In that regard, the Exchanges do not believe that the reporting provisions in the ARP program related to systems changes shed additional light on this provision of Proposed Reg SCI. First, the ARP program uses different terms in describing the type of systems changes that should be reported. The ARP program requires notification of <u>significant</u> systems changes, not

just material systems changes; the two terms could have different meanings. Moreover, some of the examples of "significant systems changes" in the 2001 ARP Interpretive Letter focus on "major" changes (*e.g.*, major system architecture changes or changes that could increase susceptibility to major outages), which would appear to be a more limited subset than material changes contemplated under Proposed Reg SCI. Therefore, ARP's significant systems changes may be included within the definition of a "material systems change," but it is not at all clear that they are coterminous. Second, because the ARP program is voluntary, ARP participants are permitted some leeway in how they interpret the reporting requirements. Unlike the ARP program, Proposed Reg SCI would impose definitive regulatory requirements on SCI entities that raise more significant interpretive as well as enforcement risks.

The Exchanges recognize that the notification requirement is similar to the material systems change requirement in Regulation ATS. The SEC provided some limited guidance as to the meaning of a material systems change in that context. It is our understanding, however, that interpretive issues regularly arise with that phrase, and that interpretations are likely to vary across ATSs. Therefore, the Exchanges do not believe that this limited guidance is sufficient to address the many interpretive questions likely to be raised by any particular systems change under Proposed Reg SCI.[36]

Second, as discussed above in Section IV(B)(2), the notification requirement with regard to "SCI security systems of an SCI entity that materially affects the existing security of such systems" should be deleted from this requirement. The reporting requirement should focus solely on SCI systems.

In sum, the Exchanges believe that a "material systems change" should be limited to major or fundamental systems changes. It should not apply to routine modifications that do not fundamentally affect the operations of systems with regard to order execution, order routing, clearance and settlement, or the transmission of required market data.

2. PERIODIC REPORTING

The proposed requirement to notify the SEC in advance of the implementation of material systems changes should be replaced with a periodic updating requirement. Such a requirement would better match the system change practices of SCI entities as well as the regulatory needs of the SEC.

The proposed 30-day prior notice of material systems changes will interfere with SCI entities' flexibility in planning and implementing systems changes, and may discourage or

---

[36] In adopting Regulation ATS, the SEC noted that "material changes" to an alternative trading system include any change to the operating platform, the types of securities traded or the types of subscribers. However, the SEC also indicated that this list was not conclusive, noting that alternative trading systems implicitly make materiality decisions in determining when to notify subscribers of changes. Securities Exchange Act Rel. No. 40760 (Dec. 8, 1998), 63 Fed. Reg. 70844, 70864 (Dec. 22, 1998).

unduly delay such changes to the detriment of the markets. Indeed, coding and systems changes can occur on a weekly, if not daily, basis at an exchange.

In keeping with the proposal to replace prior notice with periodic reporting, the Exchanges also believe that the requirement to provide updates regarding any material inaccuracies in prior notifications pursuant to Rule 1000(b)(6)(ii) should be eliminated. This provision requires SCI entities to notify the Commission, either orally or in writing, with any oral notification to be memorialized within 24 hours after such oral notification by a written notification, as early as reasonably practicable. Such updates, particularly with such abbreviated reporting timeframes, are unduly burdensome, without providing a commensurate benefit. Again, periodic reporting of any inaccuracies is sufficient for oversight purposes

Moreover, the Exchanges believe that the SEC has failed to provide an adequate explanation of the basis and purpose for the 30 days prior notice requirement.[37] It is unclear how the SEC will use this prior notification, especially since the provision does not require SEC approval for the technology changes. The SEC only states that the 30 days is necessary to "provide sufficient time for Commission staff to understand the impact of the systems change" and "that this amount of advance notice typically is needed to allow Commission staff to effectively monitor technology developments associated with a planned material systems change."[38] It does not explain the purpose or value of such a monitoring function or why it would require such a lengthy lead time. Indeed, it is unclear why this notice is necessary at all if the systems change is subject to the rule filing requirements under Rule 19b-4, as it will be in many cases.

H. THE DISSEMINATION OF INFORMATION SHOULD ENHANCE INVESTOR PROTECTION

The Exchanges believe that public dissemination of information should be required for investor protection purposes only. Specifically, SCI entities should disseminate information of SCI events that would result in significant harm or loss to those members or participants who are likely to be affected by the event. Therefore, the public dissemination provision of Proposed Reg SCI should be amended as discussed below.

1. DISSEMINATION SCI EVENTS

The Exchanges believe that the scope of the term "dissemination SCI events" is too broad. The focus of the dissemination requirement, instead, should be on providing relevant information to persons who are reasonably likely to be affected by a significant systems issue. Therefore, only systems issues that an SCI entity reasonably estimates would result in significant harm or loss to market participants should be subject to the dissemination requirement. Correspondingly, systems compliance issues should not be subject to public

---

[37] *See* Section 553 of the APA.

[38] Proposing Release at 18122.

disclosure. Such disclosure may not only provide market participants with information for circumventing regulatory surveillance, but it may also subject the SCI entity to significant litigation risks from investors and other legal risks. In addition, the Exchanges strongly recommend against disseminating information about system intrusions. Such reporting could interfere with the SCI entity's ability to investigate, or recover from, the intrusion, and potentially have an adverse effect on the security of the SCI entity (*e.g.,* copycat attacks). Finally, information about disruptions related to regulatory or surveillance systems should not be disseminated, as such disclosure may encourage prohibited activity on the market.

2. SCOPE OF DISSEMINATED INFORMATION

Furthermore, the Exchanges believe that the scope of the information required to be provided is too extensive, particularly given the timing requirements of Rule 1000(b)(5). For example, paragraph (5)(i)(A) requires prompt dissemination of information about the SCI event, including the systems affected by the SCI event, and a summary description of the SCI event. The SEC explains that such a summary should communicate the timing, nature (*e.g*., which systems were affected, the magnitude of the issue, rules that related most directly to the issue) and foreseeable consequences of a systems problem. Gathering, analyzing and submitting such information in such a short time frame is likely to lead to the dissemination of inaccurate information that will only exacerbate market confusion. Any immediate dissemination of information about a systems issue should merely communicate the basic fact that there is a systems issue. Additional information should then be provided to participants "when known."

I. THE SAFE HARBOR SHOULD BE MORE ROBUST TO PROVIDE THE INTENDED PROTECTION

The Exchanges strongly agree with the need for a safe harbor in light of the breadth and complexity of the requirements of Proposed Reg SCI, and the reality that systems issues will occur despite best efforts to the contrary. The Exchanges believe, however, that the proposed safe harbor, as set forth in Rule 1000(b)(2)(ii) and (iii), is not sufficiently robust to provide the intended protection for SCI entities and their employees. In particular, the requirements of the safe harbor are not sufficiently clear and objective to provide an SCI entity reliable guidance as to how to comply with the safe harbor. As a result, the Exchanges recommend replacing the proposed safe harbor with an objective provision that would protect SCI entities from enforcement actions by the SEC except in cases of intentional or reckless non-compliance or a pattern of non-compliance with Reg SCI ("Objective Safe Harbor Alternative"). Employees of SCI entities similarly should receive the benefit of the Objective Safe Harbor Alternative if they have not intentionally or recklessly failed to discharge their duties and obligations under the policies and procedures of the SCI entity. Such a robust safe harbor should be preferable if the intent of the Proposed Reg SCI is to ensure appropriate systems processes are in place, not to create unnecessary enforcement liabilities. Moreover, as discussed in detail below, the Objective Safe Harbor Alternative would improve upon the SEC's proposed safe harbor in a variety of ways.

1. THE SAFE HARBOR UNDER PROPOSED REG SCI

The Exchanges believe that the proposed safe harbor, as set forth in Rule 1000(b)(2)(ii) and (iii), relies upon vague and extensive requirements that are overly subjective. As a result, the provision raises the risk that compliance with the safe harbor may never be attained. Specifically, the crux of the safe harbor is that the SCI entity followed reasonable policies and procedures. However, since all SCI entities will inevitably experience a systems issue, does the occurrence of such a systems issue in and of itself mean that the SCI entity either did not have reasonable policies and procedures or did not follow them? At a minimum, the SEC is likely to review an SCI entity's interpretation of the safe harbor in the event of a systems issue with the benefit of 20/20 hindsight. This is particularly true for high profile instances that occur despite reasonable efforts taken to comply with the safe harbor. The Exchanges are concerned that the SEC will take this position even further, concluding that the occurrence of a significant systems event means that an exchange did not have reasonable policies and procedures and is therefore outside the terms of the proposed safe harbor.

The proposed safe harbor contains numerous terms that may be subject to widely differing interpretations for any particular system or systems issue. Moreover, given the myriad types of systems at issue, the Exchanges do not believe that the SEC can or will provide adequate guidance as to how to comply with the proposed safe harbor. Therefore, each SCI entity will be left to interpret the provisions on a case-by-case basis.

For example, as a threshold matter, the proposed safe harbor requires "policies and procedures reasonably designed" to provide for the various factors in the provision. The SEC provides almost no guidance in the Proposing Release as to how to interpret this phrase. Nor have the courts provided much guidance on interpreting this phrase. Similarly, with respect to Rule 1000(b)(2)(ii)(A)(1) and (2), which require testing of SCI systems and changes thereto prior to and after implementation, the frequency and type of testing for each relevant system that would satisfy the safe harbor is open to interpretation. Correspondingly, with respect to Proposed Rule 1000(b)(2)(ii)(A)(3), which would include in the safe harbor a requirement that an SCI entity establish and maintain written policies and procedures that provide for a system of internal controls over changes to SCI systems, it is unclear what minimum standards for the internal controls would satisfy this requirement. Similarly, these interpretive issues extend to the required "ongoing monitoring," "assessments," and "reviews" required in paragraphs (4), (5) and (6) of the proposed safe harbor as well. Moreover, the proposed safe harbor does not address how a systems issue or systems compliance issue impacts the applicability of the safe harbor.

2. THE OBJECTIVE SAFE HARBOR ALTERNATIVE

In light of these concerns, the Exchanges recommend that the SEC delete paragraphs (b)(2)(ii) and (iii) of Proposed Reg SCI – the proposed safe harbor, and add a new paragraph (g) to Proposed Reg SCI, which would state the following:

(g) Safe Harbor from Certain Penalties.

(1) It shall be deemed a violation of Reg SCI for all purposes under the Securities Exchange Act if an SCI entity:

(A) Fails to implement reasonable corrective action in response to a written communication from the SEC regarding Reg SCI;
(B) Engages in a continuing pattern of violations of Reg SCI; or
(C) Engages in any intentional or reckless violation of Reg SCI.

(2) It shall be deemed a violation of Reg SCI for all purposes under the Securities Exchange Act if a person employed by an SCI entity intentionally or recklessly fails to discharge his or her duties and obligations under the policies and procedures of the SCI entity.

(3) For all violations of Reg SCI other than those set forth in paragraph (1) by an SCI entity, or (2) by an employee of an SCI entity, the SEC is solely authorized to serve a warning notice and/or letter of correction on such SCI entity or employee with regard to the violation, provided that the SCI entity has self-reported such violation to the SEC in a timely manner.

The Objective Safe Harbor Alternative would provide SCI entities with clear and objective standards for qualifying for the safe harbor. An SCI entity would be protected from enforcement liability unless it failed to self-report and/or failed to take corrective action, engaged in a continuing pattern of violations, or engaged in intentional or reckless violations of Reg SCI. Employees of an SCI entity charged with implementing Reg SCI – with all of its complexity and the acknowledged expectation that SCI entities will experience ongoing technology issues after adoption of the rule – would not be subject to liability based on a hindsight review unless they were reckless or engaged in intentional misconduct in performing their duties.

The Objective Safe Harbor Alternative also would provide protection from enforcement under all of Proposed Reg SCI. In contrast, the SEC's proposed safe harbor would apply only to the requirements set forth in Rule 1000(b)(2)(i) – that is, the requirement for SCI entities to establish, maintain and enforce written policies and procedures reasonably designed to ensure that its SCI systems operate in the manner intended. The SEC explained that it proposed the safe harbor for the following reason:

> Because of the complexity of SCI systems and the breadth of the federal securities laws and rules and regulations thereunder and the SCI entities' rules and governing documents, the Commission preliminary believes that it would be appropriate to provide an explicit safe harbor for SCI entities and their employees to provide greater clarity as to how they can ensure that their conduct will comply with this provision.[39]

The Exchanges believe that, under this same reasoning, the safe harbor also should apply to any potential liability under other provisions of Proposed Reg SCI, not just the policies and procedures requirements of Rule 1000(b)(2)(i). These other provisions are no less complex or extensive or subject to interpretation than paragraph (b)(2)(i). Similarly, the SEC should consider whether the safe harbor should also apply to any other potential liability of an SCI entity under other provisions of the Exchange Act that are based on the facts related to the SCI event.

While we recognize the importance of the SEC being able to take enforcement action in situations where there is an egregious failure to comply with Proposed Reg SCI, it is equally important that Proposed Reg SCI is structured to recognize that errors will inevitably occur when complex technology is involved, and that SCI entities and their staff can manage these situations responsibly, engage in constructive and collaborative dialogue with SEC staff regarding such errors, and not be subject to unnecessary second-guessing and potential liability for such matters. The public policy purposes underlying Proposed Reg SCI will not be adequately served if SCI entities and their staff are not able to operate within an objective and transparent safe harbor. We do not believe that the SEC's proposed safe harbor will address this concern.

The Objective Safe Harbor Alternative also would change the focus of Proposed Reg SCI from enforcement to compliance. It would explicitly recognize that the purpose of this regulation is to have complex systems managed as well as reasonably possible, with the recognition that problems will occur despite best efforts. Such an approach would serve to codify, with regard to Proposed Reg SCI, the SEC's practice in other contexts of not pursuing enforcement actions against firms that establish, maintain, and enforce compliance policies and procedures or otherwise act in good faith, notwithstanding a violation of a relevant regulation.[40] In doing so, it would ensure that the safe harbor is used as a shield not a sword.[41]

---

[39] *Id*. at 18115.

[40] The SEC has acknowledged such a practice in other contexts, such as Regulation NMS, Regulation FD and the Foreign Corrupt Practices Act. *See, e.g*., Securities Exchange Act Rel. No. 51808 (June 9, 2005), 70 Fed. Reg. 37496 (June 29, 2005); *SEC Files Settled Regulation FD Charges Against Former Chief Financial Officer*, Litigation Release No. 21222 (Sept. 24, 2009); *A Resource Guide to the U.S. Foreign Corrupt Practices Act,* The Criminal Division of the U.S. Department of Justice and the Enforcement Division of the U.S. Securities and Exchange Commission, at p. 56 (Nov. 14, 2012) http://www.justice.gov/iso/opa/resources/29520121114101438198031.pdf.

[41] If the SEC were to determine not to include the Objective Safe Harbor Alternative, the Exchanges nonetheless would urge the SEC to include language in any adopting release stating that the SEC will not pursue enforcement actions against SCI entities that establish, maintain, and enforce compliance policies and procedures or act in good faith, notwithstanding a violation of Reg SCI.

J. BUSINESS CONTINUITY AND DISASTER RECOVERY PLANS TESTING REQUIREMENTS

The Exchanges believe that it is of paramount importance for SCI entities to test the operation of their business continuity and disaster recovery plans. The Exchanges are concerned, however, that Proposed Rule 1000(b)(9) may lead to inconsistent testing requirements, confusion over coordinated testing, and unnecessary costs and other compliance burdens for the industry. Therefore, the Exchanges recommend that the SEC adopt specific rules governing which market participants are required to participate in testing, the frequency of testing and how testing should be coordinated across industry participants. Such a uniform SEC rule will ensure a consistent, effective approach to business continuity and disaster recovery plan testing.

Proposed Rule 1000(b)(9) requires that each SCI entity "designate those members or participants it deems necessary, for the maintenance of fair and orderly markets in the event of the activation of its business continuity and disaster recovery plans, to participate in the testing of such plans" and then requires "participation by designated members or participants in scheduled functional and performance testing of the operation of such plans." The Exchanges believe that placing the onus on SCI entities to designate the members or participants subject to the testing requirements will raise regulatory arbitrage and competitive concerns. In particular, such an open-ended regulatory requirement may cause a race to the bottom regarding how many and which members or participants are designated to participate in testing. Therefore, the Exchanges recommend replacing Rule 1000(b)(9) with a rule that sets forth which members or participants must participate in the testing. Specifically, the Exchanges believe that the SEC should require that all members or participants that represent a meaningful percentage of the volume in the marketplace participate in the testing. Such a requirement would capture the more significant market participants, while recognizing the financial burden such testing may pose for smaller players.

Similar issues are raised by the requirement in paragraph (i) of Rule 1000(b)(9), which requires each SCI entity to determine the manner and frequency of the testing. Therefore, instead of requiring each SCI entity to determine how frequent testing should be pursuant to its own rules, the Exchanges recommend that the SEC clearly set forth in the rule the frequency of the required tests (*e.g.*, one or two per year), and clarify that such tests should be a part of the coordinated industry-wide testing required under paragraph (ii). Moreover, the Exchanges recommend that the rule should require that such coordinated testing be performed pursuant to an SEC approved plan. In addition, any such rule should explicitly recognize that SCI entities have the right to maintain the confidentiality of certain critical information, such as information related to capacity, despite the requirement to test the functions related to that information.

K. DIRECT SEC STAFF ACCESS TO SYSTEMS OF SCI ENTITIES RAISES SECURITY ISSUES

Proposed Rule 1000(f) would require SCI entities to provide SEC representatives reasonable access to their SCI systems and SCI security systems to assess the SCI entity's compliance with Proposed Reg SCI. The SEC states that this provision is intended to be consistent with the Commission's authority under Section 17(b) with respect to access to records generally.[42] The Exchanges believe, however, that providing SEC representatives the ability to "directly access"[43] the systems of an SCI entity is very different than providing access to its records. Examinations performed pursuant to Section 17(b) must be reasonable; it does not authorize constant access.[44] Permitting an SEC representative, like any other person, to obtain direct access to an SCI entity's live systems to perform tests would create significant risks for the markets.[45] Therefore, to maintain the security and integrity of its systems, the Exchanges believe that this provision should be revised to require SCI entities to provide the SEC representatives with the configuration and information flows of the systems, instead of direct access. Providing this type of systems information, rather than actual access to the systems themselves, is consistent with current practice. In addition, the phrase "Commission representatives" is an undefined term that could be interpreted broadly to include not only the SEC and its staff, but others tasked with the review by the SEC that are not SEC employees. The Exchanges recommend replacing this phrase with a clearly defined category of persons employed by and authorized by the SEC to receive the information about SCI systems. Without such protective limitations, the proposed provision may undermine the very system security and integrity that Proposed Reg SCI is intended to address.

L. ANNUAL REVIEWS

Proposed Rule 1000(b)(7) would require an SCI entity to conduct an SCI review of the SCI entity's compliance with Regulation SCI not less than once each calendar year, and submit a report of the SCI review to senior management. The SEC proposes to define an "SCI review" in Proposed Rule 1000(a) as:

> A review following established procedures and standards, that is performed by objective personnel having appropriate experience in conducting review of SCI systems and SCI security systems, and which review contains: (1) a risk assessment with respect to such systems of an SCI entity; and (2) an assessment of internal control design and effectiveness to include logical and physical security controls, development processes,

---

[42] Proposing Release at 18130.

[43] *Id.* at 18169.

[44] Section 17(b) of the Exchange Act states that "[a]ll records of persons described in [Section 17(a)] are subject at any time, or from time to time, to such reasonable periodic, special, or other examinations by representatives of the Commission."

[45] For example, the Proposing Release states that "with access to an SCI entity's SCI systems and SCI security systems, Commission representatives could test an SCI entity's firewalls and vulnerability to intrusions." Proposing Release at 18130, n. 284.

and information technology governance; provided, however, that such review shall include penetration test reviews of the network, firewalls, development testing, and production systems at a frequency of not less than once every three years.

The Exchanges believe that any requirement for an annual review should incorporate a risk-based approach for determining the scope of the review. Without such an approach, the reviews will be unnecessarily broad and burdensome, and will focus on issues that do not raise the most risk to the entity.

V. CONCLUSION

The Exchanges strongly advocate using market technology in a responsible manner. The Exchanges agree with the SEC that it is critical that systems that are important to the markets have levels of capacity, integrity, resiliency, availability and security adequate to maintain their operational capability and promote the maintenance of fair and orderly markets, and operate in the manner intended. The Exchanges are concerned, however, that the significant costs and burdens of Proposed Reg SCI will operate to divert limited resources away from these goals. Therefore, the Exchanges strongly recommend a re-evaluation of the scope and purpose of each of the provisions of Proposed Reg SCI and a measured examination of the costs and benefits of each provision.

* * * * *

We appreciate the opportunity to provide our views on this proposal and look forward to discussing these issues with you further.

Sincerely,