



Financial Industry Regulatory Authority

Marcia E. Asquith
Senior Vice President and
Corporate Secretary

Phone: 202-728-8831

July 8, 2013

Via Email to rule-comments@sec.gov

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

**Re: Comment Letter on Securities Exchange Act Release No. 69077
Proposed Regulation Systems Compliance and Integrity
(File No. S7-01-13)**

Dear Ms. Murphy:

FINRA staff¹ appreciates this opportunity to comment on the Securities and Exchange Commission's ("Commission") proposed Regulation Systems Compliance and Integrity, as published in the *Federal Register* on March 25, 2013 ("Regulation SCI").²

FINRA fully supports the goals of proposed Regulation SCI to help ensure the capacity, integrity, resiliency, availability and security of automated systems relating to the U.S. securities markets, and enhance the compliance of such systems with federal securities laws and regulations, through the formalization of standards and a regulatory framework for more effective Commission oversight of these systems. However, FINRA is concerned that the scope of Regulation SCI may be overly broad and may potentially encompass a large number of systems, perhaps unintentionally, which could diminish the overall focus and effectiveness of the proposal. In addition, some of the terms and requirements contained in Regulation SCI are ambiguous and may be difficult to apply to FINRA's operations.

¹ The comments provided in this letter are solely those of FINRA staff; they have not been reviewed or endorsed by the FINRA Board of Governors. For ease of reference, this letter may use "we," "FINRA" and "FINRA staff" interchangeably, but these terms all refer only to FINRA staff.

² See Securities Exchange Act Release No. 69077 (March 8, 2013), 78 FR 18084 (March 25, 2013) (File No. S7-01-13).

While many of the requirements in Regulation SCI are comparable to the current Automation Review Policy (“ARP”) guidelines, throughout the ARP development and implementation process, flexibility was afforded to self-regulatory organizations (“SROs”) such as FINRA to adopt parameters around the guidelines that were appropriate for their systems. FINRA believes that SCI entities should have the discretion and flexibility to make judgments and adopt reasonable parameters in their policies and procedures under Regulation SCI, including those related to SCI events, material changes and reporting. If the Commission will not afford such flexibility, then the Commission needs to define with greater clarity and specificity many of the terms and requirements under Regulation SCI.

In instances that we have identified, FINRA requests that the Commission reconsider the scope of Regulation SCI. While FINRA supports the goals of the proposal, we note that the burden of compliance will be substantial and could escalate dramatically depending on the scope of the requirements. FINRA strongly encourages the Commission to work closely with FINRA and the other SCI entities to reduce the burdens of Regulation SCI wherever possible, consistent with the Commission’s stated goals.

* * * * *

- I. SCI Systems and Security Systems
 - A. Regulation and Surveillance Systems
 - 1. Non-market regulatory and surveillance systems should be excluded from the definition of SCI systems
 - 2. Clarity is needed regarding the definitions of “regulation” and “surveillance” and the application of the Regulation SCI requirements to such systems
 - 3. At a minimum, non-market regulatory and surveillance systems should be excluded from the reporting and dissemination requirements
 - B. Internal Systems
 - C. Development and Testing Environments
 - 1. Development and testing environments should not be included in the definition of SCI systems
 - 2. The scope of SCI events should be narrowed to limit the instances in which the reporting requirements apply to development and testing environments
 - 3. The policies and procedures requirements should not apply separately to development and testing environments
 - D. SCI Security Systems
 - 1. The definition of SCI security systems should be narrowed
 - 2. Intrusions and material systems changes in SCI security systems should be reportable only where they impact SCI systems

- E. Proposed Tiered Approach to SCI Systems
 - 1. The requirements of Regulation SCI should not apply uniformly to all SCI systems
 - 2. The tiers would drive policies and procedures for defining and reporting SCI events and material systems changes
- II. SCI Events
 - A. General
 - B. Scope
 - 1. The scope of reportable systems disruptions should be narrowed and clarified
 - 2. The scope of reportable systems compliance issues should be narrowed
 - 3. The scope of reportable systems intrusions should be narrowed
 - C. Reporting Requirements (Timing and Information)
 - 1. General
 - 2. A 24 hour written notice requirement is unduly burdensome and may hinder an SCI entity's ability to investigate and correct systems issues
 - 3. Even the minimum required information may not be known or confirmed within 24 hours
 - 4. A more flexible approach to reporting is recommended
 - 5. A more flexible approach to providing updates is recommended
 - 6. The requirement that notification be provided outside of normal business hours should be eliminated or narrowed
 - 7. Different reporting standards should apply to different types of systems
 - 8. Where third parties are involved in the operation of an SCI entity's systems, delays may be inherent in the reporting process, and it may not be clear which SCI entity has the reporting obligation
 - D. Dissemination SCI Events
 - 1. The dissemination requirement for systems compliance issues should be narrowed
 - 2. The dissemination requirement should not apply to systems intrusions, or in the alternative, should be narrowed
 - 3. The dissemination requirement should be clarified
 - E. Trigger for the Reporting, Corrective Action and Dissemination Requirements Relating to SCI Events
 - 1. The definition of "responsible SCI personnel" is too broad
 - 2. Awareness of an SCI event is too broad a trigger
- III. Material Systems Changes
 - A. Scope
 - B. Reporting Requirements (Timing and Format)

- IV. Form SCI
 - A. Implementation
 - 1. SCI entities need time to learn the new form submission process
 - 2. Data format
 - B. Technical Questions
 - C. Suggested "Business Impact" Category

- V. Policies and Procedures Requirements
 - A. Capacity, Integrity, Resiliency, Availability and Security
 - 1. SCI industry standards
 - 2. Additional guidance is needed on the policies and procedures requirements
 - 3. Where more than one SCI entity is involved in the operation of an SCI system, it may not be clear how an SCI entity can satisfy its obligations
 - B. Requirements for the Safe Harbor
 - 1. General
 - 2. The requirements relating to systems testing are unclear and potentially overly burdensome
 - 3. The requirement relating to ongoing systems monitoring is unclear and potentially overly burdensome
 - 4. The requirements relating to assessments by legal and compliance personnel are unclear and potentially overly burdensome
 - 5. It is unclear how an SCI entity would satisfy the requirement that it "not have reasonable cause to believe that the policies and procedures were not being complied with"
 - 6. The safe harbor for individuals should be clarified and expanded beyond employees of the SCI entity

- VI. Business Continuity and Disaster Recovery Plans and Testing
 - A. Business Continuity and Disaster Recovery Plans
 - 1. The scope of the requirements should be clarified and narrowly construed
 - 2. The geographic diversity standard should be clarified
 - B. Mandatory Testing
 - 1. The scope of SCI systems included in the mandatory testing requirement should be clarified and narrowly construed
 - 2. The scope of the required testing is potentially overly broad and the benefits may not outweigh the risks
 - 3. Designation of members to participate in testing could impose significant burdens on members

- VII. SCI Review of Systems
 - A. Definition of “SCI Review”
 - 1. The requirement that SCI entities conduct an annual SCI review is inconsistent with a risk-based audit methodology
 - 2. The required components of an SCI review are too broad
 - B. Objectives and Intended Scope of the SCI Review
- VIII. Access to SCI Systems
- IX. Implementation Period
- X. Costs

* * * * *

I. SCI Systems and Security Systems

A. Regulation and Surveillance Systems

- 1. Non-market regulatory and surveillance systems should be excluded from the definition of SCI systems**

The Commission states that the purpose of 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 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.³ In addition, the Commission indicates that it believes that the continuing evolution of the securities markets to the current state, where they have become almost entirely electronic and highly dependent on sophisticated trading and other technology (including complex regulatory and surveillance systems, as well as systems relating to the provision of market data, intermarket routing and connectivity, and other member and issuer services), has posed challenges for its ARP program.⁴

The Commission further states that the proposed definition of SCI systems would reach those systems traditionally considered to be core to the functioning of the U.S. securities markets, namely trading, clearance and settlement, order routing, market data, regulation and surveillance systems.⁵ With respect to regulatory systems in particular, the Commission identifies systems for the regulation of the OTC market, systems used to carry out regulatory service agreements and similar future systems, including the

³ See 78 FR at 18092.

⁴ See 78 FR at 18089.

⁵ See 78 FR at 18099.

Consolidated Audit Trail repository.⁶ Further with respect to regulatory systems, the Commission notes that SCI entities that are obligated to comply with Section 31 of the Exchange Act employ various systems to generate, process, transmit or store electronic messages related to securities transactions, and such systems may include matching engines, transaction data repositories, trade reporting systems and clearing databases.⁷

In light of these and other statements, FINRA believes that, taken in context, the overall focus and appropriate scope of Regulation SCI are systems – including regulatory systems – that are directly related to the market. However, in a conference call with FINRA staff on April 25, 2013, Commission staff indicated that the intended scope may be much broader, and that the definition of SCI systems⁸ may encompass such non-market systems as FINRA’s Member Regulation systems.

FINRA believes that the inclusion of non-market systems would unnecessarily broaden the scope of Regulation SCI and significantly increase the cost and burden of compliance, without attaining corresponding benefits. In its broadest interpretation, “regulation” systems could be viewed as including FINRA Member Regulation applications, including systems that collect data in support of its member examination program; Enforcement, Registration and Disclosure (“RAD”), Central Registration Depository (“CRD”) and non-market Office of Fraud Detection and Market Intelligence (“OFDMI”) systems; as well as Regulatory Filings Application, Forms Submission Framework and other pipes through which member firms submit regulatory information to FINRA, including, e.g., short interest, Bluesheets and Corporate Financing filings. The data collected via these systems is not needed on a real-time basis, and alternative methods exist to obtain data, if necessary, in an acceptable time frame, without impact on the market or FINRA’s ability to fulfill its obligations as an SRO.

By way of example, one such system is FINRA’s electronic system used by member firms to file FOCUS reports. The FOCUS report reflects balance sheet, income statement and regulatory computations as of the most recent month-end period. The filing deadline for member firms is 17 days after month end, which means that the data is almost a month old by the time it reaches FINRA. This data is not disseminated publicly and has no direct impact on the functioning of any of the U.S. securities markets. Additionally, manual processes exist to collect key data from firms (e.g., via e-mail and spreadsheets), if needed.⁹ Thus, a disruption or other issue in the electronic FOCUS filing system –

⁶ See 78 FR at 18099.

⁷ See 78 FR at 18099, note 141.

⁸ Proposed Rule 1000(a) broadly defines 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.

⁹ These manual processes are used today if FINRA needs information from a particular firm at a greater frequency than the monthly or quarterly filing schedule allows.

even if the system were to go down for several days – would have no impact on the market, FINRA member firms or FINRA’s ability to fulfill its regulatory and other obligations as an SRO.

FINRA has 37 systems that are “in scope” under the current ARP guidelines.¹⁰ If the definition of SCI systems is broadly construed to apply to non-market regulatory and surveillance systems, approximately 111 FINRA systems could be subject to Regulation SCI, which would be an increase of 200% over the current in scope systems.¹¹ This would put a substantial burden on both FINRA and Commission staff to process all the new requirements, notifications and reports.¹²

Accordingly, FINRA requests that the definition of SCI systems be amended to replace the terms “surveillance” and “regulation” with “market surveillance” and “market regulation,” such that these terms would apply to systems that directly support the surveillance and regulation of the core market functions identified in the definition of SCI systems, i.e., trading, clearance and settlement, order routing and market data. FINRA believes that this approach is more appropriate in that it focuses on a regulatory or surveillance system’s proximity to the market and allows SCI entities to concentrate their critical resources on those systems that would have market impact. FINRA believes that excluding non-market systems would not hinder the stated goals of Regulation SCI, namely, the maintenance of fair and orderly markets, and the burdens associated with applying Regulation SCI broadly to such systems clearly outweigh the benefits.

¹⁰ These systems include, among others, such real-time market facilities as the FINRA Trade Reporting Facilities (“TRFs”) and Trade Reporting and Compliance Engine (“TRACE”) and such non-real-time market regulation systems as FINRA’s Order Audit Trail System (“OATS”) and Market Regulation surveillance patterns.

¹¹ This estimate includes FINRA Member Regulation, RAD, OFDMI and Enforcement systems. Depending on how broadly the definition of SCI systems may be construed, these numbers could increase if additional FINRA systems are included. For example, would FINRA Dispute Resolution systems be considered regulatory and therefore within the scope of the definition?

¹² FINRA notes that in calculating the burden estimates for requirements that mirror the ARP guidelines, e.g., many of the policies and procedures required under proposed Rule 1000(b)(1), the Commission uses a starting baseline of 50% for SCI entities that are currently subject to ARP. *See, e.g.*, 78 FR at 18145. However, such a baseline does not account for the significant expansion of the requirements if the definition of SCI systems is construed broadly, and as a result, these burden estimates may be too low.

Inclusion of non-market systems would unnecessarily and significantly increase FINRA's costs and would divert resources from other technology initiatives.¹³ While the Commission has expressed an intention to expand the current ARP guidelines, it has not provided the rationale for broadly encompassing non-market regulatory and surveillance systems. FINRA does not believe that the costs can be justified given the minimal benefits associated with applying the Regulation SCI requirements broadly to such systems.

2. Clarity is needed regarding the definitions of “regulation” and “surveillance” and the application of the Regulation SCI requirements to such systems

The Commission does not define the terms “regulation” and “surveillance” as used in the definition of SCI systems and the distinction between the two may not be clear in all instances.¹⁴ As noted above, FINRA believes that SCI systems should apply expressly to market systems and as such, believes that it would be appropriate to define “surveillance” to apply to systems used for the monitoring of market and other data, including trade, quote and order data, to detect indications of possible violations of relevant rules of an SCI entity or federal securities laws. If surveillance were defined or interpreted this way for purposes of the definition of SCI systems, then it is not clear what additional or different functionality would be captured by separately referring to “regulation” systems, particularly if the definition is limited to market systems.

Thus, FINRA requests that the Commission define “regulation” and “surveillance” and give specific examples of the systems or business processes that would fall within the scope of each definition. Particularly if SCI systems are not limited to market systems, then additional guidance will be required as to the scope of these definitions. For example, would systems that support member oversight and examinations be the type of regulatory system that the Commission considers in scope? What about systems used to support FINRA Dispute Resolution? Clear and specific guidance is imperative to enable SCI entities to accurately identify the universe of their systems that are subject to Regulation SCI.

¹³ It is important to note that FINRA has established and maintains a robust technology program around all of its regulatory systems. For those systems that are not specifically included within the scope of Regulation SCI, FINRA would continue to have vigorous and appropriate policies and procedures around, among other things, testing, operations and disaster recovery, as part of FINRA's overall regulatory program.

¹⁴ For example, Form SCI requires that SCI entities identify the affected system as surveillance or regulation. FINRA runs automated surveillance patterns in support of market regulation – would these patterns be considered both regulatory and surveillance? Would FINRA's OATS system be classified solely as regulatory? Understanding the import and consequence of a system being identified as “regulation” versus “surveillance” would assist SCI entities in determining the applicable category for their systems, as necessary.

In addition, a number of the requirements contained in Regulation SCI are specific to market systems, and in particular, real-time market facilities. Regulation SCI does not account for the differences among an SCI entity's systems, such as real-time market transparency facilities, real-time market surveillance systems, non-real-time (T+1 or greater) market surveillance systems and member regulation and other non-market systems (none of which are real-time).

For example, the business continuity and disaster recovery plan requirements contemplate next business day resumption of trading and two hour resumption of clearance and settlement. With respect to the testing of an SCI entity's emergency plans, the Commission states that, without effective participation by members and participants, the objective of ensuring resilient and available markets in general, and the maintenance of fair and orderly markets in particular, would not be achieved.¹⁵ Such objectives carry much less import with respect to non-market systems, as well as market systems that are not real-time. However, Regulation SCI does not expressly limit the scope or clarify how these requirements apply outside of the context of trading and clearance and settlement systems.¹⁶

Another example is the requirement that SCI entities disseminate information relating to certain SCI events. The Commission states that this requirement could promote the ability of market participants to assess the operation of the markets because events would be more transparent.¹⁷ However, it is not clear how information relating to a systems issue in a non-market regulatory system or a market surveillance system that does not operate on a real-time basis would assist market participants in assessing the market.

A third example is the application of the "loss of use" element of the definition of systems disruption. The Commission notes that a failure of primary trading or clearance and settlement systems, even if immediately replaced by backup systems without any disruption to normal operations, would be covered under this element of the definition.¹⁸ However, it is not clear how this element would apply to systems other than trading or clearance and settlement systems.

FINRA requests that the Commission clarify how each of the provisions of Regulation SCI applies and operates with respect to the different types of systems, including non-market systems (if they are not excluded from the definition of SCI systems) and market systems that are not real-time.

¹⁵ See 78 FR at 18125.

¹⁶ As discussed in Section VI.A.1, FINRA does not believe that it would be appropriate to require that SCI entities adopt these business continuity targets for systems that are not real-time and do not directly support trading or clearance and settlement.

¹⁷ See 78 FR at 18164.

¹⁸ See 78 FR at 18101.

3. At a minimum, non-market regulatory and surveillance systems should be excluded from the reporting and dissemination requirements

If non-market systems are included in the definition of SCI systems, FINRA believes that, at a minimum, they should be excluded from the reporting and dissemination requirements for SCI events and the reporting requirements for material systems changes. This exclusion maintains the Commission's stated goal of comprehensive reporting of SCI events to facilitate the Commission's regulatory oversight of the national securities markets,¹⁹ because as discussed above, systems issues, as well as systems changes, in non-market systems would not have an impact on the market and market participants. Applying the reporting requirements to these types of systems would significantly increase the volume of the reports the Commission receives and thereby potentially lessen the value of reporting overall.

B. Internal Systems

Based on our discussion with SEC staff, we understand that systems that are solely internal and not accessed by member firms or other outside parties, such as electronic libraries, likely would not fall within the definition of SCI systems. FINRA requests that the Commission confirm this understanding and expressly exclude from the definition internal document and data repositories and other systems that support an SCI entity's internal business users, e.g. systems used for purposes of case management and tracking examinations, investigations and other matters.²⁰

C. Development and Testing Environments

1. Development and testing environments should not be included in the definition of SCI systems

The definition of SCI systems broadly applies to systems "whether in production, development or testing." The purpose of the development and testing environments is to build new features and functions in multiple iterations, which inherently will encounter errors and breakdowns. Test environments are typically complete from a functional standpoint (i.e., all system components, modules programs); however, these

¹⁹ For example, in expanding the scope of reportable events under Regulation SCI, the Commission notes that "significant systems outages" under ARP was a considerably narrower category than those the Commission believes could pose risks to the securities markets and market participants. *See* 78 FR at 18101.

²⁰ FINRA notes that while these systems would be excluded from the definition of SCI systems, they may fall within the definition of SCI security systems, such that intrusions into such systems or material changes that affect the security of such systems may be reportable.

environments are not fully replicated in terms of scale.²¹ In addition, these environments do not usually have service level agreements because they are not considered mission critical. These are the very environments in which FINRA expects to find problems, before they surface in production. Including development and testing environments in the definition of SCI systems, and applying to them the same requirements that are applied to the production environment, would significantly increase an SCI entity's cost to comply with Regulation SCI and create excessive "noise," for example, with respect to the reporting of an SCI event, without a corresponding benefit.

Accordingly, FINRA recommends that the definition of SCI systems be revised to apply to production systems only. FINRA believes that the goals of Regulation SCI to promote robust processes and controls for development and testing could be achieved without including these environments in the definition of SCI systems and making them separately subject to Regulation SCI. For example, the policies and procedures that SCI entities would be required to adopt under Regulation SCI, e.g., with respect to reviewing and keeping current systems development and testing methodology, and conducting regular reviews and tests of SCI systems, would impose sufficient controls on the development and testing environments.²²

2. The scope of SCI events should be narrowed to limit the instances in which the reporting requirements apply to development and testing environments

As noted above, disruptions in service are an expected part of the development and testing environments. A disruption in the testing environment would likely manifest itself as a schedule risk to an ongoing project and not pose a risk to the production system itself. However, if a disruption in a development or testing system were to inadvertently impact a production system and result in an SCI event, then the reporting requirements under Regulation SCI would be triggered for the production system. It would be duplicative and unnecessary to require an SCI entity to report the same systems disruption in multiple environments. For example, if the same functional error appears in all three environments, an SCI entity should not be required to report three separate SCI events.

Accordingly, FINRA believes that if the development and testing environments are not excluded from the definition of SCI systems altogether, they should be excluded from the definition of systems disruption. In addition, systems compliance issues and systems intrusions in a development or testing environment should be reportable only if there is a

²¹ For example, a Quality Control ("QC") environment may only have access to a subset of the data available to production or QC servers may run with a smaller number of central processing units.

²² FINRA notes that its current policies and procedures related to the systems development life cycle comprehensively address the development process, which is not tied to any particular environment.

likelihood that the same issue or vulnerabilities exist in the current production environment and cannot be verified within a certain period, e.g., 24 to 48 hours.²³

3. The policies and procedures requirements should not apply separately to development and testing environments

As noted above, FINRA believes that sufficient controls are in place with respect to production systems, e.g., the change control process and systems development life cycle (“SDLC”) policies and procedures, such that separate policies and procedures specifically for the development and testing environments are unnecessary and duplicative. Accordingly, if development and testing environments are not excluded from the definition of SCI systems altogether, then the policies and procedures requirements under Regulation SCI should not apply separately to these environments.

D. SCI Security Systems

1. The definition of SCI security systems should be narrowed

Proposed Rule 1000(a) defines SCI security systems 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. The Commission notes that this definition could include systems pertaining to corporate operations, e.g., systems that support web-based services, administrative services, electronic filing, email capability and intranet sites, as well as financial and accounting systems.²⁴

FINRA shares the Commission’s concern that certain systems may present a vulnerable entry point to an SCI entity’s network and that the breach of such systems could disrupt an SCI entity’s operations and market-related activities. FINRA also supports the Commission’s approach of not applying the full scope of Regulation SCI to SCI security systems. However, FINRA believes that the definition of SCI security systems is too broad.

First, given the examples that the Commission provides, and particularly if the definition of SCI systems is interpreted broadly to include non-market systems, SCI security systems could potentially encompass most (if not all) of FINRA’s applications and systems, including desktops, printers, file servers and anything connected to FINRA’s network. Such a broad definition, combined with the broad definition of systems intrusion to include the introduction of malware, could result in multiple reportable events daily.

²³ If it is determined within the prescribed period that the same compliance issue or vulnerability exists in the production environment, then it would be reported as an SCI event in the production system only.

²⁴ See 78 FR at 18099.

Second, FINRA believes that the definition is too broad because it does not take into account compensating controls to protect SCI systems from other systems that reside on the same network. FINRA has strong perimeter security controls and measures to deter, detect and respond to attempts to gain unauthorized access to its systems. FINRA believes that such compensating controls are sufficient to protect and secure SCI systems from vulnerabilities that may arise from shared network links.

Accordingly, FINRA requests that the definition of SCI security systems be revised to exclude systems where there are compensating controls in place. Such an approach would afford SCI entities flexibility to determine the controls that they deem necessary to enforce sufficient security separation in their systems as part of their reasonable policies and procedures.

2. Intrusions and material systems changes in SCI security systems should be reportable only where they impact SCI systems

FINRA understands the importance of identifying and notifying the Commission of potential vulnerabilities in SCI systems, including vulnerabilities caused by SCI security systems. However, FINRA does not believe that meaningful information would be derived from reporting intrusions or material systems changes in SCI security systems where there is no reasonable expectation that they would impact an SCI system. Thus, FINRA believes that intrusions in SCI security systems should be reportable only if they have, or could reasonably be expected to have, an impact on an SCI system(s), e.g., where there are no compensating controls in place to prevent impact. Similarly, material systems changes in SCI security systems should be reportable only if they have or could be reasonably expected to have an impact not only on the security of the SCI security system itself, but also on the security of the SCI system(s) with which they share network resources.

E. Proposed Tiered Approach to SCI Systems

1. The requirements of Regulation SCI should not apply uniformly to all SCI systems

Given the diversity of an SCI entity's systems, FINRA does not believe that the requirements of Regulation SCI should apply uniformly to all SCI systems. For example, FINRA assigns various metrics to each of its systems, and the metric values are used to drive reasonable policies and procedures, including those for ARP reporting, security and disaster recovery. Specifically, each system is assigned a Recovery Time Objective ("RTO") to indicate the maximum number of days following a disaster that a system

must resume normal operations in production.²⁵ Each system is assigned a risk classification that drives the security practices and controls for that system. Using FINRA's application risk classification scoring methodology, each system is assigned a risk classification of critical, high, medium or low. The methodology looks at a number of risk attributes, such as business purpose and use, data sensitivity, extent of integrity impact if the system is corrupted, extent of financial impact if the system is unavailable or if confidential data is lost or data is corrupted, availability/disaster recovery requirement, and exposure (e.g., internal network or public internet).

Using these metrics, FINRA has developed risk-based tiered thresholds for purposes of, among other things, reporting outages and material systems changes in FINRA's systems that are in scope under the current ARP program. These thresholds have historically worked well for both the Commission and FINRA, and FINRA's procedures have proven to be effective in notifying Commission staff of systems outages and material systems changes. If the Commission were to allow SCI entities to adopt a tiered approach, FINRA would apply its current framework under Regulation SCI, such that "Tier 1" would generally comprise those FINRA systems that today have an RTO of one day (or less), i.e., real-time market facilities, such as the TRFs and TRACE. For such Tier 1 systems, more stringent standards under Regulation SCI generally would apply in recognition of the potential impact that issues in these systems could have on the functioning of the market.

FINRA recommends that the Commission consider a tiered approach based on the potential risk impact to the market of each system (or type of system). In the alternative, FINRA requests that the Commission expressly give SCI entities flexibility to establish a risk-based tiered framework as part of their reasonable policies and procedures under Regulation SCI, including, for example, applying different standards to different SCI systems for purposes of defining reportable SCI events and material systems changes.

2. The tiers would drive policies and procedures for defining and reporting SCI events and material systems changes

The tiers would drive the standards included in the policies and procedures required under proposed Rule 1000(b), as well as the policies and procedures for defining and reporting SCI events and material systems changes. With respect to SCI events, a tiered approach would take into account the differences among SCI systems and their proximity to the market, as well as the differences in impact that an SCI event would have on different SCI systems. Such impact would vary with respect to the duration of the disruption, whether the system is real-time or T+1 (or greater), whether there is an

²⁵ The RTO is set by the business users and is based on the criticality of the system. A FINRA trade reporting front-end system has an RTO of one day. Many FINRA Market Regulation surveillance systems have an RTO of two days, some have an RTO of 14 days and others have an RTO of 30 days. FINRA Member Regulation systems have an RTO of 30 days.

alternative means for users to perform their functions, and whether the whole system or just one function is down.

For example, while the TRFs provide data to the market in real-time, they do not provide audit trail data to FINRA Market Regulation in real-time. Thus, some SCI events, such as a delay in dissemination of data to the securities information processor (“SIP”), could have direct market impact, while other SCI events, such as a delay in the submission of data to the audit trail, would not. In addition, FINRA conducts market surveillance on a post-trade date (T+1 or greater) basis, and many of its automated surveillance patterns run weekly, monthly, quarterly or tri-annually. A disruption in one of these systems, such as a delay caused by heavy volumes, would have no impact on the market, nor would it impact overall regulatory effectiveness, unless downtime lasts several business or trade days. Thus, FINRA believes that it would be appropriate to apply a lower threshold, such as a shorter duration, for determining what constitutes a “significant” delay in a TRF system that provides real-time data to the market than it would for a market surveillance system that conducts surveillance on a T+1 basis. This is the approach FINRA currently takes under ARP.

Similarly, a systems compliance issue in a TRF could impact a member firm’s ability to comply with FINRA rules, for example, if a firm is required to submit a trade report to FINRA with a specific trade reporting modifier that is not supported by the TRF. Compliance issues in these systems could also potentially have market impact, for example, if a trade that is required by FINRA rules to be reported for non-media purposes is erroneously disseminated to the SIP because the TRF is processing non-media trade reporting modifiers incorrectly. By contrast, a compliance issue in a surveillance system that is not real-time may have no impact on member firms or the market.

A tiered approach would also take the differences in SCI systems into account for purposes of defining material systems changes. FINRA’s current tiered approach to reporting system changes under ARP has worked well by giving the Commission relevant information regarding important system changes.²⁶

II. SCI Events

A. General

FINRA supports the establishment of a regulatory framework with respect to the reporting of SCI events to help the Commission more effectively oversee SCI entities and

²⁶ For example, FINRA has adopted criteria for identifying material systems changes in its non-real-time market surveillance systems, including changes that result in 30% or greater increase above existing planned capacity, changes to application architecture or launches of a new service or system that require 12 man-months of effort or more to implement, and changes in the FINRA risk classification of one or more of the in-scope systems. Different criteria are applied for purposes of defining material systems changes in FINRA’s market facilities.

their systems. FINRA believes that having more clearly defined standards for reporting will also assist SCI entities in understanding and meeting their obligations. However, FINRA is concerned that some of the terms used in the definitions and examples of SCI events are ambiguous and the potential scope of the reporting, dissemination and corrective action requirements is too broad in certain respects, particularly if the definition of SCI systems is broadly interpreted to include non-market regulatory and surveillance systems. SCI entities will need to devote significant resources to ensure compliance with the reporting requirements, including automation of reporting systems, to the extent practicable, additional personnel to handle reporting and regular staff training. Accordingly, these requirements must be as clearly and narrowly drawn as possible to ensure the efficient and effective use of resources, both of the SCI entities required to report and the SEC staff analyzing and reviewing the reports.

B. Scope

1. The scope of reportable systems disruptions should be narrowed and clarified

Proposed Rule 1000(a) broadly defines systems disruption to include any event that results in the following: failure to maintain service level agreements or constraints; a disruption of normal operations, including switchover to back-up equipment with near-term recovery of primary hardware unlikely; a loss of use of any such system; a loss of transaction or clearance and settlement data; significant back-ups or delays in processing; a significant diminution of ability to disseminate timely and accurate market data; or a queuing of data between system components or queuing of messages to or from customers of such duration that normal service delivery is affected.

FINRA believes that many of the elements of this definition are vague and could be broadly construed to encompass events that would not be helpful to the Commission in its oversight of the securities markets. For example, a disruption of normal operations can vary from a momentary outage to degraded performance to a complete outage. FINRA believes that a substantial amount of “noise” would be generated by requiring that relatively minor disruptions, particularly those that would have no impact on normal systems operations or the market and market participants, be reported to the Commission. Without an exception for minor events, more important issues, such as those that have the potential for loss or warrant immediate regulatory attention, risk getting lost in the sheer volume of submissions and diminish the overall value of reporting.²⁷

For example, an SCI entity’s system may be programmed to routinely monitor for, detect and resolve issues or service disruptions within the day-to-day framework of the production environment. In addition, some systems include robust rewind capability to

²⁷ FINRA notes that the volume of submissions would be substantially increased if the reporting requirements under Regulation SCI also apply to non-market regulatory and surveillance systems.

allow recovery from network glitches. SCI entities dedicate significant upfront resources to address such events to ensure that there are seamless transitions to backup systems, making it part of the SCI entities' normal operations.²⁸ Where systems issues are addressed by an established procedure or workaround, such that there is no impact to the normal operations of the system, there would be little value in reporting such incidents to the Commission. Reporting should be reserved for those incidents that are novel, not prevented by existing monitoring tools and mechanisms, or the result of a gap or defect that impacts an SCI entity's ability to respond within its existing capabilities. Accordingly, FINRA requests that the Commission expressly exclude from the reporting requirements any systems disruption that is addressed in the normal course of the system's operations.

In addition, if the Commission does not expressly provide SCI entities with flexibility under Regulation SCI to adopt their own parameters for identifying and reporting systems disruptions that are appropriate for their systems, then the Commission needs to more clearly, and with greater specificity, define the various terms used in the definition of systems disruption. For example, the Commission states that the "loss of use" element would apply where a system is broken, offline, or otherwise out of service.²⁹ Thus, would it be appropriate to interpret this element to apply only to loss of use of the entire system?³⁰ How is "significant" defined with respect to a "significant diminution of ability to disseminate timely and accurate market data" or "significant back-ups or delays in processing?" What level of data loss would trigger notification, for example, would it be a certain percentage?

2. The scope of reportable systems compliance issues should be narrowed

Proposed Rule 1000(a) defines systems compliance issue as an event at an SCI entity that has caused any SCI system to operate in a manner that does not comply with the federal securities laws and rules and regulations thereunder or the SCI entity's rules or governing documents, as applicable.

FINRA believes that systems compliance issues should be reportable only if they would directly impact the market or a member firm's ability to comply with FINRA rules.

²⁸ FINRA considers a switchover to backup equipment for some systems to be a normal part of daily business operations, and tests could demonstrate that the availability of SCI systems is seamless following such equipment failures.

²⁹ See 78 FR at 18101.

³⁰ There may be occasions where a minor function of a system, e.g., a search function, may be unavailable, but loss of that single function would not affect the market or the SCI entity's business or regulatory effectiveness. FINRA does not believe that such an event should be reportable.

FINRA does not believe that systems compliance issues that are only momentary with no market impact should be reportable.

3. The scope of reportable systems intrusions should be narrowed

Proposed Rule 1000(a) defines systems intrusion as any unauthorized entry into SCI systems or SCI security systems.

FINRA believes that systems intrusions should be reportable only if they would have a material impact on the SCI system(s) or a direct impact on the market or market participants. The Commission has indicated that while the definition of a systems intrusion would not include unsuccessful attempts at entry, an intrusion could include the introduction of malware.³¹ Malware hits FINRA's desktop computers and laptops every day and a small percentage of machines become infected each month; however, FINRA software controls generally successfully quarantine the malware and prevent spread and damage to other systems. Such an event could be considered a systems intrusion because the malware is detected and quarantined only after reaching the equipment (this assumes that SCI security system is defined broadly to include laptops and desktop computers).³²

If the Commission does not narrow the reporting requirement to only systems intrusions that have a material impact, FINRA recommends that SCI entities be permitted to report minor and innocuous, but potentially frequent, intrusions, such as malware, on an aggregated (e.g., quarterly) rather than individual basis.

C. Reporting Requirements (Timing and Information)

1. General

FINRA fully supports the Commission's goal of ensuring that Commission staff is informed of events that could potentially impact the market. FINRA also supports the Commission's approach in providing flexibility to SCI entities to immediately notify the Commission of SCI events via email or telephone and to follow-up with formal written notification after some period of time. However, FINRA is concerned that SCI entities may have difficulty meeting some of the proposed reporting requirements – both in terms of timing and information – and urges the Commission to balance the need for prompt

³¹ See 78 FR at 18103.

³² Under the broadest possible interpretation, FINRA would be required to notify the Commission several times per day (as malware is detected and quarantined). A narrower interpretation (e.g., where notification is required only in the event that it bypasses quarantine and manual clean-up is required) would result, on average, in approximately three or four reportable events per month; however, these intrusions would have no impact on SCI systems. Finally, if we were required to report an intrusion only where there is a material impact (e.g., data corrupted or exposed), then we would expect to have no more than one or two reportable events per year in this category.

reporting against the burdens placed on SCI entities. Some complex outages can take up to several days to triage, isolate and begin to resolve. FINRA's experience with ARP outage reporting has shown that it can take several days to confirm the root cause of an outage and even longer to determine the appropriate resolution and how long it will take to complete. Thus, we believe that flexibility in terms of timing, as well as informational requirements, is crucial, particularly given that each systems issue, as well as the steps needed to investigate and resolve the issue, is unique. A "one size fits all" framework will not work.

2. A 24 hour written notice requirement is unduly burdensome and may hinder an SCI entity's ability to investigate and correct systems issues

FINRA does not believe it is reasonable to expect SCI entities to complete a written submission to the Commission on Form SCI within 24 hours of becoming aware of an SCI event, when the information that is available might be sparse and SCI entity personnel will be devoting their time to correcting the problem. This requirement fails to recognize the practical reality that an SCI entity's first priority is (and should be) to get the system(s) back up and running with emergency fixes and interim measures, and only after that is completed, to begin a more in-depth root cause analysis. Onerous reporting requirements could hinder an SCI entity's ability to investigate and correct systems issues quickly, given that the same personnel working on addressing the issues likely would be needed to complete the Form SCI. FINRA believes that in a worst case scenario, these requirements could have the unintended consequence of requiring SCI entities to have "shadow staff" on hand solely for reporting SCI events as the need arises, so as not to divert staff away from working to resolve the issue. This would result in a significant added cost to SCI entities.

Preparation of the Form SCI will take a fair amount of time, not just to compile information about the SCI event, but also to review and edit the written submission. Technology and operations staff are the best source of information about the SCI event, but additional layers of review would be required to provide reports in "plain English," as well as to assess and describe the business impact of the outage. Further impediments to timely reporting may arise where an issue requires cross-department coordination (e.g., to assess the types and number of market participants potentially affected by the SCI event) or coordination with a joint facility or regulatory services agreement ("RSA") client (e.g., where a disruption in a FINRA system is caused by a problem with a data feed supplied by the client). The written notification process will take even more time where a third party's technical and data personnel are relied on to provide initial drafts or where an RSA client requests that it have the opportunity to review all written notices before they are submitted.

3. Even the minimum required information may not be known or confirmed within 24 hours

FINRA appreciates the Commission's recognition that SCI entities will not have complete information within 24 hours of becoming aware of an SCI event. However, FINRA believes that in some instances, an SCI entity may not be able to satisfy even the minimum information requirements under Regulation SCI within 24 hours.³³ The SCI entity may not even know the date and time the SCI event started within the first 24 hours. In addition, the information that is available within 24 hours may not have been fully vetted, confirmed or analyzed, and it may change as more details regarding the issue and root cause are uncovered. FINRA believes that it is wasteful to expend staff time to make the initial submission based on information that will have to be reviewed and confirmed for accuracy – and possibly revised – as additional and more reliable information is uncovered. These valuable resources would be better spent working to analyze and resolve the issue. Moreover, information submitted prematurely to the Commission without sufficient vetting ultimately could prove unreliable. Although the information would be updated or corrected at a later date, it is unclear what value there would be in the Commission receiving potentially unreliable information within 24 hours.

FINRA believes that if SCI entities are required to submit formal written notification within 24 hours of becoming aware of an SCI event, then there should be no minimum information requirements, i.e., SCI entities should be permitted to provide whatever information they believe is sufficiently reliable at that time. This would save SCI entities from having to take the extra step of later confirming and possibly correcting information that was preliminarily provided. Alternatively, FINRA requests that the Commission expressly provide that the initial written submissions are to be made on a best efforts basis and SCI entities will incur no liability or penalty for any unintentional inaccuracies or omissions contained in these submissions.

4. A more flexible approach to reporting is recommended

FINRA requests that the Commission adopt a more flexible reporting framework that would require immediate reporting via e-mail or telephone (as currently proposed) and give SCI entities more time to submit the formal written notification on Form SCI. One approach would be to require submission of written notification within a specified period, e.g., 24 to 48 hours, after final resolution (rather than awareness of the occurrence) of the SCI event. If an SCI event has not been fully resolved within a reasonable period, e.g., 10 or 15 days, an SCI entity could be required to submit written notification based on currently available information at the end of that period, with periodic status updates via

³³ Specifically, an SCI entity will be required to provide all pertinent information known about the SCI event, including a detailed description of the SCI event; a current assessment of the types and number of market participants potentially affected; the potential impact on the market; and a current assessment of the SCI event, including whether it is a dissemination SCI event. *See* proposed Rule 1000(b)(4)(iv)(A)(1).

telephone or email, and a final written submission within 24 to 48 hours after the event has been fully resolved.³⁴ This is generally consistent with the approach that FINRA currently takes with respect to reporting outages in its real-time market transparency facilities under ARP.

5. A more flexible approach to providing updates is recommended

FINRA is also concerned that the requirement to provide regular written updates on Form SCI could overtax an SCI entity's staff while they are investigating and resolving the SCI event. FINRA requests that the Commission provide clarification regarding its expectations in this regard and suggests that the Commission consider a more flexible approach, such as allowing SCI entities to provide updates via email or the telephone until the issue is resolved.

6. The requirement that notification be provided outside of normal business hours should be eliminated or narrowed

In its release, the Commission notes that if responsible SCI personnel were to become aware of an SCI event outside of normal business hours, then the SCI entity would be required to submit notification at that time, rather than at the start of the next business day.³⁵ FINRA does not understand the value in the Commission receiving notice during non-business hours, and it is not clear whether the Commission will be staffed to receive incoming notification (either via email or telephone) or whether the Commission's electronic form filing system ("EFFS") will accept Form SCI submissions during non-business hours. Given Regulation SCI's focus on the maintenance of fair and orderly markets, FINRA does not believe that waiting to report SCI events until normal business hours would hinder the goals of Regulation SCI.

As discussed in Section II.E, FINRA believes that it is appropriate to provide SCI entities sufficient time to investigate and consult with senior management before reporting an SCI event. Such consultation may not always be feasible outside of normal business hours. Accordingly, FINRA requests that the Commission clarify that where an SCI event is discovered outside of normal business hours, SCI entities have a minimum of

³⁴ Such a flexible approach would also recognize that a series of systems issues could be caused by a single release that has significant software or hardware changes. In such instances, it could potentially take much longer to identify and resolve all of the issues, and it might be reasonable and more efficient for an SCI entity to combine or group disruptions arising from a single release into a single notice, rather than making multiple ad hoc submissions.

³⁵ See 78 FR at 18118.

one full business day to report the event.³⁶ This would allow time for review by senior management and help to ensure the quality of the report. If the current requirement is retained, then FINRA asks that the Commission narrow its scope and identify specific SCI events in specific SCI systems that are sufficiently critical to warrant reporting during non-business hours.

7. Different reporting standards should apply to different types of systems

FINRA believes that the timing and information requirements for reporting should not apply uniformly to every SCI system and every SCI event. For example, where an SCI event occurs in a system that does not provide real-time data to the market, e.g., a system that is used for market surveillance on a T+1 (or greater) basis, or where an SCI event occurs in a market facility outside of market hours, immediate notification and prompt written follow-up, particularly within 24 hours of becoming aware of the event, would not be warranted and would impose an unnecessary burden on SCI entities. FINRA believes that the Commission should take into account such differences in systems and events when imposing reporting deadlines and informational requirements. Such an approach would result in a more appropriate and efficient allocation of resources for both the SCI entity and SEC staff.

8. Where third parties are involved in the operation of an SCI entity's systems, delays may be inherent in the reporting process, and it may not be clear which SCI entity has the reporting obligation

The definition of SCI systems broadly applies to "systems of, or operated by or on behalf of, an SCI entity," which could include systems operated by or on behalf of other SCI entities and systems operated by third party vendors not subject to Regulation SCI. The interconnectedness of trading and trade reporting facilities and the use of shared services and other network monitoring tools means that it may not always be clear how an SCI entity can satisfy its reporting obligations under Regulation SCI.

For example, where one of FINRA's technology service providers becomes aware of an SCI event in a FINRA system, FINRA must rely on the service provider for specifics on the technical aspects of the event. As a result, FINRA's ability to report within the prescribed time frames under Regulation SCI would depend in large part on the technology service provider.

³⁶ As discussed in Section II.C.4, FINRA believes that SCI entities should not be required to submit written notice on Form SCI until after resolution of the SCI event. In the alternative, FINRA recommends that SCI entities be given one full business day (rather than 24 hours) to report.

Similarly, the reporting responsibilities may not be clear in the context of an RSA between two SCI entities. For example, a FINRA client, which is also an SCI entity, experiences a delay in one of its systems that in turn causes a delay in a FINRA system, e.g., one used for surveillance under the RSA. FINRA believes that having both FINRA and its client report an SCI event could increase the “noise” and not provide much additional value. FINRA requests clarification on how such inter-SCI entity events should be reported (e.g., would a joint submission be permissible, recognizing that delays in the submission would be inevitable).

A third example is in the area of the FINRA TRFs. The front-end user interfaces of the TRFs are directly controlled by NASDAQ OMX (“NOMX”) and The NYSE Market (“NYSE”), as the Business Members, and are not owned or operated by FINRA.³⁷ These systems may also be an integral part of the exchange technology (e.g., NOMX’s ACT technology platform) and therefore, proprietary. Under ARP, NOMX and NYSE report outages in the TRF participant user interfaces directly to the Commission, with notification to FINRA. FINRA requests clarification on whether this reporting approach would be satisfactory under Regulation SCI.³⁸

Finally, a delay in the system of a third party (e.g., a vendor or member firm) could cause an SCI event in an SCI entity’s system. For example, a FINRA system’s data delivery could be delayed (or even if data delivery is timely, it could be based on stale data) due to a delay in data from a third party or vendor that is not subject to Regulation SCI. FINRA does not believe that an SCI entity should be responsible for reporting an SCI event caused by a third party unless there is a material impact to the market (e.g., if stale data is disseminated to the market) or the SCI entity’s ability to meet its service level agreements.

FINRA believes that SCI entities should have flexibility to adopt reasonable policies and procedures (1) addressing allocation of reporting responsibilities between SCI entities when more than one SCI entity is involved in any given SCI event, and (2) establishing standards for reporting SCI events caused by issues in vendor and other third party systems. Alternatively, FINRA requests that the Commission provide specific guidance in this regard.

³⁷ The TRFs are FINRA facilities and the user interface systems are subject to FINRA’s oversight and OTC jurisdiction.

³⁸ FINRA notes that from a practical standpoint, it may be extremely difficult and costly for FINRA to report SCI events with respect to the TRFs. For example, FINRA would likely be required to add dedicated FINRA staff on location at the TRFs, since the day-to-day operation of the TRFs is, by contract, the responsibility of the Business Members.

D. Dissemination SCI Events

1. The dissemination requirement for systems compliance issues should be narrowed

Proposed Rule 1000(a) defines dissemination SCI event as an SCI event that is a systems compliance issue; systems intrusion; or systems disruption that results, or the SCI entity reasonably estimates would result, in significant harm or loss to market participants.

FINRA agrees with the Commission's approach in providing SCI entities reasonable discretion in estimating whether a systems disruption has resulted, or would result, in significant harm or loss to market participants before triggering the dissemination requirement. FINRA believes that this standard should also apply to the dissemination of information relating to systems compliance issues. FINRA does not believe that members or market participants need or would benefit from notice regarding systems compliance issues that would not reasonably be expected to impact them, particularly in light of the stated goals underlying the dissemination requirement.³⁹

2. The dissemination requirement should not apply to systems intrusions, or in the alternative, should be narrowed

FINRA agrees with the rationale underlying the Commission's proposal to permit SCI entities to delay dissemination of information relating to systems intrusions, i.e., that dissemination could compromise the investigation or resolution of a systems intrusion. FINRA further appreciates the Commission's sensitivity to the fact that dissemination of too much detailed information regarding a systems intrusion may provide hackers or others with insight into the potential vulnerabilities of an SCI entity's systems.

However, FINRA is concerned about the public dissemination of any information, even summary information, relating to systems intrusions. FINRA believes that it would not be in the interest of (and potentially detrimental to) SCI entities to make public any information about successful systems intrusions. Confidentiality is crucial to prevent similar behavior and exposure. If market participants need to know about a systems intrusion, for example, if their data has been compromised following a breach, it would be more appropriate to notify the affected market participants on a confidential basis rather than through a widely-disseminated public notice. Public dissemination of information about intrusions in any SCI system would be unnecessary to achieve the stated goals of Regulation SCI.

³⁹ For example, the Commission notes that the dissemination requirement is designed to ensure that SCI entities provide the minimum detail that a member or participant would need to assess whether an SCI event affected or would potentially affect that member, and such information could assist members in making investment or business decisions based on disclosed facts rather than on speculation. *See* 78 FR at 18120.

Accordingly, FINRA believes that SCI entities should not be required to disseminate information relating to any systems intrusions.⁴⁰ Alternatively, FINRA suggests that the scope of dissemination SCI events be narrowed to apply only to intrusions that have resulted, or would result, in significant harm or loss to market participants.⁴¹

3. The dissemination requirement should be clarified

FINRA believes that SCI entities should only be required to notify those members and market participants that have been, or can reasonably be expected to be, affected by the SCI event. For example, information about an SCI event in a FINRA TRF would not need to be disseminated to FINRA members that are not TRF participants. FINRA requests that the Commission clarify that information about an SCI event need be disseminated only to the subset of affected (or potentially affected) members or market participants, and not more widely to the public or an SCI entity's membership.⁴²

E. Trigger for the Reporting, Corrective Action and Dissemination Requirements Relating to SCI Events

1. The definition of "responsible SCI personnel" is too broad

Proposed Rule 1000(a) defines responsible SCI personnel as, for a particular SCI system or SCI security system impacted by an SCI event, any personnel, whether an employee or agent, of an SCI entity having responsibility for such system.

FINRA believes that the scope of the definition of responsible SCI personnel is too broad for purposes of triggering the notification, dissemination and corrective action requirements relating to SCI events, given that the Commission has noted that the definition would encompass junior analysts with responsibility for monitoring an SCI system(s).⁴³ If junior analysts, or other non-managerial staff and contractors, are required to report SCI events without properly vetting the issue with senior staff or management, the problem may be misdiagnosed or miscommunicated. Such a broad trigger could

⁴⁰ FINRA notes that if an intrusion were to result in a systems disruption that could cause significant loss or harm, then information about the disruption (but not the intrusion itself) would appropriately be disseminated so that market participants could assess the impact on them.

⁴¹ This is consistent with our recommendation regarding the dissemination of information relating to systems compliance issues. Thus, if systems intrusions are not excluded altogether, then FINRA believes it is appropriate that the same standard apply to systems disruptions, systems compliance issues and systems intrusions for purposes of the dissemination requirement.

⁴² An SCI entity would have discretion to disseminate more widely, if it deems such wider distribution to be appropriate under the circumstances.

⁴³ See 78 FR at 18118.

result in a number of false positives: for example, SCI entities may unnecessarily report systems issues that a junior analyst erroneously believes rise to the level of an SCI event. It could also have a chilling effect: for example, junior staff could be reluctant to investigate a potential issue after hours because it might trigger a reporting obligation before there is time to consult senior staff. FINRA believes that SCI entities should be able to implement procedures and reporting processes that follow an appropriate chain of command and allow for the involvement of senior staff prior to triggering a reporting obligation to ensure that any given event is reportable, and if so, that it is reported properly.⁴⁴ Accordingly, FINRA recommends that the definition of responsible SCI personnel be revised to expressly apply only to senior staff or managers with decision-making authority for the SCI entity.⁴⁵

2. Awareness of an SCI event is too broad a trigger

FINRA believes that “awareness” of an SCI event should not trigger the corrective action, reporting and dissemination requirements. Such a standard is too amorphous and, broadly interpreted, could encourage reporting of potential SCI events or mere issues that are out of the ordinary and need to be explored further. FINRA believes that a more appropriate trigger would be when the SCI entity has a reasonable basis to believe that a reportable SCI event has occurred. This would afford SCI entities time to conduct an investigation to determine whether a systems issue does in fact constitute an SCI event before being required to take corrective action, report or disseminate information about the event.

III. Material Systems Changes

A. Scope

Proposed Rule 1000(a) broadly defines material systems change as a change to one or more (1) SCI systems that materially affects the existing capacity, integrity, resiliency, availability or security of such systems; relies upon materially new or different technology; provides a new material service or material function; or otherwise materially affects the operations of the SCI entity; or (2) SCI security systems that materially affects the existing security of such systems.

⁴⁴ An SCI entity’s written policies and procedures regarding its response to SCI events, including any plan that lays out possible courses of action, chains of command and responsibilities of personnel, must be flexible enough to ensure that resolution of the issue is not hindered or delayed. Such a plan should include formal steps for evaluation, decision-making and reporting.

⁴⁵ FINRA recognizes the importance of all staff understanding and applying Regulation SCI, including the reporting requirements thereunder. We would expect to incorporate as part of our policies and procedures training of junior personnel on, among other things, identifying and escalating to senior staff potential SCI events.

Many of the terms used in this definition and the examples provided in the release⁴⁶ are vague and overly broad. “Material” – without further clarification – does little to narrow the scope of terms such as capacity, integrity, resiliency, availability, security, service or function. This standard could result in a significant increase in reported systems changes that FINRA does not believe are relevant to the Commission’s oversight of the securities markets. For example, with respect to the introduction of new business functions or services, nearly every release implements new functions, and as a result, nearly every release could potentially trigger the 30-day advance notification requirement. In addition, with respect to reconfigurations of systems that would cause a variance of greater than five percent in throughput or storage, five percent is a very low threshold.

If SCI entities will not be provided flexibility under Regulation SCI to establish reasonable standards for defining material systems changes for their systems, then FINRA requests that the Commission provide specificity with respect to the terms used in the definition and provide guidance on defining “material.”

B. Reporting Requirements (Timing and Format)

Under Regulation SCI, systems change reporting is likely to evolve in complexity and require considerably more resource investments to automate or manually track metrics that feed into these reports. Depending on the level of detail and reviews required, SCI entities may incur increased costs for generating these reports. Under the current ARP framework, FINRA and other SROs have latitude with respect to reporting material systems changes – both in terms of timing and content. However, Regulation SCI requires a one-off approach to reporting planned systems changes, by requiring at least 30 days advance notice (with a status report regarding such changes every six months).

FINRA recommends that SCI entities be given flexibility to determine the timing and format for reporting material systems changes. For example, FINRA’s current practice under ARP is to submit a quarterly report that covers both planned changes for the upcoming quarter as well as changes that were completed in the prior quarter. This practice has proven to be effective in keeping Commission staff apprised of planned and completed systems changes. FINRA believes that streamlining the reporting process and reducing the number of individual submissions made to the Commission would be less burdensome for SCI entities and more helpful to Commission staff reviewing the submissions.

⁴⁶ See 78 FR at 18105 – 18106.

IV. Form SCI

A. Implementation

1. SCI entities need time to learn the new form submission process

FINRA supports the Commission's efforts to bring uniformity to the notification submission process, which would ensure that the Commission is provided a comprehensive set of data on SCI events and allow the Commission to analyze such data. However, FINRA is concerned about being able to meet the more stringent reporting time frames and information requirements under Regulation SCI while learning the new electronic Form SCI submission process. Of particular concern is the Commission's statement that Form SCI will not be considered filed unless it complies with applicable requirements.⁴⁷

FINRA requests that the Commission provide SCI entities sufficient time to learn the new Form SCI submission process, and specifically recommends that the Commission delay implementation of Form SCI until SCI entities and Commission staff have gained experience with the Regulation SCI reporting requirements. In the alternative, FINRA recommends that the Commission provide a transition period for SCI entities to establish their processes for submission of the new Form SCI. For example, during the transition period, the Commission could extend the reporting time frames or allow SCI entities to satisfy their Regulation SCI reporting obligations using current processes (e.g., submission of their own form of notice via secure email), with submission of Form SCI on a delayed basis.

2. Data format

FINRA notes that the uniform format and added detail required by Form SCI will necessitate the expenditure of additional time and resources to complete each submission. In response to the Commission's Question #169 regarding whether the Commission should mandate that Form SCI and its exhibits employ a particular structured data format, e.g., XML or XBRL, FINRA believes that such a requirement could add unnecessary complexity to the process and require SCI entities to expend even more resources on reporting. Accordingly, FINRA would like to better understand the formats that the Commission is considering so that we can comment more specifically. At a minimum, SCI entities should be provided ample time to gain experience and comfort with the Form SCI submission process before such an additional requirement is imposed.

B. Technical Questions

FINRA requests clarification of a number of technical aspects of Form SCI:

⁴⁷ See 78 FR at 18180.

- As discussed in Section II.C.3, some of the information that would be required within 24 hours may not be available or known (e.g., the date and time the SCI event started may not be known within 24 hours).
 - Would a Form SCI submission be rejected if certain elements of information are missing? If so, the Commission is requested to specifically identify what missing information (or other defect) would cause the submission to be rejected.
 - If a Form SCI submission is rejected for incompleteness, and the SCI entity is unable to resubmit within the applicable reporting time frame, would the Commission deem this to be a failure to comply with Regulation SCI? FINRA is concerned that if certain information is required before a Form SCI submission will be accepted, SCI entities might be encouraged to guess where they do not have complete information.
- Currently, FINRA submits notifications and reports to ARP with FOIA exemption requests, and each production includes the necessary FOIA letter and is bates stamped and encrypted. This is a cumbersome, but necessary, process. Would submissions via Form SCI be subject to a blanket FOIA exemption request, and if not, how could SCI entities preserve the confidentiality of sensitive information about their systems? In the interest of time and to the greatest extent practicable, FINRA recommends a streamlined reporting framework with as few additional steps as possible required for completing submissions to the Commission.
- How would SCI entities update or correct information that they previously provided on Form SCI? As discussed in Section II.C.3, if the requirement to report within 24 hours of becoming aware of an SCI event is retained, there is a very real possibility that information provided in the initial submission will need to be later corrected or amended. FINRA is concerned that the updating process could be overly cumbersome, particularly if SCI entities will be required to specifically identify, document or explain the reason for any changes to information that was previously provided. FINRA also requests that the Commission confirm that an initial submission that is later corrected or amended would still be considered properly and timely filed.
- The Commission has indicated that SCI entities' reporting obligations apply during non-business hours. Will the EFFS system be available for Form SCI submissions during non-business hours?
- Is there an alternative means by which SCI entities will be able to submit notification if the EFFS system is down or otherwise unavailable?

- FINRA requests clarification regarding the item in Section 1 of the Form relating to the estimated number of market participants impacted by the SCI event. Would it be appropriate for SCI entities to assume that this generally will be “not applicable” or zero for internally-facing systems?
- FINRA requests clarification regarding Commission staff who will be reviewing Form SCI submissions. Will they be technical and operational staff who are familiar with systems jargon and “technology speak?” SCI entities need to know the intended audience so they can ensure that their submissions can be understood by the reader. As noted in Section II.C.2, the more that technical notifications and reports need to be translated into “plain English,” the slower the submission process will be.
- FINRA requests that the Commission clarify whether SCI entities will be expected to attach documentation relating to SCI events to support the descriptions provided in the exhibits, and if so, specifically identify such documentation.

C. Suggested “Business Impact” Category

FINRA notes that there is nothing in the current Form that would give the reader a sense of the severity or impact of an SCI event outside of the estimated number of market participants impacted (which could be “not applicable” or zero for internally-facing systems). FINRA was recently asked by ARP staff to add a business impact rating of high, medium or low in current outage reports for FINRA Market Regulation’s surveillance systems. This was requested because the outage duration for these systems often may be much longer than the duration of outages for real-time market facilities (e.g., FINRA TRFs) and exchanges. The business impact rating helps to provide context, for example, where a system has been unavailable for several weeks, but the business impact is low because there is an alternative means to get the information.⁴⁸ FINRA suggests that the Commission consider adding an estimated Business Impact category to Form SCI.

V. Policies and Procedures Requirements

A. Capacity, Integrity, Resiliency, Availability and Security

1. SCI industry standards

FINRA supports the Commission’s approach in providing SCI entities flexibility to identify appropriate policies and procedures that would meet the articulated standard

⁴⁸ The business impact would vary based on a number of factors, including whether there is an alternative means for users to perform their functions; whether the impacted system is real-time or T+1 (or greater); and whether the whole system or just one function is down.

under Regulation SCI.⁴⁹ FINRA also appreciates the Commission's guidance that an SCI entity's policies and procedures would generally be deemed to satisfy Regulation SCI if they are consistent with SCI industry standards.⁵⁰

However, FINRA notes two concerns with the SCI industry standards publications that the Commission has included in Table A in its release. First, there are competing industry standards that are equally comprehensive, but provide greater specificity and may ultimately be less burdensome to adopt than the publications identified in Table A. For example, open industry standards, such as ISO 27000-series, are not included. FINRA recommends that the ISO 27000-series standards be included to make it clear that there is an alternative to NIST 800-53. In addition, the referenced NIST standards do not set specific standards in most areas and instead are a standards framework, i.e., these standards establish the need, but leave it to the organization, to adopt specific policies and controls appropriate to their mission. Thus, without additional guidance regarding any specific expectations that the Commission might have in this area, there may still be considerable uncertainty regarding whether an SCI entity's policies and controls comply with Regulation SCI.

A possible alternative would be for the Commission, in consultation with FINRA and other SCI entities, to develop a set of suggested best practices, which could be informed, as appropriate, by the identified SCI industry standards. Under such an approach, an SCI entity's policies and procedures that are consistent with the suggested best practices would be deemed to be in compliance with Regulation SCI.⁵¹

Because compliance with the identified SCI industry standards would not be the exclusive means by which to satisfy Regulation SCI, FINRA requests that the Commission provide guidance regarding how Commission staff would make a determination regarding whether an SCI entity's policies and procedures comply with Regulation SCI, where those policies and procedures are not consistent with these standards.

2. Additional guidance is needed on the policies and procedures requirements

FINRA generally supports the Commission's approach in not prescribing specific policies and procedures that SCI entities must adopt. However, we are concerned that,

⁴⁹ Specifically, an SCI entity's policies and procedures must be reasonably designed to ensure that its SCI systems have levels of capacity, integrity, resiliency, availability and security adequate to maintain the entity's operational capability and promote the maintenance of fair and orderly markets. *See* proposed Rule 1000(b)(1).

⁵⁰ *See* proposed Rule 1000(b)(1)(ii).

⁵¹ Consistent with the Commission's current proposal, this would not be the exclusive means to comply with Rule 1000(b)(1).

without further clarification, the broad scope of the policies and procedures requirements under Regulation SCI could be burdensome, in terms of the cost of developing and implementing new (or enhancing existing) policies and procedures,⁵² as well as the cost of complying and documenting compliance with such policies and procedures. Significant expertise would be required in technical writing and capacity planning; familiarity with the design, software, hardware and testing of systems and operations; and an understanding of process as well as regulatory compliance. These requirements could significantly increase technology project costs (e.g., for testing, monitoring and compliance staff) and would significantly prolong the systems development life cycle (“SDLC”) and time to market.⁵³ Because many of the SCI industry standards do not provide specific standards, FINRA recommends that the Commission provide more clarity or, as mentioned above, identify a set of best practices in this regard.⁵⁴

3. Where more than one SCI entity is involved in the operation of an SCI system, it may not be clear how an SCI entity can satisfy its obligations

As discussed in Section II.C.8, the interconnectedness of systems and the use of third party or shared services may make it difficult for an SCI entity to determine how to satisfy its obligations under Regulation SCI. For example, in the TRF area, NOMX and NYSE, as the Business Members, have policies and procedures in place (subject to FINRA oversight) relating to the front-end user interfaces of the TRFs. FINRA believes that SCI entities should have flexibility to adopt reasonable policies and procedures addressing allocation of responsibilities between SCI entities when more than one SCI entity owns or operates the same SCI system and have potentially joint or overlapping obligations. Alternatively, FINRA requests that the Commission provide specific guidance in this regard.

⁵² FINRA has policies and procedures based on the systems development life cycle for many of its systems, including but not limited to those that are currently in scope for ARP purposes. Nonetheless, there may be a number of gaps between what is currently in place and what would be required under Regulation SCI, including potentially more rigorous standards for design review processes, coding requirements, integration testing, formal stress or load testing and production testing.

⁵³ For example, overly rigorous standards for systems testing could limit an SCI entity’s ability to quickly react to changing operating, technology and market needs. However, FINRA recognizes that the counter-argument would be that the slowdown is necessary to ensure that untested or poorly tested software does not get into production.

⁵⁴ For example, it is unclear what would be required in terms of the extent and frequency of capacity planning or testing standards. FINRA notes that it would be practically impossible to comprehensively parallel test real-time transaction environments (e.g., the FINRA TRFs) during migrations because there must be a hard cut-over given the transaction volume and real-time nature of the market and transaction reporting.

B. Requirements for the Safe Harbor

1. General

FINRA supports the Commission's inclusion of an explicit safe harbor in recognition of the complexity of SCI systems and breadth of the federal securities laws and SCI entity's own rules.⁵⁵ FINRA believes that a safe harbor could assist SCI entities in understanding how to comply with the requirement that they have policies and procedures reasonably designed to ensure that their SCI systems operate in the manner intended, including in compliance with the federal securities laws and the SCI entity's own rules. However, FINRA believes that many of the safe harbor requirements are too vague and potentially too broad. Without further guidance, it will be difficult for SCI entities to determine how to qualify for the safe harbor. FINRA requests that the Commission clarify and narrow the requirements, including but not limited to the requirements discussed below, to the greatest extent possible.

2. The requirements relating to systems testing are unclear and potentially overly burdensome

The requirement that SCI entities have policies and procedures reasonably designed to provide for periodic testing of all systems and systems changes after implementation is not clear, and depending on the scope of the requirement, could be quite burdensome. For example, a functional regression test is generally executed fully or partially (for purposes of testing key functionality)⁵⁶ in connection with a release. FINRA does not believe that subsequent stand-alone regression testing, i.e., that is not tied to a release, should be required. Such a requirement could increase program testing costs by as much as 50%. Furthermore, FINRA is concerned about the potential impact of overly rigorous testing requirements on an SCI entity's ability to respond to SCI events in real-time transaction environments. It may not be practical for an SCI entity to conduct extensive testing where emergency fixes need to be implemented quickly.

3. The requirement relating to ongoing systems monitoring is unclear and potentially overly burdensome

For purposes of the requirement that SCI entities have policies and procedures reasonably designed to provide for ongoing monitoring of the functionality of SCI systems, the terms "monitoring" and "functionality" are very general. For example, FINRA has job monitoring and server operations processes in place today, and FINRA believes that such processes should be sufficient to satisfy the requirements under Regulation SCI. However, "monitoring of the functionality of such systems to detect whether they are operating in the manner intended" is potentially quite broad and seems to suggest some

⁵⁵ See 78 FR at 18115.

⁵⁶ FINRA applies a risk-based approach to testing the components impacted by a release and may not conduct a full regression test for each release.

form of independent validation. FINRA does not believe that SCI entities should be required to develop and support parallel “watcher” systems, e.g., a separate system to ensure that trade report price validation is working correctly, which could double an SCI entity’s costs. A more flexible alternative would be to allow an SCI entity to rely on periodic reviews of its monitoring approach and make incremental changes through additional technology or operational solutions as needed. Such periodic reviews could, e.g., entail reviewing the trade report price validation logic annually to ensure the validation logic is comprehensive and remove redundancies.

4. The requirements relating to assessments by legal and compliance personnel are unclear and potentially overly burdensome

FINRA commends the Commission’s efforts to foster coordination between an SCI entity’s information technology and regulatory staff and to also help ensure that an SCI entity’s business interests do not undermine regulatory, surveillance and compliance functions and more broadly, the federal securities laws, during the development, testing, implementation and operation processes for SCI systems.⁵⁷ However, it is unclear what is required for purposes of satisfying the requirements that SCI entities have policies and procedures reasonably designed to provide for (1) assessment of SCI systems compliance by personnel familiar with applicable federal securities laws and rules and regulations thereunder and the SCI entity’s rules and governing documents, as applicable, and (2) review by regulatory personnel of SCI systems design, changes, testing and controls to prevent, detect and address actions that do not comply with applicable federal securities laws and rules and regulations thereunder and the SCI entity’s rules and governing documents, as applicable.

For example, ongoing assessment and review could require dedicated full-time compliance or regulatory personnel for every project. Alternatively, this could take the form of a formal Change Control Board for potentially every major project, with participation by business, technology, regulatory and legal personnel, where minutes and project decisions are documented and SDLC documents (requirements, design and test documents) are reviewed and approved by all interested parties. Today, FINRA briefs its executive management on these issues on a weekly basis. Would including legal and regulatory personnel in those briefings satisfy the requirements of Regulation SCI? Alternatively, is it the Commission’s expectation that an SCI entity’s regulatory and legal personnel would be involved more directly in day-to-day systems operations, for example, with site visits (as opposed to their involvement being limited to the design, development and change stages)?

FINRA believes that unless narrowed or clarified, these requirements could be burdensome and difficult to satisfy, and the review process to ensure ongoing compliance will prolong projects and increase project costs, without corresponding benefits. FINRA

⁵⁷ See 78 FR at 18116.

suggests that the requirements apply only in the competing market context, where there might be more of an independent structure established between business and regulatory units, and failure to comply with a rule might give a competitive advantage (e.g., to one SCI entity over another, or perhaps to the members of one SCI entity over another).

5. It is unclear how an SCI entity would satisfy the requirement that it “not have reasonable cause to believe that the policies and procedures were not being complied with”

It is unclear how an SCI entity would demonstrate that it did not have reasonable cause to believe that the applicable policies and procedures were not being complied with. For example, would SCI entities be expected to develop metrics and trend reports of previously reported and resolved incidents, along with root cause analysis results, to show that its policies and procedures were being followed? The Commission is requested to give guidance in this regard, including identifying the factors that Commission staff would take into consideration in determining whether an SCI entity has satisfied this requirement.

6. The safe harbor for individuals should be clarified and expanded beyond employees of the SCI entity

As an initial matter, we question the need for a safe harbor for individuals. We request that the Commission clarify whether it intends to hold an SCI entity’s staff personally liable for compliance issues and, if it intends to do so, explain the underlying rationale and the circumstances under which personal liability would apply.

In addition, Regulation SCI and the Commission’s release speak in terms of persons “employed by an SCI entity.”⁵⁸ In response to the Commission’s Question #103 in the release, FINRA believes that the safe harbor, if necessary, should apply broadly to include contractors and consultants that are retained by the SCI entity and provide support in designing, developing and testing SCI systems.

VI. Business Continuity and Disaster Recovery Plans and Testing

A. Business Continuity and Disaster Recovery Plans

1. The scope of the requirements should be clarified and narrowly construed

FINRA supports the Commission’s business continuity and disaster recovery (“BC-DR”) goals of next business day resumption of trading and two-hour resumption of clearance and settlement following a wide-scale disruption. However, an SCI entity’s ability to meet the BC-DR requirements will significantly depend on the scope of the requirements. If the scope is broad and includes a large number of systems with high standards for

⁵⁸ See 78 FR at 18116.

backup facilities, without consideration for the actual market or business need for those systems, the costs could be enormous. This further highlights the need for clarity and specificity regarding the scope of Regulation SCI generally and the BC-DR requirements in particular.

There is no discussion in Regulation SCI of the BC-DR requirements for other types of systems, i.e., systems that are not critical to the resumption of trading or clearance and settlement. FINRA does not believe that an SCI entity's BC-DR plans should be required to ensure next business day resumption of operations generally following a wide-scale disruption. For example, as discussed above in Section I.E.1, FINRA's real-time market facilities, e.g., the TRFs, have an RTO of one day, while FINRA's Market Regulation surveillance systems have an RTO of two, 14 or 30 days. Those systems with an RTO greater than one are not considered to be critical to the ability of the market to resume or continue operating following a wide-scale disruption. As such, BC-DR plans for those systems should not be required to ensure next business day resumption of operations. FINRA requests that the Commission clarify any BC-DR requirements for SCI systems other than trading and clearance and settlement systems, or alternatively, expressly provide that SCI entities have discretion to adopt emergency plans with recovery times that they deem appropriate for their systems.

2. The geographic diversity standard should be clarified

In response to the Commission's Question #72 relating to the geographic diversity standard, FINRA does not believe that the Commission should specify a minimum distance between an SCI entity's primary and backup sites. There are a variety of ways to achieve the Commission's goals, with even a relatively short distance between the two sites. However, FINRA requests that the Commission clearly articulate any specific expectations it might have in this regard. For example, are primary and backup sites required to be located in different power grids and use different telecommunications vendors? What are the staffing requirements for the backup location? Such requirements would impose significant additional costs on SCI entities and would necessitate an extended compliance period.

The *Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*,⁵⁹ which is discussed in the Commission's release, states, among other things, that backup sites should be as far away from the primary site as necessary to avoid being subject to the same set of risks as the primary location. FINRA notes that it has primary and backup sites in the New York / New Jersey area and the DC / Maryland / Virginia area, at a distance of approximately 250 miles. While this distance between sites is generally considered sufficient, Hurricane Sandy affected the entire East Coast. It would impose undue costs, including for data center migrations and reconfiguration of networks, to plan for such "storms of the century."

⁵⁹ See Securities Exchange Act Release No. 47638 (April 7, 2003), 68 FR 17809 (April 11, 2003).

B. Mandatory Testing

1. The scope of SCI systems included in the mandatory testing requirement should be clarified and narrowly construed

As discussed in Section VI.A.1, it appears that the requirements relating to the BC-DR plans that SCI entities must have in place apply only to trading or clearance and settlement systems. It follows that the requirements regarding annual coordinated BC-DR testing and participation by an SCI entity's members or participants would apply only to those systems as well. FINRA requests that the Commission confirm this interpretation.

FINRA is concerned that if the BC-DR testing requirements apply broadly and include such systems as non-real-time surveillance systems (or non-market systems), compliance on an annual basis would be overly burdensome. Significant coordination would be required to conduct industry-wide testing of real-time market facilities and non-real-time market surveillance systems, which would greatly increase the scope, complexity and resources necessary for testing. For example, FINRA Market Regulation currently tests its BC-DR capabilities separately from its market facilities, as their needs are post-trade and not same day, with well defined, independent interfaces.⁶⁰ If testing were to span multiple test dates, this could be a further significant impact on an SCI entity's resources and scheduling.

2. The scope of the required testing is potentially overly broad and the benefits may not outweigh the risks

FINRA believes that the scope of the required testing is potentially too broad and the potential costs and risks could be substantial. While it is generally optimal to conduct testing on weekends and other non-business days, testing at these times has its limitations. For example, combining performance testing (i.e., stress testing) with functional testing on weekends is difficult and possibly not feasible. An end-to-end functional test combined with a stress test would require much more time to accommodate processing volumes than would be afforded in an abbreviated non-business day session.⁶¹

While all broker-dealers can successfully test connectivity on the weekend, testing transaction traffic on non-business days has its own challenges. By design, financial

⁶⁰ FINRA Market Regulation currently does not require external parties or RSA clients to participate in BC-DR testing. Connectivity can be validated separately from BC-DR testing, and it is expected that such parties and clients have their own reasonable BC-DR plans in place. In addition, FINRA does not need participation by its member firms to test its BC-DR plans for systems that are internal-facing only.

⁶¹ Today, abbreviated testing sessions on non-business days are the current industry standard to minimize processing risks for the next business day.

transaction systems do not support non-business day trading activity (e.g., they are coded to validate for a business day execution date). Testing transaction traffic on the weekends would require that the business day validations be bypassed or ignored, which would decrease the value of testing, given the importance of these validations. In some cases, a new version of code may need to be developed, tested and released to bypass business day validations. This would significantly increase cost, as well as risk (e.g., if the new code is not backed out and the validations are bypassed in the production system). There are also practical challenges to testing the connection to DTCC for settlement purposes. For example, there is a very small window of time in which to run the end-to-end test during the weekend, because testing must conclude with ample time for the production systems to restore their files for the next business day.

FINRA also is concerned about the potential impact that extensive weekend BC-DR testing might have on our ability and resources to conduct routine maintenance and testing of day-to-day operations, which must take place on weekends.

However, while testing on non-business days has its challenges, testing during regular trading hours would pose significant risks to the market that would far outweigh the benefits of such testing. For example, there is the risk that test messages might inadvertently be disseminated in production. In addition, re-enabling and re-syncing an SCI production system could be difficult, risky and time-consuming, as it would have to be done in a controlled way so as not to lose data. Thus, in response to the Commission's Question #75, FINRA strongly recommends against adding a requirement that SCI entities test their backup capabilities during regular trading hours.

FINRA requests that the Commission clarify and narrow the scope of the testing requirements, taking these limitations and risks into consideration.

3. Designation of members to participate in testing could impose significant burdens on members

FINRA is concerned about the burdens that mandatory testing could impose on some of its member firms, particularly if the scope of the testing is broad and a large number of systems are included. The SIFMA industry-wide test in October is an end-to-end connectivity test only. While it may be feasible to coordinate industry-wide testing on the same day, firms would be required to have expertise on each trading desk, which would place major demands on their staff. In addition, if the same firms are selected by multiple SCI entities to participate in testing, they might face greater costs, such as maintaining sufficient bandwidth to send transaction traffic to the backup sites of multiple SCI entities.

In response to the Commission's Question #148, some firms may have the ability today to participate in testing, although some may have gaps with respect to bandwidth and connectivity to backup sites. FINRA currently conducts disaster recovery tests of all three major multi-product platform ("MPP") components with every major release;

however, participation by member firms is not mandatory.⁶² FINRA requests that the Commission balance the benefits of coordinated testing against the potential burdens on firms and limit the scope of the mandatory testing requirements as much as possible, consistent with the goals of Regulation SCI.

Finally, FINRA notes that the value of testing would be limited without participation by certain non-members, e.g., service bureaus and data vendors. Today, their participation in testing is entirely voluntary and based on good will. Would there be a way to ensure their participation under Regulation SCI?

VII. SCI Review of Systems

A. Definition of “SCI Review”

1. The requirement that SCI entities conduct an annual SCI review is inconsistent with a risk-based audit methodology

FINRA does not believe that the proposed requirement for performance of an SCI review for all SCI systems on an annual basis is reasonable, nor is it consistent with a risk-based audit methodology, which is the current standard used by FINRA,⁶³ as well as the standard primarily used by the Commission’s Office of Compliance Inspections and Examinations (“OCIE”) when it conducts examinations of FINRA and the other SROs to evaluate their and their member firms’ compliance with the Exchange Act and rules thereunder and SRO rules.⁶⁴

The definition of SCI review requires that the SCI entity’s review contain a risk assessment with respect to SCI systems, and under proposed Rule 1000(b)(7), the SCI review must be conducted not less than once each calendar year. This greatly expands the scope of the review required under ARP today and essentially eliminates the ability of FINRA Internal Audit (“IA”) to utilize its current risk assessment approach to determine the frequency of review for each system.

FINRA IA currently conducts reviews of FINRA’s technology systems based on an established risk assessment process and frequency model. For “core” technology

⁶² Generally, FINRA publishes a notice inviting participants, but participation by member firms and the scope of their participation, is not mandated. Participants can elect to test if they are able to connect to FINRA systems or they can run selected transactions through the system to test end-to-end connectivity.

⁶³ FINRA’s Internal Audit department adheres to the International Standards for the Professional Practice of Internal Auditing established by the Institute of Internal Auditors and also complies with the FFIEC’s Audit IT Examination Handbook, identified in Table A in the Commission’s release.

⁶⁴ See 78 FR at 18087.

processes and functions (e.g., technology governance, logical and physical security, data management systems), FINRA IA has a current audit frequency of once every two years. Certain core technology audits, such as change management, are performed annually; however, the audit scope varies from year-to-year based on the current view of risk. FINRA application systems are assigned to specific business area audits and are reviewed as part of a business process audit. The risk assessment and audit frequency for business area audits and associated business application systems range from annual to up to once every four years. The requirement under Regulation SCI for an annual SCI review also ignores FINRA's assessment of risk associated with each system or application (described in greater detail in Section I.E). FINRA IA takes this risk assessment into consideration in determining audit frequency.

Based on its current practice pursuant to the standards identified in note 63 herein, FINRA IA spends approximately 160 hours for each review of a technology application in connection with its regulatory audits, and currently it reviews between 10 and 13 market-related (e.g., market surveillance) technology applications annually. Accordingly, FINRA IA spends between approximately 1600 and 2080 hours annually on market-related technology application reviews.⁶⁵ If FINRA IA were to attempt to conduct all of the market-related technology application reviews that it currently conducts over four years during one year, it would increase the number of hours spent on these reviews to between approximately 6400 and 8320 hours. This would be a significant increase and would defeat the purpose of conducting such reviews pursuant to a risk-based audit methodology.

These resource estimates do not include regulatory technology applications such as those related to Member Regulation. FINRA notes that significantly more resources would be required to conduct the proposed SCI review on an annual basis if the definition of SCI systems is broadly construed to include non-market regulatory and surveillance systems and development and testing environments.

2. The required components of an SCI review are too broad

Under Regulation SCI, the annual SCI review must contain 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. Such review must also include penetration test reviews of the network, firewalls, development, testing and production systems at a frequency of not less than once every three years.⁶⁶ FINRA believes that this requirement is overly broad in that

⁶⁵ FINRA IA also conducts reviews of FINRA's non-regulatory functions (e.g., Human Resources and Finance) as well as more general applications underlying FINRA's entire technology portfolio. Thus, the overall amount of resources that FINRA IA expends in conducting its entire program of technology audits is significantly higher than the estimates set forth above.

⁶⁶ See proposed Rule 1000(a).

many of the processes identified in the definition of SCI review are not specific to SCI systems, but apply to all FINRA applications.

For example, FINRA IA has separate audits in its “audit universe” for information technology governance, systems development processes and logical and physical security controls. Under FINRA IA’s existing technology risk assessment process, these audits are performed every two years. It would be impractical and costly for FINRA IA to perform separate audits for technology processes (e.g., a security audit) for SCI systems on an annual basis while also performing a security audit for all other FINRA applications (those that are not subject to Regulation SCI) every two years. Requiring that SCI-specific reviews be performed each calendar year diminishes the benefits and more efficient resource allocations of using a risk-based approach.

B. Objectives and Intended Scope of the SCI Review

FINRA requests that the Commission provide greater specificity as to the objectives and intended scope of the SCI review. FINRA recommends that the Commission establish an “agreed upon procedures” approach with respect to SCI reviews. Such an approach would outline specific SCI review objectives and procedures to be performed by the objective reviewer (whether an SCI entity’s internal audit personnel or an outside firm). FINRA also recommends that the Commission leverage existing OCIE reviews of FINRA IA’s processes as a basis for reliance on IA’s work.⁶⁷

VIII. Access to SCI Systems

In its release, the Commission states that with access to an SCI entity’s systems, Commission representatives could test an SCI entity’s firewalls and vulnerability to intrusions.⁶⁸ However, it is not clear why the Commission would need hands-on access to an SCI entity’s systems. In addition, FINRA is concerned about providing remote access capabilities to any non-FINRA employee, including Commission staff, particularly with respect to systems that might house confidential information. FINRA requests that the Commission provide greater specificity regarding the access to SCI systems and SCI security systems that the Commission and its representatives would expect, including the means by which Commission staff would be given access and the controls the Commission would have in place to safeguard an SCI entity’s systems and data, as well as the rationale for such access.

IX. Implementation Period

Given the breadth of the requirements, FINRA requests that SCI entities be given an extended implementation period of no less than two years for SCI systems that are

⁶⁷ FINRA notes that FINRA IA provides the Commission with copies of its reports when requested by Commission staff.

⁶⁸ See 78 FR at 18130, note 284.

currently in scope for ARP inspection purposes and three years for all other SCI systems (and SCI security systems, to the extent that they are not excluded altogether).

In addition, FINRA recommends that, prior to implementation of Regulation SCI, Commission staff formally review and approve an SCI entity's list of systems that are deemed to be in scope for purposes of Regulation SCI. Although this list would change as systems are retired and new systems are developed, an initial review would significantly aid SCI entities in focusing their policies and procedures and reporting processes to prevent over- or under-reporting, and may also reduce potential issues during inspections. FINRA also believes that it would be helpful for SCI entities to be provided an opportunity to review their policies and procedures with Commission staff, recognizing that the Commission would not approve any such procedures, but would assist in proactively identifying any deficiencies before they are implemented and in operation.

X. Costs

FINRA estimates that its one-time costs to comply with Regulation SCI would be between approximately \$1.1 million and \$1.3 million and its ongoing annual costs would be between approximately \$4.5 million and \$5.5 million, if Regulation SCI is adopted as proposed (e.g., if SCI systems is broadly defined to apply to non-market regulatory and surveillance systems and development and testing environments). If Regulation SCI is more narrowly interpreted in accordance with FINRA's comments above (e.g., if non-market systems and development and testing environments are excluded from the definition of SCI systems), then FINRA's compliance costs would be significantly reduced: FINRA estimates that its one-time costs would be between approximately \$675,000 and \$825,000 and its annual costs would be between approximately \$2.2 million and \$2.6 million. These estimates do not include the costs for FINRA IA to conduct annual SCI reviews. Monetizing the hour estimates provided in Section VII.A.1, FINRA's compliance costs would increase by between approximately \$600,000 and \$900,000. FINRA IA's costs would be considerably higher if additional systems, i.e., more than the systems that are currently in scope under ARP, are subject to annual SCI reviews.

The estimated costs of compliance with Regulation SCI are significantly higher than FINRA's current maintenance costs to comply with ARP, e.g., outage notifications, systems change reporting and ARP inspections, which costs are approximately \$300,000 annually.⁶⁹

⁶⁹ We note that FINRA has been in compliance with the ARP guidelines for a number of years, and as such, this figure does not reflect the initial costs that were incurred, for example, in drafting policies and procedures and undertaking systems enhancements consistent with ARP guidelines.

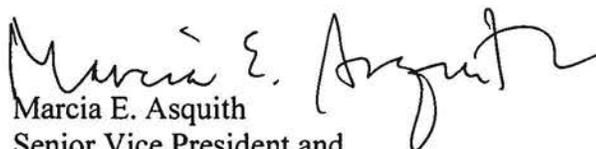
Ms. Elizabeth Murphy
July 8, 2013
Page 43 of 43

FINRA notes that these estimates are conservative and preliminary at best. As discussed above, FINRA has a number of questions regarding the scope of proposed Regulation SCI, and without clarification from the Commission on these questions, it is very difficult to assess the cost estimates provided by the Commission or to provide our own cost estimates. FINRA requests an opportunity to provide updated cost estimates after the Commission has clarified or narrowed the scope of the proposal.

* * * * *

Please contact Robert Colby, Chief Legal Officer, at (202) 728-8484, Stephanie Dumont, Senior Vice President and Director of Capital Markets Policy, at (202) 728-8176, or Lisa Horrigan, Associate General Counsel, at (202) 728-8190, if you would like to discuss FINRA's comments or have any questions.

Sincerely,



Marcia E. Asquith
Senior Vice President and
Corporate Secretary