SEC Proposes to Expand Reg SCI

MAY 8, 2023

The Securities and Exchange Commission (SEC) proposes to amend Regulation Systems Compliance and Integrity (Reg SCI) to update and expand the regulatory oversight of the core technology of the U.S. securities markets.[1] The SEC proposes to expand the definition of "SCI entity" to include registered broker-dealers exceeding an asset or transaction activity threshold, additional clearing agencies exempted from registration and security-based swap data repositories (SBSDRs). The SEC also requests comment on whether significant-volume alternative trading systems (ATSs) and/or broker-dealers using electronic or automated systems for trading of corporate debt securities or municipal securities should be subject to Reg SCI. In response to the evolution of technology and trading in the U.S. securities markets, the SEC also proposes to update certain provisions in Reg SCI relating to (1) systems classification and lifecycle management, (2) third-party/vendor management, (3) cybersecurity, (4) SCI reviews, and (5) the role of current SCI industry standards. The SEC requests comments on the proposal by June 13, 2023.

I. Definition of SCI Entity

Currently, SCI entities are the SCI SROs, SCI ATSs, plan processors, certain exempt clearing agencies and SCI competing consolidators.[2] The SEC proposes to expand the definition of SCI entity to include broker-dealers exceeding an asset or transaction activity threshold, additional clearing agencies exempted from registration and SBSDRs.[3] The SEC also requests comment on whether to include in the definition of SCI entity significant-volume ATSs and/or broker-dealers using electronic or automated systems for trading corporate debt securities or municipal securities.

[1] Securities Exchange Act Rel. No. 97143 (Mar. 15, 2023), 88 Fed. Reg. 23146 (Apr. 14, 2023).

[2] Definition of "SCI entity" in Rule 1000 of Reg SCI.

[3] Proposed definition of "SCI entity" in Rule 1000 of Reg SCI.

A. SCI Broker-Dealers

The SEC proposes to revise the definition of an SCI entity in Reg SCI to include SCI broker-dealers. The SEC proposes to define "SCI broker-dealer" to mean a broker or dealer registered with the SEC pursuant to Section 15(b) of the Exchange Act that meets or exceeds (i) a total assets threshold or (ii) one or more transaction activity thresholds.[4] The SEC states that the proposed thresholds are designed to identify a limited number of firms that by virtue of their total assets or level of transaction activity over a period of time and on a consistent basis play a significant role in the orderly functioning of US securities markets. The SEC states that the thresholds are further designed to identify firms that if adversely affected by a technology event, could disrupt or impede orderly and efficient market operations more broadly.

1. Proposed Total Assets Threshold

Under the SEC's proposal, a broker-dealer would be an SCI broker-dealer if in at least two of the four preceding calendar quarters—ending March 31, June 30, September 30, and December 31—it reported to the SEC on Form X-17A-5, FOCUS Report Part II, Item 940, total assets in an amount that equals 5 percent or more of the total assets of all security brokers and dealers.[5] The firm's total assets filed on FOCUS reports would be divided by the broader measure of total assets for all security brokers and dealers calculated and made publicly available by the Federal Reserve Board (or any subsequent provider of the information) for the associated preceding calendar quarter.[6] Based on data from recent quarters, the SEC estimates that five entities would exceed the proposed threshold (with the fifth-ranked firm in each quarter reporting total assets in excess of $300 billion, and all firms ranging from approximately 7 percent to 14 percent of the total assets reported by the Federal Reserve Board for the previous quarter).

2. Proposed Transaction Activity Threshold

The SEC also proposes to define "SCI broker-dealer" to include a broker-dealer that during at least four of the preceding six calendar months:

- with respect to transactions in NMS stocks, transacted average daily dollar volume in an amount that equals 10 percent or more of the average daily dollar volume reported by or pursuant to applicable effective transaction reporting plans, provided, however, that for

[4] An SCI broker-dealer would be required to comply with the requirements of Reg SCI six months after the SCI broker-dealer satisfied either threshold for the first time. Proposed paragraph (3) of the definition of "SCI broker-dealer" in Rule 1000 of Reg SCI.

[5] Proposed paragraph (1) of the definition of "SCI broker-dealer" in Rule 1000 of Reg SCI.

[6] This figure has been calculated by the Federal Reserve Board and made available on the Federal Reserve Economic Data website for years.

purposes of calculating its activity in transactions effected otherwise than on a national securities exchange or on an ATS, the broker-dealer shall exclude transactions for which it was not the executing party; or

- with respect to transactions in exchange-listed options contracts, transacted average daily dollar volume in an amount that equals 10 percent or more of the average daily dollar volume reported by an applicable effective national market system plan; or
- with respect to transactions in U.S. Treasury Securities, transacted average daily dollar volume in an amount that equals 10 percent or more of the total average daily dollar volume made available by the self-regulatory organizations to which such transactions are reported; or
- with respect to transactions in Agency Securities, transacted average daily dollar volume in an amount that equals 10 percent or more of the total average daily dollar volume made available by the self-regulatory organizations to which such transactions are reported.[7]

The SEC proposes to add definitions of “U.S. Treasury Security” and “Agency Security” to Reg SCI to clarify how the transaction activity threshold for these asset classes would operate. A U.S. Treasury Security would mean “a security issued by the U.S. Department of the Treasury.”[8] Agency Security would mean “a debt security issued or guaranteed by a U.S. executive agency, as defined in 5 U.S.C. 105, or government-sponsored enterprise, as defined in 2 U.S.C. 622(8).”[9]

The SEC estimates that 17 entities would satisfy one or more of the proposed transaction activity thresholds (the same five entities identified by the proposed total assets threshold plus 12 additional entities).

3. Proposed Revision to Definition of ‘SCI Systems’ for Certain SCI Broker-Dealers

In conjunction with the proposed inclusion of SCI broker-dealers as SCI entities, the SEC proposes to limit the definition of “SCI systems” for an SCI broker-dealer that qualifies as an SCI entity only because it satisfies a transaction activity threshold. The SEC preliminarily believes that an SCI broker-dealer that qualifies as an SCI entity based only on a transaction activity threshold for a particular type of security should have its Reg SCI obligations limited to systems with respect to that type of security.[10] For example, if a broker-dealer meets only the transaction activity threshold

[7] Proposed paragraph (2) of the definition of “SCI broker-dealer” in Rule 1000 of Reg SCI.

[8] Proposed definition of “U.S. Treasury Security” in Rule 1000 of Reg SCI.

[9] Proposed definition of “Agency Security” in Rule 1000 of Reg SCI.

[10] Specifically, the SEC is proposing to revise the definition of “SCI systems” in Rule 1000 of Reg SCI to add a limitation that states, “provided, however, that with respect to an SCI broker-dealer that satisfies only the requirements of paragraph (2) of the definition of ‘SCI broker-dealer,’ such systems shall include only

for NMS stocks, its systems that directly support trading, clearance and settlement, order routing, market data, market regulation, or market surveillance for NMS stocks are those that raise the concerns Reg SCI is meant to address. If the broker-dealer's activity with respect to other classes of securities is nominal, it is unlikely to pose risk to the maintenance of fair and orderly markets if the systems with respect to those types of securities were unavailable (assuming the systems for the distinct asset class are separate). If a system of the broker-dealer is used for more than one type of security (i.e., an asset class that triggered the threshold and an asset class that did not or is not subject to SCI thresholds), such system would still meet the definition of "SCI system."

4. SCI Broker-Dealer Activity in Crypto Asset Securities

The SEC discussed how the proposal would affect an SCI broker-dealer that engages in crypto asset security activity as follows:

- For purposes of assessing whether it meets a transaction activity threshold, a broker-dealer would need to consider whether it trades crypto asset securities that are NMS stocks, exchange-listed options, U.S. Treasury Securities or Agency Securities, and if so, include those transactions in its transaction tally of NMS stocks, exchange-listed options, U.S. Treasury Securities or Agency Securities to assess whether the broker-dealer satisfies one or more of the proposed thresholds.
- An SCI broker-dealer that meets the proposed total assets threshold would need to consider its crypto asset security activities and assess whether any systems pertaining to crypto asset securities meet the current definition of "SCI systems" or "indirect SCI systems."

5. Information Dissemination for SCI Broker-Dealers

In connection with the proposal to include SCI broker-dealers as SCI entities, the SEC proposes to require SCI broker-dealers to disseminate information about an SCI event in accordance with Rule 1002(c) to their customers (i.e., those with whom they trade or for whom they facilitate trades as agents).[11] In addition, SCI broker-dealers would be required to include in their notices to the SEC a copy of any information they disseminate to their customers.[12]

those systems with respect to the type of securities for which an SCI broker-dealer satisfies the requirements of paragraph (2) of the definition."

[11] Proposed Rule 1002(c)(3) of Reg SCI.

[12] Proposed Rule 1002(b)(4)(ii)(B) of Reg SCI.

B. Exempt Clearing Agencies

The SEC proposes to expand the scope of an SCI entity to cover all exempt clearing agencies rather than only those exempt clearing agencies subject to the SEC's Automation Review Policy Program (ARP).[13] The SEC believes that the application of Reg SCI to all exempt clearing agencies is appropriate given their important role in helping ensure the functioning, resilience and stability of US securities markets and their growing technological innovations and interconnectedness. This proposed change currently would require two new exempt clearing agencies to comply with Reg SCI.

C. Registered Security-Based Swap Data Repositories (SBSDRs)

The SEC proposes to expand the definition of "SCI entity" to include SBSDRs.[14] As registered securities information processors that disseminate market data and provide price transparency in the security-based swap (SBS) market and centralized trade repositories for SBS data for use by regulators, SBSDRs play a key role in the SBS market. Accordingly, the SEC believes that the current technology framework for SBSDRs should be strengthened.[15] There are currently two registered SBSDRs that would become subject to Reg SCI based on this change.

D. Significant-Volume Fixed Income ATSs and Broker-Dealers Using Electronic or Automated Systems for Trading of Corporate Debt Securities or Municipal Securities

The SEC did not include ATSs trading corporate debt or municipal securities (Fixed Income ATSs) as SCI entities when it adopted Reg SCI because the markets for such securities relied much less on automation and electronic trading than the equity markets did at that time. Due to changes in the market and updates to technology, however, the SEC requests comment on applying Reg SCI to significant-volume Fixed Income ATSs and/or to broker-dealers trading significant volume in

[13] Proposed definition of "exempt clearing agency" in Rule 1000 of Reg SCI.

[14] The SEC proposes to add a definition of "registered SBSDR" to Rule 1000 of Reg SCI, which would state that a registered SBSDR is "any security-based swap data repository, as defined in 15 U.S.C. 78c(a)(75), that is registered with the Commission pursuant to 15 U.S.C. 78m(n) and § 240.13n-1 of this chapter."

[15] SBSDR technology regulation is currently governed by Rule 13n-6 under the Exchange Act, which is a broad principles-based operational risk rule.

corporate debt or municipal securities. In particular, the SEC solicits comment on whether the distinctions drawn by the SEC in its original adoption of Reg SCI, between equities markets on the one hand and the corporate debt and municipal securities markets on the other, based on differences in their reliance on automation and electronic trading strategies, have diminished such that Fixed Income ATSs or broker-dealers with significant activity in corporate debt and municipal securities should be subject to increased technology oversight pursuant to Reg SCI.

II. Enhanced Obligations for SCI Entities

Since the adoption and implementation of Reg SCI, technology and the ways SCI entities employ such technology have continued to evolve, as have the potential vulnerabilities of and threats posed to SCI entities. Accordingly, the SEC proposes to strengthen the requirements Reg SCI imposes on SCI entities, including with regard to (1) systems classification and lifecycle management, (2) third-party provider management, (3) cybersecurity, and (4) current SCI industry standards.

A. Systems Classification and Lifecycle Management

The SEC notes that an SCI entity's identification of systems that are subject to Reg SCI is an essential step for Reg SCI compliance. Accordingly, the SEC proposes to require SCI entities to include in their policies and procedures the maintenance of a written inventory and classification of all its SCI systems, critical SCI systems and indirect SCI systems as such.[16] In addition, the SEC proposes to require that the SCI entity's policies and procedures include "a program with respect to the lifecycle management of such systems, including the acquisition, integration, support, refresh, and disposal of such systems, as applicable."[17] The purpose of this provision is to help ensure that an SCI entity is able to identify risks an SCI system may face during its various lifecycle phases. For example, the lifecycle management program would need to address the refresh of SCI systems (e.g., via up-to-date software and security patches) and their disposal (e.g., via sanitization of end-of-life systems to protect sensitive information).

B. Third-Party Provider Management

The SEC believes that the use of third-party providers by SCI entities can be appropriate and even advantageous in certain instances. When the SEC adopted Reg SCI in 2014, it accounted for the possibility that an SCI entity might utilize third-party providers to operate its SCI systems or indirect SCI systems. However, given the growing role third-party providers play with respect to SCI systems and indirect SCI systems and because of the myriad of issues associated with the use of

[16] Proposed Rule 1001(a)(2)(viii) of Reg SCI.

[17] *Id.*

third-party providers (including but not limited to oversight, access, speed of information flow, security and unauthorized access, loss of expertise internally, and lock-in), the SEC believes that it is appropriate to delineate more clearly the requirements with respect to the oversight and management of third-party providers, and thus proposes to revise Reg SCI to include additional requirements relating to third-party providers.

1. *Cloud Services Provider and Other Third-Party Provider Management Issues*

In its discussion of third-party provider management issues, the SEC highlights the growing use of cloud service providers (CSPs) and the potential third-party provider management issues that CSPs may raise with regard to Reg SCI compliance. The SEC notes that in deciding whether to utilize a CSP, an SCI entity generally should take into account the factors it would consider with regard to any other third-party providers. However, given the degree to which CSP services may be integral to the operation of SCI systems, SCI entities generally should examine closely any potential relationship and utilization of CSP services to ensure that such services can and do comply with Regulation SCI. The SEC provided the following illustrative examples of areas of potential concern in an SCI entity's relationship with a CSP:

- SCI entities must determine that they have the ability to manage a CSP relationship (whether through appropriate due diligence, contract terms, monitoring or other methods) to satisfy the requirements of Reg SCI.
- SCI entities must ensure that their own personnel have the requisite skills to properly manage and oversee a CSP relationship, and understand the issues—including technical ones—that may arise from the use of a CSP.
- SCI entities must ensure that their SCI systems in the public cloud comply with the requirement in Reg SCI to have 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.
- SCI entities should consider any lock-in effects that utilizing CSP-specific tools might have and their exit strategies with respect to the use of a CSP (e.g., consider utilizing different CSPs or on-premises backup tools).
- SCI entities should ensure that they are able to meet the notice and information dissemination requirements of Rule 1002 within the designated time requirements.
- With regard to data security and recordkeeping, SCI entities should consider how the CSP and its employees or contractors would secure confidential information; how and where it would retain information; and how the information would be accessed by the personnel of

the SCI entity or others, such as those conducting SCI reviews and Commission staff, as well as ensure that such information access will be provided in a manner that complies with the requirements of Reg SCI.

The SEC notes that similar issues may be applicable to the relationships between SCI entities and types of third-party providers other than CSPs.

2. *Third-Party Provider Management Program*

To help ensure that an SCI entity that elects to use a third-party provider will be able to meet its obligations under Reg SCI, the SEC proposes to require that SCI entities have a third-party provider management program that includes certain elements.[18] Specifically, the SEC proposes to require each SCI entity to include in its policies and procedures a program to manage and oversee third-party providers that provide functionality, support or service, directly or indirectly, for its SCI systems and, for purposes of security standards, indirect SCI systems.

First, the program would be required to include initial and periodic reviews of contracts with such third-party providers for consistency with the SCI entity's obligations under Reg SCI. The SEC provided examples of the types of issues such reviews would consider. For example, SCI entities should consider whether contractual terms:

- specify response times that are slower than those required by Reg SCI (e.g., via reliance on a third-party provider's standard contract or standard service level agreement (SLA), particularly if such contract or SLA has not been drafted with Reg SCI in mind);
- do not specifically and substantively address key aspects of Reg SCI that would need the third-party provider's cooperation (e.g., SCI event notifications and information dissemination and business continuity and disaster recovery);
- undermine the ability of the SCI entity to oversee and manage the third party; and
- restrict information flow to the SCI entity and/or the SEC and its staff in a manner inconsistent with Reg SCI.

Second, the program would be required to include a risk-based assessment of each third-party provider's criticality to the SCI entity, including analyses of third-party provider concentration; of key dependencies if the third-party provider's functionality, support or service were to become unavailable or materially impaired; and of any potential security, including cybersecurity, risks posed.

[18] Proposed Rule 1001(a)(2)(ix) of Reg SCI.

3. Third-Party Providers for Critical SCI Systems

Given the essential nature of critical SCI systems,[19] the SEC believes that it is appropriate to require SCI entities to have even more enhanced policies and procedures with respect to any third-party provider that supports such systems. Accordingly, the SEC proposes to require the business continuity and disaster recovery plans of SCI entities to be "reasonably designed to address the unavailability of any third-party provider that provides functionality, support, or service to the SCI entity without which there would be a material impact on any of its critical SCI systems."[20] For example, such business continuity and disaster recovery plans generally should not only take into account and address temporary losses of functionality, support or service—such as a momentary outage that causes a feed to be interrupted or an extended cybersecurity event at the third-party provider—but also consider more extended outage scenarios, including if the third-party provider goes into bankruptcy or dissolves or if it breaches its contract and decides to suddenly, unilaterally and/or permanently cease to provide the SCI entity's critical SCI systems with functionality, support or service. In determining how to satisfy this proposed requirement, an SCI entity could consider whether use of a CSP for its critical SCI systems also warrants maintaining an on-premises backup data center or other contingency plan that could be employed in the event of such outage scenarios.

4. Third-Party Provider Participation in Business Continuity and Disaster Recovery Testing

The SEC stated that there may be one or more third-party providers of such significance to the operations of an SCI entity that without the functions, support or services of such provider(s), the maintenance of fair and orderly markets in the event of the activation of the SCI entity's business continuity and disaster recovery plans would not be possible. The SEC proposes to include such third-party providers in the business continuity and disaster recovery testing requirements of Rule 1004. Specifically, the SEC proposes to require an SCI entity to establish standards for the designation of third-party providers (in addition to members or participants) that the SCI entity determines are, taken as a whole, the minimum necessary for the maintenance of fair and orderly markets in the event of the activation of the SCI entity's business continuity and disaster recovery plans.[21] In addition, the SEC would require each SCI entity to designate such third-party providers

[19] Rule 1000 of Reg SCI defines "critical SCI systems" to mean "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."

[20] Proposed Rule 1001(a)(2)(v) of Reg SCI.

[21] Proposed Rule 1004(a) of Reg SCI.

(in addition to members or participants) pursuant to such standards and require their participation in the scheduled functional and performance testing of the operation of such business continuity and disaster recovery plans, which would occur no less frequently than once every 12 months.[22] For example, the SEC believes it is likely that for an SCI entity that utilizes a CSP for all, or nearly all, of its operations, such CSP would be of such importance to the operations of the SCI entity and the maintenance of fair and orderly markets in the event of the activation of the SCI entity's business continuity and disaster recovery plans that it would be required to participate in the business continuity and disaster recovery testing required by Rule 1004.

C. Cybersecurity

The SEC proposes to enhance the cybersecurity provisions of Reg SCI in response to the continued and increasing risk associated with cybersecurity for SCI entities. Specifically, the SEC proposes to strengthen the security requirements of Reg SCI with regard to unauthorized access to systems and information, penetration testing, and systems intrusions.

1. Unauthorized Access to Systems and Information

The SEC proposes to require that the policies and procedures of SCI entities include a program to prevent unauthorized access to SCI systems and, for purposes of security standards, indirect SCI systems as well as to information residing therein.[23] An SCI entity's policies and procedures generally should specify appropriate access controls to ensure that its applicable systems and information are protected. Such policies and controls generally should be designed to prevent both unauthorized external intruders as well as unauthorized internal personnel from access to these systems and information. For example, this would include personnel who may be inappropriately accessing certain systems and/or information residing on such systems, though they may have authorized access to other systems, portions of systems or certain information residing in such systems at the SCI entity.

In creating and implementing such policies and procedures, SCI entities generally should develop a clear understanding of the need for access to systems and data, including identifying which users should have access to sensitive systems or data. In general, such policies and procedures should include requiring standards of behavior for individuals authorized to access SCI systems and indirect SCI systems and information residing therein, such as an acceptable use policy; identifying and authenticating individual users; establishing procedures for timing distribution, replacement and revocation of passwords or methods of authentication; restricting access to specific SCI systems or components thereof or information residing therein only to individuals requiring access to such

[22] Proposed Rule 1004(b) of Reg SCI.

[23] Proposed Rule 1001(a)(2)(x) of Reg SCI.

systems or information as is necessary for them to perform their responsibilities or functions for the SCI entity; and securing remote access technologies used to interface with SCI systems. Access to systems and data can be controlled through a variety of means, including but not limited to the issuance of user credentials; digital rights management with respect to proprietary hardware and copyrighted software; authentication methods, including multifactor authentication as appropriate; tiered access to sensitive information and network resources; and security and access measures that are regularly monitored not only to provide access to authorized users but also to remove access for users that are no longer authorized (e.g., due to termination of employment). SCI entities may, if they choose, look to SCI industry standards in developing their policies and procedures to prevent unauthorized access to information and systems.

2. Penetration Testing

The SEC also proposes to amend the Reg SCI requirements related to penetration testing.[24] The SEC proposes to increase the frequency of penetration testing by SCI entities such that the tests are conducted at least annually rather than once every three years.[25] In addition, the SEC proposes to require SCI entities to include testing of the vulnerabilities identified pursuant to its regular review and testing requirement in designing its penetration testing.[26] Thus, for example, rather than running a static annual test against a portion of its SCI systems, this proposed language would require an SCI entity's penetration testing program to include any identified relevant threats and then conduct penetration testing accordingly.

3. Systems Intrusions

The SEC proposes to amend the Reg SCI requirements applicable to systems intrusions. Specifically, the SEC proposes to expand the definition of "systems intrusion" and to revise the reporting requirements and information dissemination requirements for systems intrusions.

a. Definition of Systems Intrusion

Reg SCI currently defines "systems intrusion" as "any unauthorized entry into the SCI systems or indirect SCI systems of an SCI entity."[27] The SEC proposes to expand the definition of "systems intrusion" to include two additional types of cybersecurity events.

[24] The SEC proposes to move the requirements related to penetration test reviews from Rule 1003(b)(1)(i) of Reg SCI to proposed paragraph (2) of the definition of "SCI review" in Rule 1000 of Reg SCI.

[25] Proposed Rule 1003(b)(1) of Reg SCI.

[26] Proposed paragraph (2) of the definition of "SCI review" in Rule 1000 of Reg SCI.

[27] Definition of "systems intrusion" in Rule 1000 of Reg SCI.

The SEC proposes to include in the definition of "systems intrusion" any "[c]ybersecurity event that disrupts, or significantly degrades, the normal operation of an SCI system,"[28] regardless of whether the event resulted in an entry into or access to the system. For example, in distributed denial-of-service attacks, the attacker, often using malware-infected machines, typically seeks to overwhelm or drain the resources of the target with illegitimate requests in order to prevent the target's systems from providing services to those seeking to access or use them. Unlike cybersecurity events that would qualify under the current definition of "systems intrusion," the objective of these attacks is often simply to disrupt or disable the target's operations, rendering them unable to run efficiently—or run at all.

The SEC also proposes to include in the definition of "systems intrusion" any "[s]ignificant attempted unauthorized entry into the SCI systems or indirect SCI systems of an SCI entity, as determined by the SCI entity pursuant to established reasonable written criteria."[29] This new type of systems intrusion is intended to capture unsuccessful but significant attempts to enter an SCI entity's SCI systems or indirect SCI systems. The term "significant attempted unauthorized entry" would not be defined in the rule. Rather, the proposed rule would require each SCI entity to establish reasonable written criteria to determine whether a significant attempted unauthorized entry has occurred. However, the SEC believes that certain characteristics of attempted unauthorized entries would generally weigh in favor of such attempted unauthorized entries being considered significant and constituting systems intrusions that should be considered SCI events subject to the requirements of Reg SCI, including:

- when an SCI entity becomes aware of reconnaissance that may be leveraged by a threat actor;
- a targeted campaign that is customized to the SCI entity's system;
- an attempted cybersecurity event that required the SCI entity's personnel to triage, even if it was ultimately determined to have no impact;
- an attempted attack from a known sophisticated advanced threat actor;
- the depth of the breach in terms of proximity to SCI systems and critical SCI systems; and
- a cybersecurity event that, if successful, had meaningful potential to result in widespread damage and/or loss of confidential data or information.

b. Reporting Requirements for Systems Intrusions

Reg SCI currently states that the SEC notification requirements in Rule 1002(b)(1) through (4) do not apply to any de minimis SCI events, including systems intrusions. Instead, SCI entities are

[28] Proposed paragraph (2) of the definition of "systems intrusion" in Rule 1000 of Reg SCI.

[29] Proposed paragraph (3) of the definition of "systems intrusion" in Rule 1000 of Reg SCI.

currently required to make, keep and preserve records relating to all such SCI events and provide the SEC with a quarterly report of de minimis systems intrusions and disruptions.[30] The SEC proposes to eliminate systems intrusions from the types of SCI events that may make use of this exception for de minimis SCI events and be quarterly reported. Instead, the SEC proposes to require that each systems intrusion be reported under the framework in Rule 1002(b)(1) through (4).[31]

c. Information Dissemination for Systems Intrusions

Rule 1002(c) requires SCI entities to disseminate information to their members or participants regarding SCI events. The SEC believes that it would be appropriate that information about systems intrusions under the proposed second prong of the "systems intrusion" definition (a "cybersecurity event that disrupts, or significantly degrades, the normal operation of an SCI system") be disseminated pursuant to Rule 1002(c)'s requirements. However, the SEC does not believe that information regarding significant attempted unauthorized entries should be required to be disseminated to an SCI entity's members or participants, as any benefits associated with disseminating information about unsuccessful attempted unauthorized entries to members or participants of an SCI entity would likely not be justified, due to distractions that such information would bring, particularly since the SCI entity's security controls were able, in fact, to repel the cybersecurity event. In addition, disseminating information regarding unsuccessful intrusions could result in the threat actors being unnecessarily alerted that they have been detected, which could make it more difficult to identify the attackers and halt their efforts on an ongoing, more permanent basis. Therefore, the SEC proposes to exclude systems intrusions that are significant attempted unauthorized entries into the SCI systems or indirect SCI systems of an SCI entity from the information dissemination requirements of Rule 1002(c)(1)-(3).[32]

D. SCI Review

The SEC proposes to revise the requirements relating to SCI reviews, including proposed changes to the definition of "SCI review," the requirements for an SCI review and the reports related to SCI review that SCI entities submit both to the SEC and their board of directors.

1. Definition of 'SCI Review' in Rule 1000

[30] Rule 1002(b)(5) of Reg SCI.

[31] Rule 1002(b) provides the framework for notifying the SEC of SCI events, including, among other things, requirements to notify the Commission of the event immediately; provide a written notification on Form SCI within 24 hours that includes a description of the SCI event and the system(s) affected, with other information required to the extent available at the time; provide regular updates regarding the SCI event until the event is resolved; and submit a final detailed written report regarding the SCI event.

[32] Proposed Rule 1002(c)(4)(iii) of Reg SCI.

The SEC proposes to revise and expand the definition of "SCI review" in a variety of ways.[33] The SEC proposes to revise the lead-in provision to the definition of "SCI review" to require SCI entities and the objective personnel conducting SCI reviews to document the work that is done during the SCI review and to require the SCI review to use "appropriate risk management methodology."

Proposed paragraph (1) of the definition of "SCI review" sets forth three specific assessments to be performed. The SEC proposes to revise the lead-in to this paragraph to indicate that the three required assessments of the SCI review would apply to each individual SCI system and indirect SCI system and to require that each of these assessments be performed by objective personnel.

In the current definition of "SCI review" in Rule 1000, the first required assessment for an SCI review is "a risk assessment with respect to such systems of an SCI entity." The SEC proposes to replace this requirement with an assessment of "the risks related to the capacity, integrity, resiliency, availability, and security" of each such system.[34] The SEC believes that the additional detail in the proposed language would tie the required risk assessment more closely to the key principles of Reg SCI relating to the "capacity, integrity, resiliency, availability and security" of each SCI entity's systems while maintaining the focus of the assessment on the overall risks associated with such systems.

An SCI review currently is required to contain a second assessment—"[a]n assessment of internal control design and effectiveness of its SCI systems and indirect SCI systems to include logical and physical security controls, development processes, and information technology governance, consistent with industry standards."[35] The SEC proposes to revise the phrase "internal control design and effectiveness" in this provision to read "internal control design and operating effectiveness" to clarify that the associated assessment must examine how well the internal controls performed in actual operations, i.e., in practice, not just in theory.[36] The SEC also proposes to expand the list of controls to be assessed as set forth in the definition by adding "systems capacity and availability" and "information technology service continuity."[37]

The SEC also proposes to require an SCI review to include a third assessment—an assessment of third-party provider management risks and controls with respect to each of its SCI systems and indirect SCI systems.[38] This provision is related to the enhanced requirements discussed above regarding third-party provider management.

[33] Proposed definition of "SCI review" in Rule 1000 of Reg SCI.

[34] Proposed paragraph (1)(i) of the definition of "SCI review" in Rule 1000.

[35] Paragraph (2) of the definition of "SCI review" in Rule 1000.

[36] Proposed paragraph (1)(ii) of the definition of "SCI review" in Rule 1000.

[37] *Id.*

[38] Proposed paragraph (1)(iii) of the definition of "SCI review" in Rule 1000.

The SEC also proposes to add a new paragraph to the definition of "SCI review" related to penetration test reviews. As discussed above with regard to penetration testing, this new paragraph would include within an SCI review "[p]enetration test reviews performed by objective personnel of the network, firewalls, and production systems, including of any vulnerabilities of its SCI systems and indirect SCI systems identified pursuant to § 242.1001(a)(2)(iv)."[39]

In addition, Rule 1003(b)(1)(ii) currently allows assessments of SCI systems directly supporting market regulation or market surveillance to be conducted, based on a risk assessment, at least once every three years rather than annually. The SEC proposes to move this requirement from Rule 1003 to the definition of "SCI review."[40]

2. Requirements for SCI Review: Rule 1003(b)

The SEC proposes to revise Rule 1003(b)(2) to set forth specific requirements for the contents of the report of the SCI review.[41] Specifically, the SEC proposes to require the report of the SCI review to include:

- the dates the SCI review was conducted and the date of completion;
- the entity or business unit of the SCI entity performing the review;
- a list of the controls reviewed and a description of each such control;
- the findings of the SCI review with respect to each SCI system and indirect SCI system, which must include, at a minimum, assessments of the risks related to capacity, integrity, resiliency, availability and security; internal control design and operating effectiveness; and vendor management risks and controls;
- a summary, including the scope of testing and resulting action plan, of each penetration test review conducted as part of the SCI review; and
- a description of each deficiency and weakness identified by the SCI review.[42]

[39] Proposed paragraph (2) of the definition of "SCI review" in Rule 1000.

[40] Proposed paragraph (3) of the definition of "SCI review" in Rule 1000.

[41] Rule 1003(b)(1) states that each SCI entity shall "[c]onduct an SCI review of the SCI entity's compliance with Reg SCI not less than once each calendar year." The SEC proposes to amend this provision to state that if an SCI entity is an SCI entity for any part of the calendar year, it must conduct the SCI review and submit the associated report of the SCI review to the SCI entity's senior management and board as well as to the SEC. In addition, as discussed above, the SEC also proposes to move the requirements set forth in Rule 1003(b)(1)(i) and (ii) of Reg SCI to the definition of "SCI review" in Rule 1000 of Reg SCI.

[42] Proposed Rule 1003(b)(2) of Reg SCI.

3. *Reports of SCI Reviews*

The SEC proposes to revise the requirements related to the submission of the report of the SCI review to the SEC and to the board of directors (or its equivalent) of the SCI entity.[43] The proposed revisions would require that when the report is submitted to the board of directors of the SCI entity and the SEC, it must also include the date the report was submitted to senior management. In addition, the revisions would make it mandatory to include a response from senior management to the report when it is submitted to the SEC and the board, whereas previously the language appeared permissive.

E. Current SCI Industry Standards

Rule 1001(a)(4) of Reg SCI states that an SCI entity's policies and procedures will be deemed to be reasonably designed if they are consistent with "current SCI industry standards." SCI entities are not required to avail themselves of the safe harbor of Rule 1001(a)(4) by aligning their policies and procedures required by Rule 1001(a) with current SCI industry standards.[44] If an SCI entity chooses to rely on this safe harbor, however, the SEC proposes to require such SCI entity's policies and procedures to include "[a]n identification of the current SCI industry standard(s) with which each such policy and procedure is consistent, if any."[45]

F. Other Changes

The SEC proposes two additional changes to Reg SCI requirements:

- The SEC proposes to modify Form SCI to reflect the changes discussed above.
- The SEC proposes to clarify that the requirement to make, keep and preserve for five years certain records related to compliance with Reg SCI survives even if an SCI entity ceases to do business or ceases to be registered under the Exchange Act.[46] For example, this provision would require an SCI ATS that no longer satisfies a volume threshold to make, keep and preserve its records related to its compliance with Reg SCI related to the period during which it was an SCI entity for the applicable remainder of the five years.

[43] Proposed Rule 1003(b)(3) of Reg SCI.

[44] To make clear that Rule 1001(a)(4)'s reference to and definition of "current industry standards" provides a safe harbor for SCI entities with respect to their policies and procedures, the SEC proposes to add the words "safe harbor" to Rule 1001(a)(4).

[45] Proposed Rule 1001(a)(2)(xi) of Reg SCI.

[46] Proposed Rule 1005(c) of Reg SCI.

Contributors

Andre E. Owens

PARTNER

andre.owens@wilmerhale.com

+1 202 663 6350

Cherie Weldon

SPECIAL COUNSEL

cherie.weldon@wilmerhale.com

+1 212 230 8806

Wilmer Cutler Pickering Hale and Dorr LLP is a Delaware limited liability partnership. WilmerHale principal law offices: 60 State Street, Boston, Massachusetts 02109, +1 617 526 6000; 2100 Pennsylvania Avenue, NW, Washington, DC 20037, +1 202 663 6000. Our United Kingdom office is operated under a separate Delaware limited liability partnership of solicitors and registered foreign lawyers authorized and regulated by the Solicitors Regulation Authority (SRA No. 287488). Our professional rules can be found at www.sra.org.uk/solicitors/code-of-conduct.page. A list of partners and their professional qualifications is available for inspection at our UK office. In Beijing, we are registered to operate as a Foreign Law Firm Representative Office. This material is for general informational purposes only and does not represent our advice as to any particular set of facts; nor does it represent any undertaking to keep recipients advised of all legal developments. Prior results do not guarantee a similar outcome.