WILMERHALE

Securities Alert

January 13, 2015 SECURITIES

SEC Adopts Regulation Systems Compliance and Integrity

A. Executive Summary

On November 19, 2014, the Securities and Exchange Commission ("Commission" or "SEC") voted unanimously to adopt proposed Regulation Systems Compliance and Integrity ("Reg SCI") under the Securities Exchange Act of 1934 ("Exchange Act"), as well as certain conforming amendments to Regulation ATS ("Reg ATS").[1] Reg SCI is intended "to strengthen the technology infrastructure of the U.S. securities markets, to improve its resilience, and to enhance the Commission's ability to oversee it."[2] The adoption of Reg SCI represents the Commission's latest action in its broader, ongoing efforts to strengthen and reform U.S. equity market structure.[3] As explained by SEC Chair Mary Jo White, Reg SCI "provide[s] greater accountability for those responsible for our critical market systems, helping ensure that such systems operate effectively and that any issues are promptly corrected and communicated to market participants and the Commission."[4]

As it explained when proposing Reg SCI in 2013, the Commission believes that high-speed, automated trading that occurs on national securities exchanges and alternative trading systems ("ATSs") has increased the potential for technological problems to broadly impact the equity markets.[5] The ramifications of such problems have been manifested in recent market events, the occurrence of which further encouraged the Commission to revisit U.S. equity market structure.[6] The Proposing Release outlined a framework that would replace the voluntary requirements of the SEC's existing Automation Review Policy ("ARP Program"),[7] and the system capacity, integrity, and security requirements of Rule

---

[1] Securities Exchange Act Release No. 73639 (Nov. 19, 2014), 79 Fed. Reg. 72252 (Dec. 5, 2014) (the "Adopting Release"). *See also* Securities Exchange Act Release No. 69077 (Mar. 8, 2013), 78 Fed. Reg. 18084 (Mar. 25, 2013) (proposing Reg SCI) (the "Proposing Release").

[2] Statement at Open Meeting on Regulation SCI, Mary Jo White, SEC Chair (Nov. 19, 2014).

[3] *See* Enhancing Our Equity Market Structure, Mary Jo White, SEC Chair (June 5, 2014) (outlining the SEC's efforts to enhance U.S. equity market structure by addressing market stability, high frequency trading, market transparency, broker conflicts, and market issues faced by small companies).

[4] SEC Adopts Rules to Improve Systems Compliance and Integrity, SEC Press Release 2014-260 (Nov. 19, 2014).

[5] Opening Statement at the SEC Open Meeting, Elise Walter, SEC Chairman (Mar. 7, 2013) (discussing the proposal of Reg SCI).

[6] Such events included, among others: the Flash Crash of May 6, 2010; systems issues that affected the initial public offerings of BATS Global Markets, Inc. and Facebook, Inc.; the hacking of systems of NASDAQ OMX Group; and the two-day market closure due to superstorm Sandy.

[7] The ARP Program, established by the Commission's two policy statements, each entitled "Automated Systems of Self-Regulatory Organizations," issued in 1989 and 1991, is a voluntary technology review program ("ARP I" and "ARP II," respectively). ARP I stated that SROs should establish comprehensive planning and assessment programs to test systems capacity and vulnerability, including annual reviews by an independent reviewer. In ARP II, the SEC further articulated its views on how SROs should conduct independent reviews. ARP II also addressed how SROs should notify the SEC of material systems changes and significant systems problems, and suggested the development of standards for meeting the ARP policy statements. The ARP Inspection Program was developed by the SEC to implement the ARP policy statements. All active registered clearing agencies, national securities exchanges, FINRA, one exempt clearing agency and one ATS participate in the program. *See* Securities Exchange Act Release Nos. 27445 (Nov. 16, 1989), 54 Fed. Reg. 48703 (Nov. 24, 1989) ("ARP I") and 29185 (May 1, 1991), 56 Fed. Reg. 22490 (May 15, 1991) ("ARP II").

301(b)(6) of Reg ATS, with mandatory uniform requirements relating to the automated systems of "SCI entities," which include certain self-regulatory organizations ("SROs"),[8] ATSs,[9] plan processors, and exempt clearing agencies subject to the ARP Program. The Proposing Release provided that SCI entities must, among other things:

- establish written policies and procedures reasonably designed to ensure that their systems have capacity, integrity, resiliency, availability, and security, and that they operate as intended;
- provide notice and reports to the Commission regarding certain systems-related events and take corrective action regarding such events, as necessary, and disseminate to members or participants information related to such events;
- mandate that members or participants participate in testing of business continuity and disaster recovery plans and coordinate testing on an industry- or sector-wide basis;
- conduct an objective annual review of their systems; and
- make, keep, and preserve certain books and records related to matters covered by Reg SCI.

In response to the concerns expressed in some of the 60 comment letters submitted regarding the Proposing Release that the scope of the proposal was unnecessarily broad and could be more tailored to lower compliance costs and still achieve the goal of reducing significant technology risk in the markets, the adopted, final rules reflect substantial changes from the original proposal. As a general matter, Reg SCI, as adopted, has been narrowed in numerous respects as the final rules use a risk-based approach and scaled back requirements to "provide the proper balance between requiring that the appropriate entities are subject to baseline standards for systems capacity, integrity, resiliency, availability, security, and compliance, while reducing the overall burden of the rule for all SCI entities."[10] Notable changes reflected in the adopted version of Reg SCI, and as described more fully below, include:

- tailoring various obligations based on the criticality of a system and based on the significance of an event by revising certain key definitions and introducing new defined terms;[11]
- eliminating a safe harbor from liability for an SCI entity if it implements policies and procedures reasonably designed to ensure that its systems operate in the manner intended (the final rules continue to include a safe harbor for certain individuals);
- narrowing the definition of "SCI ATS" to exclude ATSs that trade only municipal securities or corporate debt securities;
- replacing the proposed 30-day advance reporting requirement for material systems changes with a quarterly reporting requirement;
- eliminating the proposed requirement to permit the Commission to directly access an SCI entity's systems;
- requiring that an SCI entity submits a report evidencing its required SCI review to its senior management and board of directors;

[8] As discussed in Section B.1, Reg SCI applies to an SRO that is a national securities exchange, registered securities association, or registered clearing agency, or the Municipal Securities Rulemaking Board ("MSRB"). The definition excludes an exchange that is notice registered with the Commission pursuant to 15 U.S.C. § 78f(g) or a limited purpose national securities association registered with the Commission pursuant to 15 U.S.C. § 78o-3(k).
[9] As discussed in Section B.1.b, Reg SCI applies to significant volume ATSs that satisfy certain volume thresholds, and it does not apply to ATSs that trade only municipal securities or corporate debt securities.
[10] Adopting Release, *supra* note 1, at 72260.
[11] As described further below, adopted Reg SCI includes an amended definition of "SCI systems" and a new defined terms "critical SCI system," "indirect SCI system," and "major SCI event," all of which serve to narrow Reg SCI.

- limiting the set of SCI entity members and participants required to participate in mandatory business continuity/disaster recover testing; and

- refining the reporting framework for SCI events by using a scaled approach that takes into account the nature of the severity of a particular event.

Although the adopted version of Reg SCI does not broaden the definition of an "SCI entity," the Commission continues to indicate that it is considering an "SCI-like" framework that would apply more broadly to other market participants. Specifically, SEC Chair White "directed the [SEC] staff to prepare recommendations for the Commission's consideration as to whether an SCI-like framework should be developed for other key market participants, such as broker-dealers and transfer agents."[12] SEC Commissioner Aguilar supported a broader framework, particularly one that applies to key market participants, such as "broker-dealers, that operate proprietary trading platforms" and "broker-dealers and other entities that run proprietary trading algorithms."[13] These comments reflect the Commission's continued focus on reforming the equity markets and further regulating key market participants, such as market makers and those using high frequency and/or algorithmic trading strategies.

Reg SCI will become effective on February 3, 2015. SCI entities must comply with the rule by November 3, 2015, nine months after the effective date. ATSs that meet the volume thresholds in the definition of "SCI ATS" for the first time are permitted an additional six months from the time that they first meet the applicable volume threshold to comply with Reg SCI. SCI entities must comply with the industry or sector wide testing requirements by November 3, 2016.

B. Definitions and Key Terms (Rule 1000)

Final Rule 1000 sets forth a series of definitions designed to establish the scope of Reg SCI. In particular, the rule describes the entities, the systems of those entities, and events involving those systems that are subject to Reg SCI.

1. SCI Entities

The SEC has adopted the definition of "SCI entity" as proposed. Rule 1000 defines an "SCI entity" as an "SCI self-regulatory organization, SCI alternative trading system, plan processor, or exempt clearing agency subject to ARP."[14] Rule 1000 further defines each of these terms in turn, as discussed below.

a. SCI Self-Regulatory Organization

The SEC adopted the definition of "SCI self-regulatory organization" ("SCI SRO") as proposed. The definition of SCI SRO is consistent with the definition of SRO as set forth in Section 3(a)(26) of the Exchange Act, and therefore includes all national securities exchanges registered under Section 6(b) of the Exchange Act,[15] registered securities associations,[16] registered clearing agencies,[17] and the MSRB. However, the definition excludes an exchange that lists or trades security futures products that is notice-registered with the Commission as a national securities exchange pursuant to Section 6(g) of the Exchange Act, along with any limited purpose national securities association registered with the Commission pursuant to Section 15A(k) under the Exchange Act.[18]

b. SCI Alternative Trading System

---

[12] Statement at Open Meeting on Regulation SCI, Mary Jo White, SEC Chair (Nov. 19, 2014).
[13] Statement at Open Meeting on Regulation SCI, Luis A. Aguilar, SEC Commissioner (Nov. 19, 2014).
[14] Reg SCI, 17 C.F.R. § 242.1000 (2014); Adopting Release, *supra* note 1, at 72437.
[15] Currently, there are 18 registered national securities exchanges: BATS, BATS-Y, BOX, CBOE, C2, CHX, EDGA, EDGX, ISE, MIAX, Nasdaq OMX BX, Nasdaq OMX Phlx, Nasdaq, NSX, NYSE, NYSE MKT, NYSE Arca, and ISE Gemini. Note that this definition would also cover facilities of a national securities exchange, as defined in Section 3(a)(2) of the Exchange Act.
[16] Currently, the only registered securities association is FINRA.
[17] There are seven registered clearing agencies with active operations: DTC, FICC, NSCC, OCC, ICE Clear Credit, ICE Clear Europe, and CME.
[18] *See* Adopting Release, *supra* note 1, at 72260. These entities are security futures exchanges and the National Futures Association, for which the CFTC serves as their primary regulator.

The SEC adopted the definition of "SCI ATS" substantially as proposed with regard to ATSs trading NMS stocks and ATSs trading non-NMS stocks, but it added a six-month compliance period for entities satisfying the thresholds in the definition for the first time, as discussed below. However, the Commission determined to exclude from the definition ATSs that trade only municipal securities or corporate debt securities and, accordingly, such ATSs will not be subject to the requirements of Reg SCI. As part of the Adopting Release, the Commission also approved amendments to Reg ATS that would conform Reg ATS with Reg SCI, as discussed below.

The term "SCI alternative trading system" ("SCI ATS") means an ATS, as defined in Rule 300(a) of Reg ATS, which during at least four of the preceding six calendar months, had: (1) with respect to NMS stocks (i) five percent or more in any single NMS stock, and 0.25 percent or more in all NMS stocks, of the average daily dollar volume reported by applicable effective transaction reporting plans; or (ii) one percent or more, in all NMS stocks, of the average daily dollar volume reported by applicable effective transaction reporting plans; (2) with respect to equity securities that are not NMS stocks and for which transactions are reported to an SRO, five percent or more of the average daily dollar volume as calculated by the SRO to which such transactions are reported. Any SCI ATS that satisfies these volume thresholds is not required to comply with Reg SCI until six months after meeting the thresholds. The definition modifies the thresholds for complying with the capacity, integrity and security requirements currently in Rule 301(b)(6) of Reg ATS that apply to significant-volume ATSs that trade NMS stocks and non-NMS stocks, and moves the thresholds to Rule 1000 of Reg SCI.

As adopted, the final rule, with respect to NMS stocks, changes the volume threshold from the current Reg ATS requirement of 20% of average daily volume in any NMS stock such that an ATS that trades NMS stocks that meets either of the above-described alternative volume tests would be subject to the requirements of Reg SCI. The Commission believes that this threshold will identify those ATSs that could have a significant impact on the stock market as a whole, or that could have a significant impact on a single NMS stock and some impact on the NMS stock market as a whole at the same time. The Commission estimates that approximately twelve ATSs trading NMS stocks currently would exceed the thresholds and fall within the definition of SCI entity, accounting for approximately 66% of the dollar volume market share of all ATSs trading NMS stocks.[19] Moreover, the Commission believes that the thresholds appropriately include ATSs that have NMS stock dollar volume comparable to the NMS stock dollar volume of the equity exchanges that are subject to Reg SCI.

With respect to non-NMS stocks for which transactions are reported to an SRO, the Commission adopted the threshold as proposed. Thus, for such securities, an ATS will be subject to the requirements of Reg SCI if, during at least four of the preceding six calendar months, it had five percent or more of the average daily dollar volume as calculated by the SRO to which such transactions are reported. The Commission estimates that two ATSs currently would exceed this threshold and fall within the definition of SCI entity, accounting for approximately 99% of the dollar volume market share of all ATSs trading non-NMS stocks.[20]

The Commission, after considering the views of commenters regarding the unique nature of the current fixed income markets, determined to exclude ATSs that trade only municipal securities or corporate debt securities from the definition of SCI ATS.[21] Accordingly, such fixed-income ATSs will not be subject to the requirements of Reg SCI. Rather, fixed-income ATSs will continue to be subject to the existing requirements in Rule 301(b)(6) of Reg ATS regarding systems capacity, integrity and security if they meet the 20 percent threshold for municipal securities or corporate debt securities provided by that rule.[22]

The Commission agrees with commenters that it is appropriate to provide ATSs meeting the volume thresholds in the definition of SCI ATS for the first time a period of time before they are required to comply with Reg SCI. Thus, consistent with these comments, the Commission revised the proposed definition of

[19] *See* Adopting Release, *supra* note 1, at 72266.
[20] *See* Adopting Release, *supra* note 1, at 72269.
[21] However, Reg SCI applies to such activities if they are transacted on a national securities exchanges that qualifies as an SCI SRO.
[22] Note that the provisions in Reg ATS applicable to ATSs that trade municipal securities and corporate debt (Rule 301(b)(6)(i)(C) and (D)) will be re-designated as Rule 301(b)(6)(i)(A) and (B), respectively.

SCI ATS to provide that an SCI ATS will not be required to comply with the requirements of Reg SCI until six months after satisfying any of the applicable thresholds in the definition of SCI ATS for the first time.

c. Plan Processor

The SEC adopted the definition of "plan processor" as proposed. The term plan processor will have the meaning set forth in Rule 600(b)(55) of Regulation NMS, which defines a "plan processor" as "any self-regulatory organization or securities information processor acting as an exclusive processor in connection with the development, implementation and/or operation of any facility contemplated by an effective national market system plan."[23] Since a plan processor is not required to be an SRO, and the systems of such entities deal with key market data that are central features of the national market system, the Commission believes that such entities should be independently subject to the requirements of Reg SCI. Currently, this definition covers the Securities Industry Automation Corporation ("SIAC"), as the processor for the CTA, CQS and OPRA Plans, and Nasdaq, as the processor for the Nasdaq UTP Plan.

d. Exempt Clearing Agency Subject to ARP

The SEC adopted the definition of the term "exempt clearing agency subject to ARP" as proposed. This term is defined as "an entity that has received from the Commission an exemption from registration as a clearing agency under Section 17A of the Exchange Act, and whose exemption contains conditions that relate to the Commission's ARP program, or any Commission regulation that supersedes or replaces such policies."[24] This definition presently would apply to one entity, Omgeo Matching Services-US, LLC.

e. Other Entities *Not* Included in Definition of "SCI Entity"

The Commission declined to extend the definition of "SCI entity" to include a variety of other types or categories of market participants suggested by commenters, such as non-ATS broker-dealers. Instead, the Commission concluded that a "a measured approach that takes an incremental expansion from the entities covered under the ARP Inspection Program is an appropriate method for imposing the mandatory requirements of Regulation SCI at this time given the potential costs of compliance."[25] The Commission noted that this approach "will enable the Commission to monitor and evaluate the implementation of Reg SCI, the risks posed by the systems of other market participants, and the continued evolution of the securities markets, such that it may consider, in the future, extending the types of requirements in Reg SCI to additional categories of market participants, such as non-ATS broker-dealers, security-based swap dealers, investment advisers, investment companies, transfer agents, and other key market participants."[26] If the SEC decides to propose to apply some or all of the requirements of Reg SCI to additional types of entities, the Commission will issue a separate release discussing such a proposal and seeking public comment. As previously noted, SEC Chair White has directed the SEC staff to prepare recommendations for the Commission's consideration as to whether an SCI-like framework should be developed for other key market participants that are not included in the current definition of SCI entity, such as broker-dealers and transfer agents.

2. Relevant Systems: SCI Systems, Critical SCI Systems and Indirect SCI Systems

In the Proposing Release, Reg SCI would have applied to "SCI systems" and "SCI security systems." In response to comments that the proposed definitions of "SCI systems" and "SCI security systems" were too broad, the Commission determined to apply Reg SCI to a more targeted set of systems than initially proposed. Additionally, the adopted approach recognizes that some systems pose greater risk than others to the maintenance of fair and orderly markets if they malfunction. Accordingly, Reg SCI, as adopted, identifies three broad categories of systems that are subject to the regulation: SCI systems, critical SCI systems, and indirect SCI systems, with each category subject to differing requirements under Reg SCI.

---

[23] Regulation NMS, 17 C.F.R. § 242.600(b)(55) (2014).
[24] Reg SCI, 17 C.F.R. § 242.1000 (2014); Adopting Release, *supra* note 1, at 72436.
[25] Adopting Release at 72259.
[26] Adopting Release at 72259.

a. SCI Systems

In response to commenters, the Commission refined the scope of the systems covered by the definition of "SCI systems." As adopted, the term "SCI systems" means "all computer, network, electronic, technical, automated, or similar systems of, or operated by or on behalf of, an SCI entity that, with respect to securities, directly support trading, clearance and settlement, order routing, market data, market regulation, or market surveillance."[27] The adopted definition has been limited to apply to production systems that relate to securities market functions, and in particular to those six functions—trading, clearance and settlement, order routing, market data, market regulation, or market surveillance—that traditionally have been considered to be central to the functioning of the U.S. securities markets. The Commission believes that systems providing these six functions may pose a significant risk to the maintenance of fair and orderly markets if their capacity, integrity, reliability, availability or security is compromised, and therefore they should be covered by the definition of "SCI systems." SCI systems are subject to all provisions of Reg SCI, except for certain requirements applicable only to "critical SCI systems."

In light of comments, the adopted definition of SCI systems differs from the proposed definition in various ways, including: (1) the adopted definition clarifies that SCI systems are limited to only those systems that, with respect to securities, *directly support* the six aforementioned functions; (2) the reference to development and testing systems in the proposed definition has been deleted; and (3) the definition has been limited to those systems relating to market regulation and market surveillance, rather than including all regulation and surveillance systems (*e.g.,* those relating to member registration, capital requirements, or dispute resolution).

Despite comments to the contrary, the Commission, however, decided to retain the phrase "directly support" in the adopted definition in order to acknowledge that systems of SCI entities are complex and highly interconnected and that the definition of SCI systems should not exclude functionality or supporting systems on which the six identified categories of systems rely to remain operational. Additionally, systems of an "SCI entity" directly supporting proprietary market data or consolidated market data are both within the scope of the definition of "SCI systems" and subject to Reg SCI. Furthermore, the Commission rejected the recommendation of some commenters to exclude systems operated on behalf of SCI entities by third parties, noting that, if a system is operated on behalf of an "SCI entity" and directly supports one of the six key functions listed within the definition of "SCI system," it should be included as an "SCI system."[28]

b. Critical SCI Systems

In response to comment advocating for a risk-based approach, the Commission adopted a new term, "critical SCI systems," which is a subset of SCI systems that are subject to the highest level of requirements under Reg SCI. Guided significantly by commenters' views on those systems that are most critical, the Commission defined this term as "any SCI systems of, or operated by or on behalf of, an SCI entity that: (1) directly support functionality relating to: (i) clearance and settlement systems of clearing agencies; (ii) openings, reopenings, and closings on the primary listing market; (iii) trading halts; (iv) initial public offerings; (v) the provision of consolidated market data; or (vi) exclusively-listed securities; or (2) provide functionality to the securities markets for which the availability of alternatives is significantly limited or nonexistent and without which there would be a material impact on fair and orderly markets."[29] Systems in this category are those that, if they were to experience systems issues, the Commission believes would be most likely to have a widespread and significant impact on the securities markets, and therefore should be subject to the highest level of requirements.

---

[27] Reg SCI, 17 C.F.R. § 242.1000 (2014); Adopting Release, *supra* note 1, at 72437.

[28] The Commission notes that the term "SCI system" under Reg SCI is separate and distinct from the term "facility" in Section 3(a)(2) of the Exchange Act.

[29] Reg SCI, 17 C.F.R. § 242.1000 (2014); Adopting Release, *supra* note 1, at 72436. The latter category of critical SCI systems—those for which alternatives are significantly limited or unavailable—is intended to serve as a broad, catchall provision that accounts for future technological developments. As of the date of Reg SCI's adoption, the Commission is unaware of any systems that fall within this definition. Adopting Release, *supra* note 1, at 72279.

c. Indirect SCI Systems

The Commission replaced the proposed definition of "SCI security systems" with the adopted term "indirect SCI systems." The term "indirect SCI systems" means "any systems of, or operated by or on behalf of, an SCI entity that, if breached, would be reasonably likely to pose a security threat to SCI systems."[30] Indirect SCI systems are subject only to certain provisions of Reg SCI, including those related to establishing reasonably designed policies and procedures regarding security standards, system intrusions, material changes to system security, system reviews, and recordkeeping and electronic filing requirements.[31] In response to comments that the proposed term would cover too many systems unrelated to SCI systems, the adopted term excludes the phrase "share network resources" because it could be interpreted in a manner that would include almost any system that is part of an SCI entity's network. The Commission notes that the definition of indirect SCI systems will not include any systems of an SCI entity for which the SCI entity establishes reasonably designed and effective controls that result in SCI systems being logically or physically separated from such non-SCI systems. Thus, the universe of an SCI entity's indirect SCI systems is in the control of each SCI entity, and an SCI entity should reasonably expect Commission examination staff to assess its security controls around SCI systems. If these controls are absent or are not reasonably designed, the applicable non-SCI systems would be deemed indirect SCI systems and subject to the security standards and systems intrusions provisions of Reg SCI.

3. SCI Events

Certain types of events—SCI events—give rise to obligations under Reg SCI. Such obligations include, among others, taking corrective action, reporting to the Commission, and disseminating information to members or participants. The Commission adopted the definition of "SCI event" as proposed; thus, "SCI event" is defined as "an event at an SCI entity that constitutes: (1) a systems disruption; (2) a systems compliance issue; or (3) a systems intrusion."[32] Each of these three terms is defined further, as described below.

a. Systems Disruption

The Commission substantially modified the proposed definition of "systems disruption," defining the term in the final rule as "an event in an SCI entity's SCI systems that disrupts, or significantly degrades, the normal operation of an SCI system."[33] Agreeing with commenters' concerns that the proposed definition had the potential to be both over-inclusive and under-inclusive, the Commission removed the seven specific types of systems malfunctions that were included in the proposed definition. The Commission believes that the new approach sets forth a standard that SCI entities can apply in a wide variety of circumstances to determine, in their discretion, whether a systems issue should be appropriately categorized as a "systems disruption."

In shifting to a standards-based approach, the Commission notes that an SCI entity likely would find it helpful to establish parameters that can aid it in determining what constitutes the "normal operation" of each of its SCI systems, and when such "normal operation" has been disrupted or significantly degraded because those parameters have been exceeded.

b. Systems Compliance Issue

The Commission adopted the definition of "systems compliance issue" substantially as proposed, with certain modifications to refine its scope. Specifically, the SEC replaced the proposed definition's broad reference to federal securities laws with a reference to the Exchange Act. As adopted, "systems compliance issue" means "an event at an SCI entity that has caused any SCI system of such entity to operate in a manner that does not comply with the [Securities Exchange] Act and the rules and regulations thereunder or the entity's rules or governing documents, as applicable."[34] As noted in the Proposing Release, a systems compliance issue could, for example, occur when a change to an SCI

[30] Reg SCI, 17 C.F.R. § 242.1000 (2014); Adopting Release, *supra* note 1, at 72436.
[31] *See* Adopting Release, *supra* note 1, at 72281.
[32] Reg SCI, 17 C.F.R. § 242.1000 (2014); Adopting Release, *supra* note 1, at 72437.
[33] Reg SCI, 17 C.F.R. § 242.1000 (2014); Adopting Release, *supra* note 1, at 72437.
[34] Reg SCI, 17 C.F.R. § 242.1000 (2014); Adopting Release, *supra* note 1, at 72437.

system is made by information technology staff, without the knowledge or input of regulatory staff, that results in the system operating in a manner that does not comply with the Exchange Act, and the rules thereunder, or the entity's rules and other governing documents.[35]

c. Systems Intrusion

The SEC adopted the proposed definition of "systems intrusion," with one technical modification to replace the term "SCI security systems" in the definition with "indirect SCI systems." Therefore, as adopted, "systems intrusion" means "any unauthorized entry into the SCI systems or indirect SCI systems of an SCI entity."[36] This definition is intended to cover any unauthorized entry into SCI systems or indirect SCI systems, regardless of the identity of the person committing the intrusion (whether they are outsiders, employees, or agents of the SCI entity), and regardless of whether or not the intrusion was part of a cyber-attack, potential criminal activity, or other unauthorized attempt (whether intentional or inadvertent) to retrieve, manipulate, or destroy data, or access or disrupt systems of SCI entities.

C. Policies and Procedure of SCI Entities (Rule 1001)

1. Capacity, Integrity, Resiliency, Availability and Security

The Commission adopted Rule 1001(a) with modifications that it believes will better provide SCI entities with sufficient flexibility to develop their policies and procedures to achieve robust systems while also providing guidance on how an SCI entity may comply with the rule. Rule 1001(a) requires an SCI entity to "establish, maintain, and enforce written policies and procedures reasonably designed to ensure that its SCI systems and, for purposes of security standards, indirect SCI systems, have levels of capacity, integrity, resiliency, availability, and security, adequate to maintain the SCI entity's operational capability and promote the maintenance of fair and orderly markets."[37] Rule 1001(a)(2) sets forth minimum requirements for an SCI entity's policies and procedures, including:

- the establishment of reasonable current and future technological infrastructure capacity planning estimates;[38]
- periodic capacity stress tests of such systems to determine their ability to process transactions in an accurate, timely, and efficient manner;[39]
- a program to review and keep current systems development and testing methodology for such systems;[40]
- regular reviews and testing, as applicable, of the SCI entity's SCI systems and, for purposes of security standards, indirect SCI systems, including backup systems, to identify vulnerabilities pertaining to internal and external threats, physical hazards, and natural or manmade disasters;[41]

---

[35] For an SCI SRO, systems compliance issues would include SCI systems operating in a manner that does not comply with the SCI SRO's rules, as defined in the Exchange Act, and the rules thereunder. For a plan processor, systems compliance issue would include SCI systems operating in a manner that does not comply with an applicable effective national market system plan. For an SCI ATS or exempt clearing agency subject to ARP, a systems compliance issue would include SCI systems operating in a manner that does not comply with certain documents, such as subscriber agreements and any rules provided to subscribers and users and, for an ATS, described in its Form ATS filings with the Commission.

[36] Reg SCI, 17 C.F.R. § 242.1000 (2014); Adopting Release, *supra* note 1, at 72437.

[37] Reg SCI, 17 C.F.R. § 242.1001(a)(1) (2014); Adopting Release, *supra* note 1, at 72437.

[38] Rule 1001(a)(2)(i) (previously, proposed Rule 1000(b)(1)(i)(A)). Because the Commission intended this item to relate to capacity planning for SCI systems, rather than capacity planning more broadly (*e.g.,* in relation to an SCI entity's office space), the SEC added the word "technology" to the final rule.

[39] Rule 1001(a)(2)(ii) (previously, proposed Rule 1000(b)(1)(i)(B)). The Commission adopted the proposed language without amendment.

[40] Rule 1001(a)(2)(iii) (previously, proposed Rule 1000(b)(1)(i)(C)). The Commission adopted the proposed language without amendment.

- business continuity and disaster recovery plans that include maintaining backup and recovery capabilities sufficiently resilient and geographically diverse and that are reasonably designed to achieve next business day resumption of trading and two-hour resumption of critical SCI systems following a wide-scale disruption;[42]

- standards that result in the design, development, testing, maintenance, operation, and surveillance of such systems in a manner that facilitates the successful collection, processing, and dissemination of market data;[43] and

- monitoring of such systems to identify potential SCI events.[44]

Rule 1001(a)(3) requires each SCI entity to periodically review the effectiveness of the policies and procedures described above, and to take prompt action to remedy deficiencies in such policies and procedures.

Final Rule 1001(a)(4)[45] deems an SCI entity's policies and procedures reasonably designed if they are consistent with current SCI industry standards. Such SCI industry standards must be comprised of information technology practices that are widely available to information technology professionals in the financial sector and issued by an authoritative body that is a U.S. governmental entity or agency, association of U.S. governmental entities or agencies, or widely recognized organization. Compliance with such current SCI industry standards, however, will not be the exclusive means to comply with the requirements of this provision.

Rule 1001(a)(4) was adopted, subject to certain modifications. First, the final rule excludes the criterion in the proposal that a technology standard be available free of charge. Second, in response to significant comment, the SEC revised its approach to Table A, which, in the Proposing Release, listed the publication(s) that the Commission had preliminarily identified as SCI industry standards.[46] The Commission acknowledges that the proposed framework for identifying and updating publications on Table A may not be sufficiently nimble to assure that its list of publications does not become obsolete as technology and standards evolve. Therefore, rather than issuing Table A with the Adopting Release, the Commission determined that SEC staff should issue guidance to assist SCI entities in developing policies and procedures consistent with "current SCI industry standards" and periodically update such guidance as appropriate. Thus, concurrent with the Commission's adoption of Reg SCI, Commission staff issued guidance to SCI entities on developing policies and procedures consistent with "current SCI industry

---

[41] Rule 10001(a)(2)(iv) (previously, proposed Rule 1000(b)(1)(i)(D)). The Commission added the phrase "as applicable" to this provision to emphasize that the provision does not specifically require both regular reviews and regular testing in connection with an SCI entity's identification of vulnerabilities. Instead, the provision requires reviews or testing (or both) to occur as applicable, so long as the approach is effective to identify vulnerabilities in SCI systems, and indirect SCI systems, as applicable. Moreover, this adopted provision does not dictate the precise manner or frequency of reviews and testing, and does not prohibit an SCI entity from determining that there are methods other than reviews and testing that may be effective in identifying vulnerabilities.

[42] Rule 1001(a)(2)(v) (previously, proposed Rule 1000(b)(1)(i)(E)). The Commission revised the proposed version of this provision to: (i) specify that the stated recovery timeframes in Reg SCI are goals, rather than inflexible requirements; and (ii) provide that the stated two-hour recovery goal applies to critical SCI systems generally. In addition, the SEC adopted the geographic diversity requirement, which does not specify any minimum distance for an SCI entity's backup and recovery facilities, as proposed. The Commission continues to believe, however, that backup sites should not rely on the same infrastructure components, such as transportation, telecommunications, water supply, and electric power.

[43] Rule 1001(a)(2)(vi) (previously, proposed Rule 1000(b)(1)(i)(F)). The Commission adopted the proposed language without amendment.

[44] Rule 1001(a)(2)(vii). This new provision was added in response to comments that Reg SCI should allow entities to adopt and follow escalation procedures instead of providing that obligations under Reg SCI are triggered by one employee's awareness of a systems issue. This new requirement makes explicit that escalation of a systems problem should occur not only if a systems problem is identified by chance, but rather that an SCI entity should have a monitoring process in place so that systems problems may be identified as a matter of standard operations and pursuant to parameters reasonably established by the SCI entity.

[45] Previously, proposed Rule 1000(b)(1)(ii).

[46] The publications listed in Table A set forth industry standards that the SEC understood were currently used by information technology and audit professionals in the financial and government sectors.

standards."[47] The guidance lists publications describing processes, guidelines, frameworks, or standards that an SCI entity may consider in developing reasonable policies and procedures.

2. Systems Compliance

Final Rule 1001(b)(1)[48] requires each SCI entity to establish, maintain, and enforce written policies and procedures reasonably designed to ensure that its SCI systems operate in a manner that complies with the Exchange Act, and the rules and regulations thereunder, and the entity's rules and governing documents, as applicable.[49] In adopting this rule, with minor changes from the proposal,[50] the Commission emphasized that the occurrence of a systems compliance issue at an SCI entity does not necessarily mean that the SCI entity has violated Rule 1001(b), or that the SCI entity will be subject to an enforcement action.

The Proposing Release included a safe harbor from liability for SCI entities and persons employed by SCI entities.[51] In response to considerable comment, the Commission determined not to adopt the proposed safe harbor for SCI entities. Rather, Rule 1001(b)(2), as adopted, sets forth minimum elements based on the proposed safe harbor that an SCI entity must include in its systems compliance policies and procedures. These elements are:

- testing of all SCI systems and any changes to SCI systems prior to implementation;
- a system of internal controls over changes to SCI systems;
- a plan for assessments of the functionality of SCI systems designed to detect systems compliance issues, including by responsible SCI personnel and by personnel familiar with applicable provisions of the Exchange Act, and the rules and regulations thereunder, and the SCI entity's rules and governing documents; and
- a plan of coordination and communication between regulatory and other personnel of the SCI entity, including by responsible SCI personnel, regarding SCI systems design, changes, testing, and controls designed to detect and prevent systems compliance issues.

In recognizing that the precise nature, size, technology, business model, and other aspects of each SCI entity's business may vary, the Commission explained that the aforementioned minimum elements are intended to be general in order to accommodate such differences, and each SCI entity will need to exercise judgment in developing and maintaining specific policies and procedures that are reasonably designed to achieve systems compliance. Additionally, SCI entities should consider the evolving nature of the securities industry, as well as industry practices and standards, in developing and maintaining such policies and procedures. As such, the elements specified in Rule 1001(b) are non-exhaustive, and each SCI entity should consider on an ongoing basis what steps it should take in order to ensure that its policies and procedures are reasonably designed.

In contrast to its elimination of the safe harbor for SCI entities, the Commission determined to adopt the proposed safe harbor for individuals, albeit with certain modifications. Specifically, Rule 1001(b)(4)[52] states that personnel of an SCI entity shall be deemed not to have aided, abetted, counseled, commanded, caused, induced, or procured the violation by an SCI entity of Rule 1001(b) if the person: (1) has reasonably discharged the duties and obligations incumbent upon such person by the SCI entity's policies and procedures; and (2) was without reasonable cause to believe that the policies and procedures relating to an SCI system for which such person was responsible, or had supervisory

[47] SEC Staff Guidance on Current SCI Industry Standards (Nov. 19, 2014), *available at* http://www.sec.gov/rules/final/2014/staff-guidance-current-sci-industry-standards.pdf.
[48] Previously, proposed Rule 1000(b)(2)(i).
[49] Rule 1001(b)(3) requires each SCI entity to periodically review the effectiveness of the policies and procedures required by Rule 1001(b), and to take prompt action to remedy deficiencies in such policies and procedures.
[50] To provide consistency between the definition of systems compliance issue and the requirements for policies and procedures to ensure systems compliance, the Commission replaced the reference to federal securities laws with a reference to the Exchange Act.
[51] Proposed Rules 1000(b)(2)(ii) and (iii).
[52] Previously, proposed Rule 1000(b)(2)(iii).

responsibility, were not established, maintained, or enforced in accordance with Rule 1001(b) in any material respect.

In response to commenters, the Commission extended this safe harbor to contractors, consultants, and other non-employees used by SCI entities in connection with their SCI systems through the use of the new phrase "personnel of an SCI entity," rather than only persons employed by an SCI entity. Additionally, rather than requiring an individual to be without reasonable cause to believe that systems compliance policies and procedures "were not being complied with in any material respect" as proposed, the adopted safe harbor requires the applicable personnel to be without reasonable cause to believe that the relevant systems compliance policies and procedures "were not established, maintained, or enforced" in accordance with Rule 1001(b) in any material respect. These changes narrow the applicability of the adopted safe harbor to address comments that the broad scope of the proposed safe harbor would create an environment of distrust and limit the ability of SCI entities to hire high quality personnel. Furthermore, the second element of the adopted individual safe harbor specifies that it applies only to a person who is responsible for or has supervisory responsibility over an SCI system, rather than to all employees of an SCI entity. To respond to comments regarding the scope of individual liability under the safe harbor, the Commission explained that "personnel of an SCI entity will not be deemed to have aided, abetted, counseled, commanded, caused, induced, or procured [a] violation by an SCI entity of Regulation SCI merely because the SCI entity experienced a systems compliance issue, whether or not the person was able to take advantage of the individual safe harbor."[53]

D. SCI Events: Corrective Action; Commission Notification; Dissemination of Information (Rule 1002)

Adopted Rule 1002[54] requires an SCI entity to take corrective action, notify the Commission, and disseminate information regarding certain SCI events and certain SCI systems, in certain circumstances, as described further below.

1. Trigger Standard

The Commission has modified the proposed standard for triggering the need for corrective action, notification to the Commission, and information dissemination requirements under Rule 1002, including modifying the definition of "responsible SCI personnel."

In response to commenters, the Commission revised the term responsible SCI personnel to mean, "for a particular SCI system or indirect SCI system impacted by an SCI event, such senior manager(s) of the SCI entity having responsibility for such system, and their designee(s)."[55] The Commission agreed that the proposed definition was too broad and that it is more appropriate for the adopted definition to focus on senior personnel of SCI entities that have responsibility for a particular system. Moreover, the Commission believes that the revised definition addresses commenters' concerns that the obligations of the rule could have been triggered upon the awareness of junior or inexperienced employees who lack the knowledge or experience to be able to make a determination regarding whether an SCI event had, in fact, occurred. Additionally, the Commission believes that the revised definition will appropriately allow SCI entities to adopt procedures that would require personnel of an SCI entity to escalate a systems issue to senior individuals (and their designees, if applicable) who are responsible for a particular system and who have the ability and authority to appropriately analyze and assess the issue affecting the SCI system or indirect SCI system.

Correspondingly, the Commission believes it is appropriate to also adopt a policies and procedures requirement with respect to the designation of responsible SCI personnel and escalation procedures. Specifically, the Commission is adopting Rule 1001(c), which requires each SCI entity to establish, maintain, and enforce reasonably designed written policies and procedures that include criteria for identifying responsible SCI personnel, the designation and documentation of responsible SCI personnel, and escalation procedures to quickly inform responsible SCI personnel of potential SCI events. The Commission notes that each SCI entity may establish escalation procedures that conform to its needs,

[53] Adopting Release, *supra* note 1, at 72313.
[54] Previously, proposed Rules 100(b)(3)–(5).
[55] Rule 1000.

organization structure, and size. By requiring that responsible SCI personnel are "quickly inform[ed]" of potential SCI events, the Commission intends to require that escalation procedures emphasize promptness and ensure that responsible SCI personnel are informed of potential SCI events without delay. At the same time, the rule does not prescribe a specific time requirement in order to give flexibility to SCI entities in recognition that immediate notification may not be possible or feasible. Further, Rule 1001(c) requires that an SCI entity periodically review the effectiveness of the policies and procedures related to responsible SCI personnel, and to take prompt action to remedy deficiencies in such policies and procedures.

In addition to the change in the definition of responsible SCI personnel, the Commission also revised the triggering standard by requiring compliance with Rule 1002 upon "any responsible SCI personnel having a reasonable basis to conclude that an SCI event has occurred[.]"[56] This standard permits an SCI entity to gather relevant information and perform an initial analysis and assessment as to whether a systems issue may be an SCI event, rather than requiring an SCI entity to take corrective action, notify the Commission, and/or disseminate information about an SCI event immediately upon responsible SCI personnel "becoming aware" of a potential SCI event.

2. Corrective Action

Except for the revised trigger standard, described above, Rule 1002(a)[57] was adopted as proposed, and will require an SCI entity, upon any responsible SCI personnel having a reasonable basis to conclude that an SCI event has occurred, to begin to take appropriate corrective action. Such corrective action must include, at a minimum, mitigating potential harm to investors and market integrity resulting from the SCI event and devoting adequate resources to remedy the SCI event as soon as reasonably practicable. The specific steps that an SCI entity must take to mitigate the harm will depend on the particular systems issue, it causes, and the estimated impact of the issue, among other factors.

3. Commission Notification

Rule 1002(b)[58] addresses the obligation of an SCI entity to notify the SEC upon any responsible SCI personnel having a reasonable basis to conclude that an SCI event occurred. The Commission believes that the comprehensive reporting of SCI events pursuant to this rule would facilitate the Commission's regulatory oversight of the national securities markets. Nevertheless, while retaining its general framework, the Commission made various modifications to the proposed rule to address concerns about the potential for over-reporting.

To further narrow the scope of the adopted notification requirement,[59] the Commission incorporated a risk-based approach that requires SCI entities, for purposes of Commission notification, to divide SCI events into two main categories: (1) SCI events that "[have] had, or the SCI entity reasonably estimates would have, no or a de minimis impact on the SCI entity's operations or on market participants" ("de minimis" SCI events); and (2) SCI events that are not de minimis SCI events. De minimis SCI events will not be subject to an immediate Commission notification requirement as proposed. Instead, all de minimis SCI events will be subject to recordkeeping requirements, and de minimis systems disruptions and de minimis systems intrusions will be subject to a quarterly reporting obligation, as set forth in adopted Rule 1002(b)(5). For SCI events that are not de minimis, Commission notification will be governed by adopted Rules 1002(b)(1)-(4), as discussed in more detail below.

Rule 1002(b)(1)[60] requires an SCI entity, upon any responsible SCI personnel having a reasonable basis to conclude that an SCI event has occurred, to notify the Commission of such SCI event immediately (unless it is a de minimis SCI event). Such notification may be provided orally (*e.g.*, by telephone) or in

[56] Reg SCI, 17 C.F.R. § 242.1002(a) (2014); Adopting Release, *supra* note 1, at 72438. Rule 1002(a).
[57] Previously, proposed Rule 1000(b)(3).
[58] Previously, proposed Rule 1000(b)(4).
[59] The Commission noted that, even without the modifications in adopted Rule 1002(b), the proposed notification rule would have required notice to the Commission of fewer SCI events as a result of the adopted definitions of SCI systems, indirect SCI systems, systems disruption, and systems compliance issue, and the revised triggering standard discussed above.
[60] Previously, proposed Rule 1000(b)(4)(i).

writing (*e.g.*, by email or on Form SCI). Although many commenters were critical of the immediate notification provision, Rule 1002(b)(1) substantially retains the proposed requirements.

Adopted Rule 1002(b)(2)[61] requires an SCI entity, within 24 hours of any responsible SCI personnel having a reasonable basis to conclude that the SCI event has occurred, to submit a written notification pertaining to such SCI event to the Commission (unless it is a de minimis SCI event). Rule 1002(b)(2) allows for such written notifications to be made on a good faith, best efforts basis and requires that it include:

- a description of the SCI event, including the system(s) affected; and
- to the extent available as of the time of the notification:
    - the SCI entity's current assessment of the types and number of market participants potentially affected by the SCI event;
    - the potential impact of the SCI event on the market;
    - a description of the steps the SCI entity has taken, is taking, or plans to take, with respect to the SCI event;
    - the time the SCI event was resolved or timeframe within which the SCI event is expected to be resolved; and
    - any other pertinent information known by the SCI entity about the SCI event.

In response to concerns about providing accurate information about an SCI event within 24 hours, the Commission added the "good faith, best efforts" language. Additionally, given concerns expressed about too much information required to be reported within 24 hours, the Commission also limited the breadth of the requested information.

Rule 1002(b)(3)[62] requires that, until such time as an SCI event is resolved[63] and the SCI entity's investigation of the SCI event is closed, an SCI entity must provide the Commission with updates pertaining to the SCI event on a regular basis, or at such frequency as reasonably requested by a representative of the Commission. Updates are required to correct any materially incorrect information previously provided, or when new material information is discovered, including, but not limited to, any of the information listed in Rule 1002(b)(2)(ii). The Commission believes that this requirement is important to keep the Commission up to date with accurate information about an SCI event. The Commission underscores that the adopted rule alleviates the reporting burden because it now contains a materiality limitation, and it has eliminated the proposed requirements that an SCI entity attach a copy of any information disseminated to date regarding the SCI event to its members or participants or on the SCI entity's publicly available website; a description of the SCI entity's rule(s) and/or governing document(s), as applicable, that relate to the SCI event; and an analysis of parties that may have experienced a loss, whether monetary or otherwise, due to the SCI event, the number of such parties, and an estimate of the aggregate amount of such loss. Additionally, the Commission removed the proposed requirement that such updates be provided in written form; thus, submission of updates may be provided either orally or in writing.

Moreover, Rule 1002(b)(4)(i)(A) requires that if an SCI event is resolved and the SCI entity's investigation of the SCI event is closed within 30 days of the occurrence of the SCI event, then within five business days after the resolution of the SCI event and closure of the SCI entity's investigation regarding the SCI event, the SCI entity must submit to the Commission a final written notification pertaining to the SCI event (a "final report"). Rule 1002(b)(4)(ii) requires the final report to include:

- a detailed description of the SCI entity's assessment of the types and number of market participants affected by the SCI event; the SCI entity's assessment of the impact of the SCI event on the market; the steps the SCI entity has taken, is taking, or plans to take, with respect to the

[61] Previously, proposed Rule 1000(b)(4)(ii).
[62] Previously, proposed Rule 1000(b)(4)(iv)(B).
[63] An SCI event is resolved when the event no longer meets the definition of a systems disruption, systems intrusion, or systems compliance issue, as defined in Rule 1000, and an SCI entity's Rule 1002(b) reporting obligations are completed when an SCI entity submits a final report as required by Rule 1002(b)(4).

SCI event; the time the SCI event was resolved; the SCI entity's rule(s) and/or governing document(s), as applicable, that relate to the SCI event; and any other pertinent information known by the SCI entity about the SCI event;

- a copy of any information disseminated pursuant to Rule 1002(c) by the SCI entity to date regarding the SCI event to any of its members or participants; and

- an analysis of parties that may have experienced a loss, whether monetary or otherwise, due to the SCI event, the number of such parties, and an estimate of the aggregate amount of such loss.

Rule 1002(b)(4)(B) specifies that, if an SCI event is not resolved or the SCI entity's investigation of the SCI event is not closed within 30 calendar days of the occurrence of the SCI event, then the SCI entity must submit to the Commission an interim written notification pertaining to such SCI event within 30 calendar days after its occurrence that contains the information required to be in the final report, to the extent known at the time. Within five business days after the resolution of such SCI event, and closure of the investigation regarding such SCI event, the SCI entity must submit to the Commission a final written notification pertaining to such SCI event that contains the information specified in Rule 1002(b)(4)(ii).

4. Dissemination of Information to Members or Participants

Rule 1002(c)(1)[64] generally addresses the requirements to disseminate information regarding systems disruptions and systems compliance issues. Specifically, Rule 1002(c)(1)(i) requires an SCI entity, promptly after any responsible SCI personnel has a reasonable basis to conclude that an SCI event that is a systems disruption or systems compliance issue has occurred, to disseminate certain information about such SCI event to its members or participants, unless an exception applies.

In adopting Rule 1002(c),[65] the Commission adopted several modifications to the proposed rule. In particular, the Commission eliminated the definition of "dissemination SCI event" from the final rule and adopted an information dissemination requirement that scales dissemination obligations in accordance with the nature and severity of an SCI event, as described below. In response to comment that the proposed rule would result in over-reporting and have limited usefulness, the Commission further focused the rule by introducing the concept of a "major SCI event"[66] and requiring dissemination of information about SCI events to all of a SCI entity's members or participants only in the case of a "major SCI event." Conversely, with respect to non "major SCI events," the adopted rule requires an SCI entity to disseminate information only to affected SCI entity members and participants. At the same time, as with other SCI events, any SCI event that meets the definition of a major SCI event that has had, or the SCI entity reasonably estimates would have, no or a de minimis impact on the SCI entity's operations or on market participants is excepted from the information dissemination requirement. Additionally, de minimis SCI events and SCI events regarding market regulation or market surveillance systems are exempt from the information dissemination requirement.[67]

When the dissemination obligation is triggered, Rule 1002(c)(1)(i) requires an SCI entity to disseminate to the persons specified in Rule 1002(c)(3) information on the system(s) affected by the SCI event and a summary of the SCI event. Thereafter, Rule 1002(c)(1)(ii) provides that, when known, an SCI entity shall promptly disseminate: (1) a detailed description of the SCI event; (2) the SCI entity's current assessment of the types and number of market participants potentially affected by the SCI event; and (3) a description of the progress of its corrective action for the SCI event and when the SCI event has been or is expected to be resolved. Rule 1002(c)(1)(iii) provides that, until resolved, an SCI entity shall provide regular updates of any information required to be disseminated under Rules 1002(c)(1)(i) and (ii). The Commission continues to believe that, for the dissemination of information to be meaningful, it is

[64] Previously, proposed Rule 1000(b)(5).
[65] Previously, proposed Rule 1000(b)(5).
[66] A "major SCI event" is an SCI event that has had, or the SCI entity reasonably estimates would have: (i) any impact on a critical SCI system; or (ii) a significant impact on the SCI entity's operations or on market participants. Reg SCI, 17 C.F.R. § 242.1000 (2014); Adopting Release, *supra* note 1, at 72436-7.
[67] Specifically, Rule 1002(c)(4) provides that the requirements of Rules 1002(c)(1)-(3), discussed above, shall not apply to: (1) SCI events, to the extent they relate to market regulation or market surveillance systems; or (2) any SCI event that has had, or the SCI entity reasonably estimates would have, no or a de minimis impact on the SCI entity's operations or on market participants.

necessary for an SCI entity to describe the SCI event in sufficient detail to permit a member or participant to determine whether and how it was affected by the SCI event and make appropriate decisions based on that determination. The specified types of information and the update requirements are unchanged from the proposal.

Rule 1002(c)(2) requires an SCI entity, promptly after any responsible SCI personnel has a reasonable basis to conclude that an SCI event that is a systems intrusion has occurred, to disseminate a summary description of the systems intrusion, including a description of the corrective action taken by the SCI entity and when the systems intrusion has been or is expected to be resolved, unless the SCI entity determines that dissemination of such information would likely compromise the security of the SCI entity's SCI systems or indirect SCI systems or an investigation of the systems intrusion, and documents the reasons for such determination. This rule applies to systems intrusions that are not de minimis events.

Rule 1002(c)(3) states that the information required to be provided under Rules 1002(c)(1) and (2) promptly after any responsible SCI personnel has a reasonable basis to conclude that an SCI event has occurred, shall be promptly disseminated by the SCI entity to those members or participants of the SCI entity that any responsible SCI personnel has reasonably estimated may have been affected by the SCI event. The rule also requires that an SCI entity promptly disseminate such information to any additional members or participants that any responsible SCI personnel subsequently reasonably estimates may have been affected by the SCI event.

E. Rule 1003—System Changes and Review

1. Notification of Material Systems Changes

Rule 1003(a)(1)[68] requires an SCI entity, within 30 calendar days after the end of each calendar quarter, to submit to the Commission a report describing completed, ongoing, and planned material systems changes to its SCI systems and security of indirect SCI systems, during the prior, current, and subsequent calendar quarters, including the dates or expected dates of commencement and completion. In response to commenters, the Commission adopted the quarterly reporting requirement in place of the proposed 30-day advance notification requirement. Furthermore, in light of the new quarterly report, the Commission eliminated the proposed "exigent circumstances" qualifier as unnecessary. Correspondingly, the Commission also adopted Rule 1003(a)(2), which requires an SCI entity to promptly submit a supplemental report to notify the Commission of a material error in, or material omission from, a report previously submitted under Rule 1003(a)(1).

Rather than adopting the detailed definition of material systems change as proposed, Rule 1003(a)(1) requires an SCI entity to establish reasonable written criteria for identifying a material change to its SCI systems and the security of indirect SCI systems, and to report to the Commission those changes the SCI entity identified as material. This approach replaces the detailed definition of "material systems change," as originally proposed. This change is responsive to a commenter's suggestion that SCI entities should be granted flexibility to establish reasonable standards for determining whether a systems change is material. Additionally, the Commission does not believe that it is appropriate to adopt a precise definition for the term "material systems change" because SCI entities differ in nature, size, technology, business model, and other aspects of their businesses.

2. Review of Systems

The Commission adopted the proposed provisions relating to SCI reviews with certain modifications in response to comment. Specifically, adopted Rule 1003(b)[69] requires an SCI entity to conduct an SCI review of the SCI entity's compliance with Reg SCI not less than once each calendar year, subject to certain exceptions. Specifically, penetration test reviews of the network, firewalls, and production systems must be conducted at a frequency of not less than once every three years; and assessments of SCI systems directly supporting market regulation or market surveillance must be conducted at a frequency based upon the risk assessment conducted as part of the SCI review, but in no case less than once every three years. In addition, an SCI entity must submit a report of the required SCI review to senior

[68] Previously, proposed Rule 1000(b)(6).
[69] Previously, proposed Rule 1000(b)(7).

management of the SCI entity for review no more than 30 calendar days after completion of such SCI review, and must submit to the Commission, and to the board of directors of the SCI entity or the equivalent of such board, a report of the SCI review, together with any response by senior management, within 60 calendar days after its submission to senior management of the SCI entity. For the purposes of this provision, "senior management" is defined in Rule 1000 to mean an SCI entity's Chief Executive Officer, Chief Technology Officer, Chief Information Officer, General Counsel, and Chief Compliance Officer, or the equivalent of such employees or officers of an SCI entity.

Because the Commission revised the definition of "SCI systems," fewer systems of each SCI entity will be subject to the SCI review than originally proposed, thereby focusing the overall scope of the SCI review requirement. In addition, to address some commenters' concerns about the burdens and inflexibility of the proposed rule and the recommendation that the proposed rule utilize a more risk-based approach, the adopted rule is revised to allow assessments of SCI systems directly supporting market regulation or market surveillance to be conducted, based upon a risk-assessment, at least once every three years, rather than annually.

F. SCI Entity Business Continuity and Disaster Recovery Plans Testing Requirements for Members or Participants (Rule 1004)

Adopted Rule 1004[70] addresses testing of SCI entity business continuity and disaster recovery plans, including backup systems, by SCI entity members or participants. In response to significant comment, the adopted rule requires designation of a more limited set of SCI entity members and participants for mandatory participation in business continuity/disaster recovery testing than the proposed rule. Further, the adopted rule does not require an SCI entity to file designation standards or member/participant designations with the Commission on Form SCI, as was proposed, but instead an SCI entity must keep records of its standards and designations.

The scope, frequency, and coordination aspects of the proposed rule, however, have been adopted as proposed.

Specifically, Rule 1004, as adopted, states that, with respect to business continuity and disaster recovery plans, including its backup systems, each SCI entity is required to (1) establish standards for the designation of those members or participants that the SCI entity reasonably determines are, taken as a whole, the minimum necessary for the maintenance of fair and orderly markets in the event of the activation of such plans; (2) designate members or participants pursuant to the standards established pursuant to Rule 1004 and require participation by such designated members or participants in scheduled functional and performance testing of the operation of such plans, in the manner and frequency specified by the SCI entity, provided that such frequency shall not be less than once every 12 months; and (3) coordinate the testing of such plans on an industry- or sector-wide basis with other SCI entities.

G. Recordkeeping Requirements (Rule 1005)

Rule 1005[71] sets forth the recordkeeping requirements for SCI entities with respect to records relating to Reg SCI compliance. In adopting Rule 1005, the Commission eliminated the proposed requirement to provide Commission staff with direct access to an SCI entity's systems in order to assess the SCI entity's compliance with Reg SCI.[72] The Commission noted that existing recordkeeping requirements and the Commission's examination authority in combination with new Rule 1005 can achieve the same goal.

Under Rule 1005(a), SCI SROs are required to make, keep, and preserve all documents relating to their compliance with Reg SCI, as prescribed by Rule 17a-1 under the Exchange Act. Consistent with the recordkeeping requirements applicable to SCI SROs, Rule 1005(b) requires each SCI entity that is not an SCI SRO (*i.e.*, SCI ATSs, plan processors, and exempt clearing agencies subject to ARP), to make, keep, and preserve at least one copy of all documents, including correspondence, memoranda, papers, books, notices, accounts, and other such records, relating to its compliance with Reg SCI, including, but not limited to, records relating to any changes to its SCI systems and indirect SCI systems, for a period of not

[70] Previously, proposed Rule 1000(b)(9).
[71] Previously, proposed Rule 1000(c).
[72] Previously, proposed Rule 1000(f).

less than five years, the first two years in a place that is readily accessible to the Commission or its representatives for inspection and examination. Upon request of any representative of the Commission, such SCI entities are required to promptly furnish to the possession of such representative copies of any documents required to be kept and preserved by it under Rule 1005(b). Finally, Rule 1005(c), which is applicable to all SCI entities, requires each SCI entity, upon or immediately prior to ceasing to do business or ceasing to be registered under the Exchange Act, to take all necessary action to ensure that records required to be made, kept, and preserved by Rule 1005 are accessible to the Commission or its representatives in the manner required for the remainder of the period required by Rule 1005(c).

H. Electronic Filing and Submission (Rule 1006)

Rule 1006,[73] which is adopted substantially as proposed, requires that any notification, review, description, analysis, or report to the Commission required to be submitted under Reg SCI (except with respect to notifications to the Commission made pursuant to Rule 1002(b)(1) or updates to the Commission made pursuant to Rule 1002(b)(3)) be filed electronically on Form SCI, include all information as prescribed in Form SCI and the instructions thereto, and contain an electronic signature. Pursuant to Rule 1006(b), the signatory to an electronically filed Form SCI also must manually sign a signature page or document, in the manner prescribed by Form SCI, authenticating, acknowledging, or otherwise adopting his or her signature that appears in typed form within the electronic filing. Such document must be executed before or at the time Form SCI is electronically filed and shall be retained by the SCI entity in accordance with Rule 1005. The Commission believes that Rule 1006 provides a uniform manner for SCI entities to provide, and the SEC to receive, material pursuant to Reg SCI, thereby enhancing the efficiency of the process.

I. Service Bureaus (Rule 1007)

Rule 1007,[74] which was adopted as proposed, provides that, if records required to be filed or kept by an SCI entity under Reg SCI are prepared or maintained by a service bureau or other recordkeeping service on behalf of the SCI entity, the SCI entity shall ensure that the records are available for review by the Commission and its representatives by submitting a written undertaking, in a form acceptable to the Commission, by such service bureau or other recordkeeping service that is signed by a duly authorized person of such service bureau or recordkeeping service. Such a written undertaking must include an agreement by the service bureau to permit the Commission and its representatives to examine such records and to promptly furnish to the Commission and its representatives true, correct, and current electronic files in an acceptable form, or hard copies of such records, upon request, periodically, or continuously and within the same time periods as would apply to the SCI entity for such records. The preparation or maintenance of records by a service bureau or other recordkeeping service shall not relieve an SCI entity from its obligation to prepare, maintain, and provide the Commission and its representatives access to such records.

J. Form SCI

The notices, reports, and other information required to be provided to the Commission pursuant to Reg SCI (except with respect to notifications to the SEC made pursuant to Rule 1002(b)(1) or updates to the SEC made pursuant to Rule 1002(b)(3)) must be submitted electronically on new Form SCI. Form SCI solicits information through a series of questions designed to elicit short-form answers. It also requires SCI entities to provide information and/or reports in narrative form by attaching specified exhibits. All filings on Form SCI require that an SCI entity identify itself and indicate the basis for submitting the form. SCI entities may request confidential treatment of any or all information submitted to the Commission pursuant to Reg SCI on Form SCI.[75] If such a confidential treatment request is properly made, the Commission will keep the information collected pursuant to Form SCI confidential to the extent permitted by law.[76]

---

[73] Previously, proposed Rule 1000(d).
[74] Previously, proposed Rule 1000(e).
[75] The SEC has amended Rule 24b-2 under the Exchange Act regarding confidential treatment requests to reference Form SCI.
[76] The Freedom of Information Act ("FOIA") provides at least two pertinent exemptions under which the Commission has authority to withhold certain information—FOIA Exemption 4 and 8. 5 U.S.C. 552(b)(4) and (8).

FOR MORE INFORMATION ON THIS OR OTHER SECURITIES MATTERS, CONTACT:

Andre E. Owens +1 202 663 6350 andre.owens@wilmerhale.com
Stephanie Nicolas +1 202 663 6825 stephanie.nicolas@wilmerhale.com
Cherie Weldon +1 212 230 8806 cherie.weldon@wilmerhale.com
Jeremy Moorehouse +1 202 663 6522 jeremy.moorehouse@wilmerhale.com
Mahlet Ayalew +1 202 663 6903 mahlet.ayalew@wilmerhale.com
