sifma
Invested in America

July 8, 2013

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

Ms. Elizabeth M. Murphy
Secretary
U.S. Securities and Exchange Commission
100 F Street, N.E.
Washington, DC 20549-1090

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

Dear Ms. Murphy:

The Securities Industry and Financial Markets Association ("SIFMA")[1] appreciates the opportunity to provide the Securities and Exchange Commission ("Commission" or "SEC") with comments regarding proposed Regulation Systems Compliance and Integrity, also known as proposed "Regulation SCI."[2]

I. INTRODUCTION AND SUMMARY

SIFMA supports the proposed rule's policy goal of enhancing the Commission's oversight of the capacity, integrity, resiliency, availability and security of key automated systems of entities of particular importance to the national market system.[3] The pervasiveness of automation and the rapid pace of technological changes in our securities markets underscore the need to ensure appropriate oversight of such systems. Notably, the degree of automation and change also reinforce the reality that achieving effective regulatory oversight will require extensive and ongoing investments of time and money, both by industry participants and the Commission. Thus, it is critical that our collective efforts are focused on crafting a rule that not

---

1 The Securities Industry and Financial Markets Association (SIFMA) brings together the shared interests of hundreds of securities firms, banks and asset managers. SIFMA's mission is to support a strong financial industry, investor opportunity, capital formation, job creation and economic growth, while building trust and confidence in the financial markets. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA). For more information, visit http://www.sifma.org.

2 Securities Exchange Act Release No. 69077 (Mar. 8, 2013) 78 *Fed.Register* 18084 (Mar. 25, 2013) (Regulation Systems Compliance and Integrity) ("Proposing Release").

3 The Commission stated that the purpose of "proposed Regulation SCI is to enhance the Commission's regulatory supervision of SCI entities and thereby further the goals of the national market system by helping to ensure the capacity, integrity, resiliency, availability, and security, and enhance compliance with federal securities laws and regulations, of automated systems relating to the U.S. securities markets through the formalization of standards to which their automate systems would be held, and a regulatory framework for ensuring more effective Commission oversight of these system." *See* Proposing Release, 78 *Fed.Register* at 18092.

only enhances the Commission's oversight of these important systems but also does so in a manner that: (1) is cost effective; (2) applies resources to those systems that are most critical; (3) is flexible enough to permit technological innovation to keep up with the needs of market participants in a timely manner; and (4) is appropriately tailored to enable effective compliance.

SIFMA believes that proposed Regulation SCI ("Reg. SCI") should focus on the resiliency of our markets as a whole, and take into account the relative degrees of risk to the markets posed (i) by various functions performed by "SCI entities," and (ii) enabled by "SCI systems" under the proposed rule. Correspondingly, the SEC should calibrate the attendant obligations under the proposed rule based on these risk profiles. As discussed herein, certain participants, the functions they perform, and the systems they use to perform those functions, are more critical to the effective operation of the markets than are others, and some SCI events similarly are of more urgency than others. The "one-size-fits-all" approach of the proposed rule with respect to the definitions and obligations of SCI entities does not recognize these facts. Similarly, SCI systems should be categorized so that those systems that are more critical to the markets – from an outage impact and timeliness perspective – are afforded more focus under the rule than other important, but less critical systems. SIFMA believes strongly that the implementation of Reg. SCI with this tailored approach would enhance the resiliency and viability of the market as a whole, without unduly focusing on a single component of the market or creating unnecessary costs and burdens.

SIFMA appreciates the opportunity to provide comments on the proposal, which are set forth in detail below. Overall, SIFMA offers the following comments:

- SIFMA believes that tailoring obligations based on the criticality of the entity and its systems would enhance greatly the effectiveness of the proposal. Specifically, the requirements for policies and procedures, notification of events to Commission staff, advance notification of systems changes, and annual review of systems would all benefit from a tiering of those obligations.

- We also believe the Commission may achieve the goal of ensuring the security of SCI systems in a more straightforward and simplified manner by eliminating the definition of an "SCI security system" and its related requirements, in favor of a more general requirement related to the security of SCI systems.

- SIFMA believes that the requirement to provide the Commission advance notification of material changes to SCI systems is overly broad. As currently proposed this requirement could result in a significant number of filings by any given SCI entity, which would result in substantial costs, and inhibit an SCI entity's ability to implement changes to their systems in a timely manner.

- Importantly, moving to a mandatory, detailed and prescriptive regulatory approach to systems oversight requires an appreciation by the Commission that, despite their best efforts, SCI entities *will* experience systems problems on

occasion, and that will be the case even if Reg. SCI is adopted. The Commission should make clear that SCI entities will not be punished simply for experiencing a systems issue. Specifically, SIFMA proposes that the Commission include language in any adopting release for Reg. SCI clearly indicating that the focus of the rule will be on the reasonableness and application of an SCI entity's policies and procedures.

- In response to the Commission's request for comments, SIFMA does not support the expansion of proposed Reg. SCI to all broker-dealers. In many cases, broker-dealers generally perform functions that do not have any systemic impact on the operation of the national market system. In addition, broker-dealers already are subject to numerous regulations requiring the establishment of controls, including the Commission's Market Access Rule.[4]

- With respect to the obligations of the proposed rule, we have specific concerns about the systems access provisions, and the corrective action, dissemination of information to members or participants, and BCP testing requirements.

    - For example, the proposal that SCI entities provide Commission representatives direct onsite or remote access to SCI systems is fraught with security risks and possible unanticipated market impacts without any demonstrable indication that the information accessed – which will be complex and likely will vary substantially by firm – will be digestible and useful to the Commission and its staff.

    - Similarly, the requirement that corrective action be taken by any SCI personnel upon becoming aware of an SCI event fails to recognize the complexity of analyzing and determining an appropriate course of action in the midst of an SCI event. It also risks subverting the internal escalation policies and procedures of SCI entities.

    - The proposed business continuity and disaster recovery plan testing for SCI entities and their members/participants presents significant technological and logistical challenges. More broadly, as demonstrated during Superstorm Sandy in October 2012, determining whether and how the markets should respond during a disaster may, from time-to-time, involve important considerations related to employee safety and other factors.

- Finally, SIFMA believes the costs of the proposed rule are difficult to quantify given the vagueness of various provisions of the proposed rule. We are concerned that such costs are very likely to be significantly understated. Our analysis is

[4] *See e.g.,* Rule 15c3-5 under the Securities Exchange Act of 1934 ("Exchange Act").

currently ongoing and we plan to provide the Commission with additional comments about the estimated costs once the analysis is completed.

Each of these and other comments related to the Proposed Rule are discussed below.

II. SCI ENTITIES

A. *One-Size-Fits-All Approach Should Be Changed to a Risk-Based Tiered Approach*

Proposed Reg. SCI defines a universe of SCI entities and would impose mandatory uniform requirements on all such entities.[5] While, subject to its comments on SCI ATSs below, SIFMA agrees with the scope of SCI entities, we strongly believe that Reg. SCI should not adopt a one-size-fits all approach in terms of the obligations imposed on SCI entities. Instead, Reg. SCI should reflect the Commission's recognition that SCI entities play different roles with respect to the national market system. For example, a disruption to a primary listing exchange, a market data distributor, or a clearing agency will have a greater impact on the market as a whole, rather than a disruption to a single SCI ATS or non-primary exchange.

Instead of imposing uniform obligations on all SCI entities, the SEC should adopt a risk-based approach that takes into account the criticality of the functions performed by an SCI entity to the maintenance of fair and orderly markets. The criticality of the function that the SCI entity performs would provide the basis for a tiering of obligations under the rule. Under this approach, "criticality" would vary based on the function performed by an SCI entity and the footprint of that entity on the market (e.g., the number of entities and/or market participants affected). Using a tiered structure that takes into account the criticality of functions performed by SCI entities, the Commission may more effectively tailor the associated responsibilities under the rule.

The performance of functions essential to ensuring that the NMS markets operate effectively on a continuous basis should be considered highly critical, such that a disruption to the performance of such a function would be expected to cause a serious impact to the market. Multiple functions performed by SCI entities should be distinguished based on time sensitivity. Time sensitivity would depend on whether a disruption to the function would impact the market in real-time or whether the outage could exist for a certain duration before its impact was felt. Notification and remediation requirements under Reg. SCI should be tailored to the time sensitivity of each of the functions performed, not applied uniformly across all activities of an SCI entity. Highly critical functions would include the primary listing exchanges, trading of securities on an exclusive basis, securities information processors, clearance and settlement agencies, distribution of unique post-trade transparency information, and real-time market surveillance.

---

[5] "Proposed Regulation SCI would provide mandatory uniform requirements for ''SCI entities." *See* Proposing Release 78 *Fed.Register* at 18092. Proposed regulation defines an "SCI entity" as an "SCI self-regulatory organization, SCI alternative trading system, plan processor, or exempt clearing agency subject to ARP." *See* proposed Rule 1000(a)(78).

Medium criticality functions are important to the national market system; however, a systems issue for any of them may not require the same level of timely resolution as a high criticality function for the markets to continue to operate effectively. Medium criticality functions would include providers to the consolidated quote stream, non real-time surveillance, and outbound routers operating as facilities of self-regulatory organizations ("SROs"). "Lower criticality" SCI entities would include the remaining participants included as SCI entities in the original proposal, such as broker crossing networks.

This risk-based approach to classifying the functions performed by SCI entities and correlating the related requirements under Reg. SCI would be a change in structure from the SEC's proposed rule. However, SIFMA believes this approach is consistent with Reg. SCI's purpose of ensuring the resiliency of the national market system and, importantly, the Commission's mission to maintain fair, orderly, and efficient markets, and facilitate capital formation. Focusing on the key responsibilities of SCI entities based on the criticality of functions they perform will ensure that the markets are resilient under stress, without unduly burdening entities by applying the proposed requirements of Reg SCI to systems that if effected will have a limited impact.

Such a risk-based approach is consistent with other significant initiatives relating to the soundness of the financial markets. For example, it was used in the Interagency White Paper on Sound Practices to Strengthen the Resiliency of the U.S. Financial Systems, which focused on clearance and settlement issues. Specifically, in the course of promulgating the Interagency White Paper with a consortium of financial regulatory agencies, the Commission noted the preference of commenters that the agencies retain a "sound practices paper format" rather than adopt a regulatory approach that could be susceptible to a "one-size-fits-all" application.[6] Ultimately, the Commission and other agencies agreed with this view and did not dictate a one-size-fits-all approach. As discussed below, we believe that the obligations applicable to any particular SCI entity under proposed Reg. SCI should vary based on the criticality of the function performed and the materiality of the SCI event.

B. *SCI Alternative Trading Systems*

The proposed rule would define an SCI alternative trading system ("SCI ATS") using specified thresholds. Specifically, with respect to NMS stocks, an SCI ATS would, during at least four of the preceding six calendar months, have: (i) five percent or more in any single NMS stock, and 0.25 percent or more in all NMS stocks, of the average daily dollar volume reported by an effective transaction reporting plan, or (ii) one percent or more, in all NMS stocks, of the average daily dollar volume reported by an effective transaction reporting plan.[7] With respect to equities securities that are not NMS stocks, an ATS would be subject to Reg. SCI if the

---

[6] *See* Securities Exchange Act Release No. 47638 (Apr. 7, 2003), 68 *Fed.Register* 17809 (Apr. 11, 2003) (Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial Systems) ("Interagency White Paper").

[7] *See* proposed Rule 1000(a).

transactions reported to a SRO are five percent or more of the average daily dollar volume as calculated by the SRO to which such transactions are reported. A fixed income ATS would be subject to Reg. SCI if it had five percent or more of either: (i) the average daily dollar volume traded in the United States, or (ii) the average daily transaction volume traded in the U.S.[8]

SIFMA does not believe that the optimal manner in which to define SCI entities is by trading volume. Instead, we urge the Commission to consider the risk-based approach that focuses on the criticality of functions performed when applying Reg. SCI. Under this approach, any obligations under Reg. SCI would depend solely on the function performed by an ATS rather than on whether an ATS met a given volume threshold. As noted, for example, an ATS that directly affects the public quotation stream might reasonably be deemed more critical than a marketplace that is responsible for the function of providing non-displayed liquidity. Similarly, an ATS that is not responsible for the primary price-setting function for NMS securities should only be obligated to adhere to the requirements for a low to medium criticality function.

However, in the event that the Commission determines to press forward with the volume-based approach, we have the following questions and comments on the proposed definition of an SCI ATS.[9] Generally speaking, we agree that, under a volume based approach to identifying SCI ATSs, the Regulation ATS percentage threshold of 20 percent for compliance with systems capacity integrity and security planning may be too high. However, while a 20 percent threshold may be too high, we respectfully disagree with the proposed alternative thresholds for determining SCI ATSs for NMS stocks. In particular, we believe that the proposed threshold of one percent of the volume in all NMS stocks during a period of four out of six consecutive months will capture SCI ATSs systems that do not impact the national market system sufficiently to warrant the onerous requirements of the proposed regulation.

Alternatively, we propose that the test for an SCI ATS trading NMS securities be whether the ATS was responsible for five percent or more of the volume in all NMS stocks during any twelve month period. This approach would eliminate the alternative prong of one percent or more threshold of average daily dollar volume in all NMS stocks and, instead, focus on those ATSs that have demonstrated sustained trading of NMS stocks at a level commensurate with the obligations that would be imposed under a significant market under Reg. SCI. Correspondingly, this approach would weed out ATSs that temporarily crossed the threshold in NMS securities, but do not have a sustained level of market volume. The longer measurement period of 12 months is particularly important given the enhanced obligations that would be imposed on an SCI ATS under Reg. SCI in comparison to the capacity, integrity and security obligations under

---

8 *See* proposed Rule 1000(a); *see also* Proposing Release at 78 *Fed.Register* 18093.

9 In response to the Commission's request for comments, SIFMA does not support the expansion of proposed Reg. SCI to all broker-dealers. In many cases, broker-dealers generally perform functions that do not have any systemic impact on the operation of the national market system. In addition, broker-dealers already are subject to numerous regulations requiring the establishment of controls, including the Commission's Market Access Rule.

Rule 301(b)(6) of Regulation ATS. We further recommend that the determination be performed once a year and in the same given month (i.e., June) for consistency and planning purposes.

Notwithstanding our proposed recommendations put forth above, should the Commission determine to press forward with its volume-based approach for NMS stocks, SIFMA requests clarification on one aspect of the definition of a SCI ATS. Specifically, when evaluating if an ATS meets the definition of a SCI ATS under the proposed rule, the Commission proposes one prong of the volume threshold to be "0.25 percent or more in all NMS stocks, of the average daily dollar volume reported by an effective transaction reporting plan."[10] As there is more than one transaction reporting plan, SIFMA requests clarification if the proposed volume thresholds will be calculated per plan or calculated off of all NMS volume?

As to the volume thresholds for SCI ATSs that process non-NMS stocks, municipal securities and corporate debt securities, SIFMA believes that reducing the threshold from 20 percent of the average daily volume per Rule 301(b)(6) of Regulation ATS to 5 percent is too low and will unnecessarily include ATSs for these product types that are not systemic to maintaining fair, orderly, and efficient markets. SIFMA recommends that the Commission undertake further study to determine the proper thresholds for non-NMS securities, taking into account the unique nature of those types of securities. In addition, once the proper thresholds have been identified, we recommend that the determination be performed once a year and in the same given month (i.e., June) for consistency and planning purposes.

Regardless of the threshold ultimately adopted by the Commission for SCI ATSs, it will be important that the rule provide an appropriate phase-in period prior to effectiveness for an ATS that becomes subject to Reg. SCI for the first time. Such an ATS will need sufficient time to establish and implement the policies and procedures and to build the infrastructure needed to ensure compliance with the rule. We recommend that ATSs that become SCI ATSs for the first time be required to begin complying with Reg. SCI within six months of satisfying the threshold for becoming an SCI ATS.

III. SCI SYSTEMS AND SCI SECURITY SYSTEMS

Proposed rule 1000(a) would define the term "SCI systems" as "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."[11] Proposed Rule 1000(a) also would define the term "SCI security system" 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."[12]

---

[10] *See* proposed Rule 1000(a).

[11] *See* proposed Rule 1000(a); *see also* Proposing Release 78 *Fed.Register* at 18099.

[12] *Id.*

SIFMA believes that, consistent with its comments concerning the definition of SCI entity, the definition of an SCI system can be streamlined and tailored to reflect differences in the priority of such systems. SCI entities should be responsible for assessing and identifying those SCI systems that are of highest priority to their proper functioning as an SCI entity. For example, some ATS operators currently categorize their higher priority systems to include: (1) matching engines; (2) market data systems; (3) order routing systems; and (4) real-time surveillance risk systems. Lower priority systems in an ATS might include end of the day / non-real-time surveillance systems, and non-real-time (e.g., not ACT) regulatory reporting, as well as clearance and settlement systems. Non-ATS SCI entities may have different ways of prioritizing their SCI systems.

Importantly – and whether the Commission adopts a risk-based approach as recommended herein, or proceeds with its current proposal – SIFMA strongly recommends that the Commission eliminate the term "SCI security system" in the proposed rule. That definition is overly broad and may encompass a significant number of systems in each SCI entity that will require separate tracking and application of security standards and reporting requirements but that create no unique risks to the operation of the markets.[13] Instead, the Commission should require that SCI entities take appropriate measures to ensure the security of SCI systems. This would allow SCI entities to review the security of critical SCI systems holistically, rather than in a piecemeal and fragmented manner. Allowing firms to address security issues in this manner would be more efficient from a resource perspective and, we believe, more effective than addressing system security in a more proscriptive manner.

Notwithstanding our belief that a risk-based approach would more effectively achieve the goals of the proposed rule, we note several comments on the proposed definition of an SCI system more generally. First, the definition is vague and potentially very broad, particularly in light of the rule's approach to covered entities. The current definition lacks materiality thresholds for firms making the requisite determinations, particularly given that the breadth of the listed functions arguably encompasses most, if not all, of an SCI entity. Greater clarity is necessary with respect to all aspects of the definition, and examples of what the Commission would view as within the definition would be important to firms making determinations under the rule. Finally, SIFMA believes that systems used in testing and development should not be included in the definition of SCI system. Testing and development systems, by their nature, are designed to uncover and address potential issues with new coding or systems. Therefore, it is not clear why they would need to be included in the definition of an SCI system.

SIFMA also disagrees with the proposal to include systems that are operated "on behalf of" an SCI entity within the definition of an SCI system. The breadth of this provision is significant given that an SCI system includes any system that directly supports "order routing" or

---

[13] The Commission provides that "the proposed definition of SCI security systems is designed to cover other types of systems if they *share network resources* with SCI systems and, if breached, would be reasonably likely to pose a security threat to SCI systems." [emphasis added] *See* Proposing Release 78 *Fed.Register* at 18099. The proviso that the systems share network resources is quite broad and has the potential to subject all systems to Reg. SCI.

"market data," the rule could be interpreted to require any SCI ATS that permits its subscribers to use third party order management systems to send it orders to ensure that the third party OMS vendor is in compliance with the rule. The same holds true for market data vendors, many of which may not be subject to the Commission's jurisdiction. While SCI entities could seek to address their Reg. SCI obligations with such vendors contractually, it seems unlikely that third party vendors would agree to provide the level of oversight / inspection that might be required in order for an SCI entity to demonstrate its compliance with this aspect of the rule. We believe that Reg. SCI should be limited to those systems under the control of an SCI entity. To the extent that an SCI entity engages in an outsourcing arrangement related to an SCI system, such arrangements are already addressed by Section 17(d) of the Exchange Act, and the rules promulgated thereunder for SROs, and SRO guidance which would apply to SCI ATSs.[14]

IV. SCI EVENTS

Certain substantive requirements for SCI entities are triggered upon the occurrence of an SCI event. The Commission proposes to define an SCI event as an event at an SCI entity that constitutes: (1) a systems disruption; (2) a systems compliance issue; or (3) a systems intrusion.[15]

As discussed in greater detail below, SIFMA believes the proposed definition of SCI event is too broad and requires greater clarity and specificity. Further guidance is critical given the obligations triggered under Reg. SCI, and necessary to facilitate consistent application and understanding by SCI entities. Lastly, and importantly, the proposed definitions of SCI events should include a materiality component. Specifically, SCI events should be those events that constitute: (1) a material systems disruption; (2) a material systems compliance issue; or (3) a material systems intrusion. As discussed below, SIFMA believes materiality thresholds should likewise apply to each aspect of a reporting requirement.

A. *Systems Disruptions*

The Commission proposes that the term "systems disruption" be defined to mean "an event in an SCI entity's SCI systems that results in: (1) [a] failure to maintain service level agreements or constraints; (2) a disruption of normal operations, including switchover to back-up equipment with near-term recovery of primary hardware unlikely; (3) a loss of use of any such system; (4) a loss of transaction or clearance and settlement data; (5) significant back-ups or delays in processing; (6) a significant diminution of ability to disseminate timely and accurate market data; or (7) a queuing of data between system components or queuing of messages to or from customers of such duration that normal service delivery is affected."[16]

---

[14] *See e.g.*, 15 U.S.C 78q(d), and 17 CFR.240.17d-2; *see also* NASD NTM 05-48, ("Outsourcing: Members' Responsibilities When Outsourcing Activities to Third-Party Service Providers"); *see also* NASD Office of General Counsel Interpretative Letter re "A Member's Responsibilities Regarding the Outsourcing of Certain Activities," available at http://www.finra.org/Industry/Regulation/Guidance/InterpretiveLetters/P017175.

[15] *See* proposed Rule 1000(a).

[16] *See* Proposing Release, 78 *Fed.Register* at 18101.

As currently defined, not all systems disruptions would create risk to an SCI entity and the market functions it performs. For example, data queues are not unusual in today's markets and, in light of this, it is not clear when a queue will rise to the level of affecting "normal service." Similarly, a temporary disruption to clearance and settlement data that is resolved before the end of the trading day might be viewed differently, say, than the loss of a matching engine for the same period of time. Also, it is not clear why a seamless switchover to back up equipment should trigger the same requirements under Reg. SCI as the failure of an SCI system.

In addition, the proposed definition of a systems disruption is designed to capture problems with SCI systems such as "programming errors, testing errors, system failures, or if a system release is backed out after it is implemented in production."[17] SIFMA respectfully disagrees with the inclusion of "testing errors" in the definition. Errors are a common part of testing – indeed, testing is intended in part to help identify errors – and should not result in a reporting obligation.

B. *Systems Compliance Issues*

Under the proposed rule, a "systems compliance issue" is 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 governing documents, as applicable."[18] This requirement is particularly troubling in light of the broad definition of an SCI system and the rate at which firms modify their systems. Firms have systems issues regularly; to the extent that a system is found to be deficient in any manner, it is likely that it may be argued that the deficiency had some impact on the SCI entity's ability to comply fully with the federal securities laws. SRO self-reporting rules implicitly recognize the inevitability of systems problems and appropriately limit the extent to which systems issues must be self-reported to those issues that arise from a material failure of a member firm's systems, policies or practices, involving numerous customers, multiple errors or significant dollar amounts.[19]

C. *Systems Intrusion*

The Commission proposes to define "systems intrusion" as "any unauthorized entry into the SCI systems or SCI security systems of an SCI entity."[20] SIFMA believes that the proposed definition would benefit from greater clarity and guidance from the Commission to ensure that the SCI entities interpret the definition consistently. For example, it is unclear whether a "systems intrusion" would include physical security breaches. SIFMA also believes that the

---

17 *Id.*

18 *See* Proposing Release, 78 *Fed.Register* at 18103.

19 *See e.g.*, FINRA Rule 4530.

20 *Id.*

proposed rule should be modified to make clear that an intrusion by an SCI entity employee into an SCI system that has been reasonably determined by an SCI entity as inadvertent should not constitute a "systems intrusion."

It is appropriate to exclude from the rule attempted intrusions that do not breach systems or networks. Unfortunately it is not uncommon for firms to experience repeated, unsuccessful attempts to gain access to their systems. The inclusion of such "attempts" in the rule would result in excessive notices to the Commission and the triggering of other obligations under the rule when, in fact, an SCI entity had effective security controls. Consequently, SIFMA agrees with the Commission's proposed definition that unsuccessful "attempts" at intrusions are not SCI events.[21]

Similarly, SIFMA notes that resilient security architecture is designed to be multi-layered, and while unauthorized access into an "outer layer" technically could constitute an intrusion, it would neither impair the system nor put that system at risk. The fact that the peripheral system with limited exposure is intruded is immaterial, and SCI entities' systems are designed to address such occurrences. For example, if an initial control fails, standard architecture design provides that a secondary control would be triggered. Thus, SIFMA recommends the Commission clarify that the definition of "systems intrusion" excludes such an event.

SIFMA believes it is appropriate to include the "unauthorized use or unintended release of information data." However, the definition should specify that the intrusion resulted in unauthorized use or unintended release of information data. Moreover, the definition should specify that an intrusion arises only when there is unauthorized access to (i) confidential information or (ii) the SCI systems of an SCI entity that materially disrupt the operations of such systems. SIFMA notes that discovery of an intrusion that results in the release of confidential information is not real-time, but rather occurs after the fact. That being said, SIFMA further notes that there are industry standards (e.g., standards promulgated by the Federal Financial Institutions Examination Council) that govern annual reporting of breaches.

D. *Dissemination of SCI events*

The Commission proposes that the term "dissemination SCI event" be defined as "an SCI event that is a: (1) systems compliance issue; (2) systems intrusion; or (3) systems disruption that results, or the SCI entity reasonably estimates would result, in significant harm or loss to market participants."[22] As discussed in greater detail below, the Commission proposes requirements for disseminating information regarding certain SCI events to members or participants.[23]

---

21 *See* Proposing Release, 78 *Fed.Register* at 18103.

22 *See* Proposing Release, 78 *Fed.Register* at 18104

23 *Id.*

SIFMA believes the definition of "dissemination SCI event" should be amended to apply only to material systems intrusions and system compliance issues and materiality should be defined as those events that would result in significant harm or loss to market participants.

V. OBLIGATIONS OF SCI ENTITIES

A. *Overview of Proposed Obligations*

Paragraph (b) of proposed Rule 1000 sets forth requirements that would apply to SCI entities. Certain of the requirements, such as the need for policies and procedures, would apply generally to all SCI entities at the outset. Other requirements are triggered by an SCI event. As proposed, each of these requirements would apply equally to all SCI entities.[24]

As discussed below, SIFMA believes the Commission should provide a baseline standard under Reg. SCI to which all SCI entities are subject, with additional obligations placed on SCI entities and systems based on the tier and profile of such entity, system or event.

B. *Proposed Requirement to Establish and Maintain Policies and Procedures*

SIFMA agrees and supports the notion that all SCI entities must have policies and procedures designed to: (1) safeguard capacity, integrity, resiliency, availability and security of SCI systems; and (2) ensure that SCI systems operate in the manner intended. SIFMA believes, however, that pursuant to a risk-based approach, certain of these policies and procedures should be applied based on the function supported by the SCI entity and enabled via an SCI system.

The Commission proposes that Reg. SCI policies and procedures include "[p]eriodic capacity stress tests of such systems to determine their ability to process transactions in an accurate, timely, and efficient manner."[25] SIFMA appreciates the importance of stress testing for functions performed by high criticality Reg. SCI entities. However, SIFMA believes it is more appropriate for the SCI entities to implement policies and procedures for periodic capacity *monitoring*, or stress testing as the SCI entity determines. Monitoring capacity allows such SCI entities to manage their systems performance and availability on a more cost effective basis.

The Commission also proposes that "business continuity and disaster recovery plans that include maintaining backup and recovery capabilities sufficiently resilient and geographically diverse to ensure next business day resumption of trading and two-hour resumption of clearance and settlement services following a wide-scale disruption".[26] SIFMA notes that the Interagency Whitepaper distinguishes between "core clearing and settlement organizations" and firms that

---

[24] "Proposed Regulation SCI would provide mandatory uniform requirements for 'SCI entities.'" *See* Proposing Release 78 *Fed.Register* at 18092; *see also supra* note 5.

[25] *See* proposed Rule 1000(b)(1)(i)(B).

[26] *See* proposed Rule 1000(b)(1)(i)(E).

play a significant role in the financial markets. Specifically, the agencies recommend that "core clearing and settlement organizations develop the capacity to recover and resume clearing and settlement activities within the business day on which the disruption occurs with the overall goal of achieving recovery and resumption within *two hours* after an event." [emphasis added][27] Whereas, firms that "play significant roles in the other critical functions of the financial markets should strive to achieve a *four-hour* recovery time capability for clearing and settlement activities in order to ensure that they will be able to meet the one day business recovery target." [emphasis added][28] SIFMA recommends that the SEC continue to distinguish between SCI entities responsible for the highly critical function of centralized counterparties (e.g., clearing agencies registered with the SEC) and SCI entities that are not.

C. *Notification to the Commission of an SCI Event*

Proposed Rule 1000(b)(4) would require an SCI entity to notify the Commission orally or in writing upon any responsible SCI personnel becoming aware of an "immediate notification SCI event" – a systems disruption that the SCI entity reasonably estimates would have a material impact on its operations or on market participants, any systems compliance issue or any systems intrusion. In the event such personnel became aware of an immediate notification event outside of normal business hours, notification would need to be made at that time rather than at the start of the next business day. Written notification would be required within 24 hours of awareness of any SCI event.[29] SIFMA notes again that there is only one materiality qualifier among the requirements that would trigger Commission notification (systems disruption). SIFMA believes it is more appropriate to report only material SCI events and, therefore, recommends that the definitions of SCI events be amended to include materiality thresholds. Alternatively, the Commission could amend the definition of "material notification SCI event" to include the broader materiality standard.

SIFMA believes that when applying a risk-based approach to Reg. SCI, not all SCI events rise to the level of requiring immediate notification to the Commission. SIFMA agrees that events that occur to higher priority systems warrant immediate notification to the Commission. However, events involving lower priority systems likely will not warrant the need to notify the Commission immediately. Those events could be reported to the Commission on an aggregated and periodic basis. SIFMA believes that attendant with a policies and procedures approach, market participants should identify those events that warrant Commission notification. For those items that merit notification, SIFMA believes that the timing of such notification should not be the same for all SCI events.

As currently contemplated, the notification requirement may not be very useful to the Commission staff. It takes time to review and analyze data to determine the cause of a systems disruption. Under these circumstances, the 24 hour requirement for written notification is

---

[27] *See* Interagency White Paper, 68 *Fed.Register* at 17813.

[28] *Id.*

[29] *See* proposed Rule 1000(b)(4); *see also* Proposing Release 78 *Fed.Register* at 18118.

insufficient and likely will result in cursory notifications at best. SIFMA respectfully proposes as an alternative that for those events that require "real-time" notification to the Commission staff, SCI entities be allotted additional time to provide the written report. Further, the Commission should acknowledge that inherent in any real-time notification obligation is the likelihood that information will change as more investigation is performed. SCI entities should not be held liable for information that is later found to be incomplete or inaccurate because of additional information subsequently obtained.

In order to maximize the benefit of the notification requirement, SIFMA respectfully recommends that the notification of an SCI event related to a systems intrusion be reported to the Financial Services Information Sharing and Analysis Center ("FS-ISAC"), in addition to the Commission.[30] The FS-ISAC is capable of not only analyzing the data to determine trends in cyber threats and attacks, but also in disseminating such information to all market participants. Consequently, SCI entities would be informed how to enhance their SCI systems to thwart known cyber security threats.

SIFMA also is concerned that SCI entities will err on the side of caution when evaluating notification requirements, which will result in over-reporting of "events," for fear of violating Reg. SCI. This, in turn, could ultimately penalize SCI entities if the SEC is monitoring the reports strictly on a quantity basis. To alleviate this concern, SIFMA proposes that the Commission include language in the adopting release that the focus on Reg. SCI will be on the reasonableness of an SCI entity's policies and procedures and the application of such policies and procedures. SIFMA notes that this was done in Regulation NMS with respect to the likelihood of some trade-throughs notwithstanding policies and procedures to comply with Rule 611.[31]

D. *Dissemination of Information to Members or Participants of an SCI event*

Proposed Rule 1000(b)(5) would require prompt dissemination of information to members or participants of SCI entities relating to SCI events that the SCI entity reasonably estimates will result in significant harm or loss to such participants. There is a limited exception to this requirement for systems intrusions so as to not compromise the investigations of such intrusions.[32]

---

[30] The FS-ISAC was established by the financial services sector in response to 1998's Presidential Directive 63. "That directive - later updated by 2003's Homeland Security Presidential Directive 7 - mandated that the public and private sectors share information about physical and cyber security threats and vulnerabilities to help protect the U.S. critical infrastructure." *See* "About FS-ISAC" at https://www.fsisac.com/about.

[31] *See* Exchange Act Release No. 51808 (Jun. 9, 2005) 70 *Fed.Register* 37496, 37534, where the Commission noted that the "requirement of written policies and procedures, as well as the responsibility assigned to trading centers to regularly surveil to ascertain the effectiveness of their procedures and take prompt remedial steps, is designed to achieve the objective of eliminating all trade-throughs that reasonably can be prevented, while also recognizing the inherent difficulties of eliminating trade-through transactions that, despite a trading center's reasonable efforts, may occur." *See also* 17 CFR 242.611.

[32] *See* proposed Rule 1000(b)(5).

SIFMA has two general comments on this proposed obligation. First, SCI entities should have the discretion to determine which participants or members are affected and require notification. There can be occasions where an "event" occurs that does not affect all members; therefore an SCI entity should only be obligated to inform those impacted. Second, SIFMA believes that SCI entities should have the authority to dictate the method of notification; specifically, an SCI entity should be permitted to notify the participants or impacted parties directly, as opposed to posting such a notification to a public website.

E. ***Notification of Material Systems Change***

Proposed Rule 1000(b)(6) would require an SCI entity, absent exigent circumstances, to notify the SEC in writing at least 30 calendar days before implementation of any planned material systems changes.[33] Rule 1000(a) would define a "material systems change" as 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 affect the existing security of such systems.

SIFMA appreciates the policy objective of keeping the SEC staff informed of major changes to SCI systems. However, SIFMA does not believe that advance notification of material systems changes is necessary for all SCI entities and all SCI systems. If the Commission elects to maintain this requirement, SIFMA believes it is appropriate to limit the notification of material systems changes only to higher priority SCI systems. Changes to lower criticality systems could provide notification at the time of the systems change, or periodically throughout the year.

Additionally, SIFMA believes that the Commission clarify the "materiality" aspect of this proposed requirement. The SEC could, for example, clarify that a material change to an outward facing system (i.e., a system that interfaces with users) would be a change that requires the users to recode or test their own systems to maintain connection to the SCI system.

SIFMA believes that absent the proposed narrowing of this requirement, the obligation to notify the Commission of material systems changes could have significant unintended consequences. The proposal could affect a firm's ability to take decisive action. Firms often must take decisive action without any time for a lengthy review and approval processes given that the speed-of-response to cyber incidents often is measured in seconds. SIFMA appreciates that the Commission has provided the carve-out to implement material systems changes without notification under "exigent" circumstances. However, SIFMA is concerned that if the Commission or its staff disagrees with the SCI entity as to what constitutes an exigent

[33] *See* proposed Rule 1000(b)(6); *see also* Proposing Release 78 *Fed.Register* at 18122.

circumstance, after the fact, the SCI entity could be cited for a violation of Regulation SCI even though it responded to an event in good faith.

SIFMA also is concerned that the proposal could inadvertently affect the soundness of SCI entities' systems. For example, firms implement systems updates and modifications over time to, among other things, minimize potential risk and disruption. However, if the notification requirement becomes sufficiently burdensome, it will incentivize firms to bundle systems changes to limit the number of reports filed, which generates risks to the SCI systems. Consequently, the Commission's proposed requirement, if not properly implemented, could make systems more vulnerable and curtail innovation.

SIFMA notes that the definition of SCI system includes development and testing systems. As previously discussed, SIFMA does not believe that non-production systems should be included in the adopted definition of SCI system. SIFMA therefore requests confirmation that the proposed notification requirement does not mean that prior notification would be required for changes that do not pertain to the production environment.

We note that this notification requirement could result in a de facto rule filing requirement, similar to the SRO rule filing requirements pursuant to Section 19(b) of the Securities Exchange Act of 1934[34] and Rule 19b-4[35] promulgated thereunder. SIFMA notes that Proposed Form SCI contains, in the instructions, that the proposed change must be "clearly and comprehensively" described. This requirement raises concern that the SEC staff would be authorized to "reject" a notification for inadequate description, which in turn would delay a planned systems change.

F. *Annual Review*

Proposed Rule 1000(b)(7) would require an SCI entity to conduct a review of its compliance with Reg. SCI not less than once each calendar year, and submit a report of the SCI review to senior management of the SCI entity no more than 30 calendar days after completion of such review.[36] Proposed Rule 1000(a) would define the term "SCI review" to mean a review, following established procedures and standards, that is performed by objective personnel having appropriate experience in conduction reviews of SCI systems and SCI security systems, and which review contains: (1) a risk assessment with respect to such systems of the SCI entity; and (2) an assessment of internal control design and effectiveness to include logical and physical security controls, development processes, and information technology governance, consistent with industry standards.[37]

---

34 15 USC § 78s(b).

35 17 CFR 240.19b-4

36 *See* Proposed Rule 1000(b)(7); *see also* Proposing Release 78 *Fed.Register* at 18123.

37 *Id.*

SIFMA believes the annual review requirements should be scaled pursuant to the proposed risk-based approach. The Commission should rely on SCI entities to perform a risk-based analysis of their systems based on priority and review accordingly. Under this approach, only higher priority systems, as discussed above, would be subject to annual review, whereas lower priority SCI systems would be subject to a longer review period.

G. *Business Continuity and Disaster Recovery Plans*

Proposed Rule 1000(b)(9) would require testing of SCI entity business continuity and disaster recovery plans by SCI entity members and participants. Specifically, proposed Rule 1000(b)(9)(i) would require an SCI entity, with respect to its business continuity and disaster recovery plans, including its backup systems, to require participation by designated members or participants in scheduled functional and performance testing of the operation of such plans, in the manner and frequency as specified by the SCI entity, at least once every 12 months. Proposed Rule 1000(b)(9)(ii) would further require an SCI entity to coordinate such testing on an industry or sector-wide basis with other SCI entities.[38]

The Commission stated that it preliminarily believes that, even if an SCI entity is able to operate following an event that triggers its business continuity and disaster recovery plans, unless there is effective participation by certain of its members in the testing of such plans, the objective of ensuring resilient and available markets in general, and maintenance of fair and orderly markets in particular, would not be achieved. Furthermore, the SEC provided that each entity would need to schedule, and require their designated members to participate in, scheduled "functional and performance testing."[39] Functional testing examines whether a system operates in accordance with its specifications, whereas performance testing examines whether a system is able to perform under a particular workload.[40]

SIFMA agrees with the overall goals and policy objectives of business continuity plan ("BCP") and disaster recovery testing. However, SIFMA has two primary concerns with the proposal: (1) the obligation / mandate to require participation by SCI entities' members or participants; and (2) the requirement for end-to-end testing. It is unclear how SCI entities could enforce the requirement that their customers engage in BCP testing. SIFMA respectfully requests the SEC clarify the authority to mandate such participation Irrespective, it is SIFMA's belief that it would be more appropriate for SCI entities' members and participants to be responsible for their own business continuity plans and testing.

SIFMA notes that firms currently undergo their own BCP testing as a best business practice. SIFMA also sponsors and facilitates an annual industry-wide connectivity test. However, the SEC's proposal for industry-wide, end-to-end testing is a significant change to

---

38 *See* Proposed Rule 1000(b)(9); *see also* Proposing Release 78 *Fed.Register* at 18125.

39 *See* Proposing Release 78 *Fed.Register* at 18125.

40 *See* Proposing Release 78 *Fed.Register* at footnote 267.

industry best practices. Additionally, there is a great deal of uncertainty with respect to the logistics and implementation of the proposed member/participant and industry-wide BCP testing, including who ultimately would be responsible for planning and organizing the industry-wide testing.

SIFMA respectfully recommends that the SEC adopt a BCP testing requirement more akin to the best practices described in the Interagency White Paper.[41] SIFMA appreciates that the best practices of the Interagency White Paper were limited to clearing and settlement functions. However, SIFMA believes that the SEC should leverage the best practices of the Interagency White Paper, and expand them to include the functions classified as "highly critical" as described above. SIFMA further proposes a phased-in approach to the implementation of this broader BCP testing over a period of years. Specifically, SCI entities could conduct testing of specific SCI systems over the course of time, rather than a full end-to-end test, which cannot be done without significant planning and coordination across the industry that could conceivably take significant time to agree on. SIFMA believes that this approach would be consistent with our overall proposal for a risk-based implementation of the Reg. SCI requirements.

VI. ACCESS TO SYSTEMS

Proposed Rule 1000(f) would require SCI entities to provide Commission representatives reasonable access to their SCI systems and SCI security systems. The SEC notes in the Proposing Release that representatives of the Commission would be permitted access to SCI systems either remotely or on-site.[42]

SIFMA strongly disagrees with this aspect of the proposal. SIFMA is not aware of any instance in which securities regulators have had direct and real-time access to systems. SIFMA notes that industry standards require that technology systems be safeguarded with numerous controls surrounding access. It is counter to the policy objective of maintaining system security to provide representatives of the SEC with direct, uncontrolled access to the systems.

Furthermore, providing SEC representatives with access would generate significant risk, because it is unclear what controls the SEC would implement to protect the systems. There is no clarity as to how the SEC would ensure that the remote access to the member firms' systems would be done from a secure location. SIFMA notes that customers of broker-dealers must subscribe to governance standards and technology controls when accessing the systems of the broker-dealers. Customers are required to demonstrate their compliance with the broker-dealers' controls. SIFMA also disagrees with granting Commission staff access to production and test / development systems, because it could severely impact such a system. For example, an SEC

---

41 As noted in the Interagency White Paper, "[t]he agencies have identified four broad sound practices for core clearing and settlement organizations and firms that play significant roles in critical financial markets. The sound practices are based on long-standing principles of business continuity planning in which critical activities are identified, a business impact analysis is conducted, and plans are developed, implemented and tested."

42 *See* Proposed Rule 1000(f); *see also* Proposing Release, 78 *Fed.Register* at 18130.

representative with direct, uncontrolled access to testing and development systems could inadvertently impact the implementation of an upgrade to an SCI system.

SIFMA also believes it would be problematic even to provide "read-only" real-time access to the regulators. Regulators may get the wrong information, or misunderstand the functioning of the systems. Read-only access also may affect system performance. There is a steep learning curve in understanding the complicated systems utilized in the operation of SCI entities. Furthermore, systems change frequently. Even if an SEC representative gained familiarity with a specific system, the system may have changed by the time that the SEC representative schedules a follow-up audit or inspection of the system.

The proposed access rule would extend to the systems of third-party vendors of SCI entities. It is unclear how the regulated entities would facilitate such access. This aspect of the proposal could generate contractual issues with the third-party vendors.

SIFMA proposes as an alternative that SCI entities provide an individual contact for a designated SEC representative interested in the operation of an SCI entity's SCI systems. Specifically, SIFMA believes it is more appropriate for SEC representatives to be kept up to date through communications and designated meetings with the SCI entities' designated contact.

VII. SUPERSTORM SANDY

SIFMA would like to take the opportunity to address the Commission's discussion related to Superstorm Sandy contained in the Proposing Release.[43] As the Commission knows, Superstorm Sandy was an unprecedented storm; it has been described as a 1 in 250 year storm event, and resulted in the loss of life, as well as damage into the many billions of dollars. SIFMA and its members served a critical function during the storm of disseminating key information to and coordinating efforts among market participants and regulators.

In the days leading up to Superstorm Sandy, and during the course of the storm, there was consistent communication and dialogue between the securities industry and regulators discussing the potential consequences of the storm. These discussions included the SEC, the U.S. Commodity Futures Trading Commission ("CFTC"), Financial Industry Regulatory Authority ("FINRA"), the Federal Reserve, the United States Treasury, clearing agencies, and national securities exchanges. SIFMA considers the consistent dialogue between industry and the SEC during Superstorm Sandy as an example of highly successful coordination and communication during extreme conditions, particularly given the constantly changing nature of the storm. As a result, we were extremely surprised by the Commission's negative discussion of the collective efforts of industry and the regulators in the proposing release, which portrayed the market closures during the storm as an industry failure.

---

[43] *See e.g.*, Proposing Release, 78 *Fed. Register* at 18125; *see also* Proposing Release at 18164, where the Commission stated that "the two day closure of the equities and options markets in the wake of Superstorm Sandy has shown that more significant testing and better coordination of such testing could benefit market participants."

As the Commission is aware, the U.S. equity markets were closed for two days during Superstorm Sandy. This decision to close the markets during Superstorm Sandy and the immediate aftermath was driven primarily by concerns for the safety of personnel, not by systems issues. In addition, SIFMA and other industry members reviewed the closure decision and the safety concerns with senior Commission staff, who raised no objections to the decision. SIFMA and its members also stand by the decision to close the markets to preserve orderly market execution in an environment that was already taxing the infrastructure upon which we rely (for example, power, public transportation, and telecommunications).[44] To build on the lessons learned during Superstorm Sandy, SIFMA has been actively working with member firms and industry participants to develop a protocol that will provide a formal and organized process for future events that require a determination of whether equity markets should be closed.

SIFMA appreciates the importance of system and market resilience and shares the overriding goal to maintain open and orderly markets in the face of an event or to resume trading as soon as possible after a disaster. However, there will be times when markets will need to be closed, which SIFMA and its members hope will be rare. The operation of the SCI systems is just one component required for the markets to function. The securities markets also rely on critical infrastructure providers and people to operate, and in some instances the latter considerations may trump the former.

[44] During Superstorm Sandy, the New York City transportation system was severely impacted. For example, streets were closed and the subway system was shut down for a number of days. At least 750,000 New York City residents were without power.

* * *

SIFMA supports the proposed rule's policy goal of enhancing the Commission's oversight of the capacity, integrity, resiliency, availability and security of key automated systems of entities of particular importance to the national market system. SIFMA greatly appreciates the opportunity to provide the Commission with the foregoing comments and recommendations regarding the Proposal and stands ready to provide any additional information or assistance that the Commission might find useful. Should you have any questions, please do not hesitate to contact me at [redacted]), or Tom Price at [redacted]), or Karl Schimmeck at ([redacted]), or Timothy Cummings at ([redacted]).

Sincerely,

Theodore R. Lazo
Managing Director and
Associate General Counsel
SIFMA

CC: Mary Jo White, Chairman
Elisse B. Walter, Commissioner
Luis A. Aguilar, Commissioner
Troy A. Paredes, Commissioner
Daniel M. Gallagher, Commissioner

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