KPMG

Regulatory Alert

Regulatory Insights for Financial Services

March 2023

SEC Proposal to Expand Regulation SCI

***KPMG Regulatory Insights**:*

- *The expansion of Regulation SCI to SBSDRs, exempt clearing agencies, and broker-dealers meeting certain asset or trading thresholds follows an earlier proposal to expand the applicability of the rules to certain alternative trading systems (see KPMG Regulatory Alert, here.)*
- *Key areas of focus include: i) written policies and procedures, ii) incident notification, and iii) systems reviews and testing.*
- *Other cyber-related proposals released the same day address cybersecurity risk management for market entities and enhancements to Regulation S-P.*

The Securities and Exchange Commission (SEC) released proposed amendments to expand and update the provisions of Regulation SCI (Systems Compliance and Integrity).

The proposal is part of a comprehensive effort by the SEC to enhance cybersecurity preparedness and resilience across all registrants of the SEC.

Proposed Amendments to Regulation SCI

The SEC proposed amendments to Regulation SCI, the rules that lay out the obligations and requirements around the resiliency of technology infrastructure in the U.S. securities markets. The proposed amendments both expand the definition of "SCI Entities" to include a broader range of market participants and update Regulation SCI's rules to account for technology developments, as outlined below.

SCI Entities. The proposed amendments would expand the definition of "SCI Entities" to include:

- Registered Security-Based Swap Data Repositors (SBSDRs).
- All clearing agencies exempted from registration.
- SEC-registered broker-dealers exceeding one or more size thresholds ("SCI broker-dealers"):
  - Total Asset Threshold: In at least two of the four preceding calendar quarters reported to the SEC (on Form X-17A-5) total assets in an amount that equals five (5) percent or more of the total assets of all security brokers and dealers.
  - Transaction Activity Threshold: During at least four of the preceding six calendar months had transaction activity (purchases and sales) equaling ten (10) percent or more of average daily dollar volume in NMS stocks, exchange-listed options, U.S Treasury securities, and/or agency securities.

Regulation SCI Updates. The proposed amendments would update the obligations of SCI Entities in the following areas:

- **Policies and Procedures:** Specify that under Rule 1001(a), an SCI entity's required policies and procedures must include:
  - Systems Classification and Lifecycle Management: A written inventory, classification, and lifecycle management program for SCI systems and indirect SCI systems.
  - Third-Party Provider Management: Program(s) to manage and oversee third-party service providers, including cloud service providers, that provide or

support SCI or indirect SCI systems. Includes a requirement to conduct a risk-based assessment of the criticality of each third-party provider as well as concentrations, key dependencies, and potential security risks.

- Business Continuity and Disaster Recovery: "BC/DR" Plans that address the unavailability of any third-party provider without which there could be a material impact on critical SCI systems. (The proposal also specifies that SCI entities include key third-party providers in annual BC/DR testing.)
- Cybersecurity: Program(s) to prevent unauthorized access to SCI systems, indirect SCI systems, and information.
- Industry Standards: Identification of current SCI industry standards and policy and procedure alignment, if applicable.

— **"Systems Intrusion":** Amend the definition of "systems intrusion" under Rule 1000 to mean "any unauthorized entry into the SCI systems or indirect SCI systems of an SCI entity." This could include additional types of cyber events and threats and is intended to capture cybersecurity events such as certain distributed denial-of-service attacks and to require notification of all systems intrusions to the SEC "immediately".

— **SCI Reviews:** Update provisions of Rule 1000 regarding the SCI review process to require three assessments to be performed by "objective personnel". The assessments would include:

- Risks to related to the capacity, integrity, resiliency, availability, and security of the covered systems.
- Internal control design and operating effectiveness, to include logical and physical security controls, development processes, systems capacity and availability, information technology service continuity, and information technology governance, consistent with industry standards.
- Third-party provider management risks and controls with respect to each of its SCI systems and indirect SCI systems, as well as require annual systems penetration testing.

— **Recordkeeping:** Updating existing Regulation SCI recordkeeping provisions and Form SCI (Rules 1005 – 1007) consistent with the other proposed amendments.

Comment Period. The SEC is seeking public comment on the proposed rule. The comment period will remain open for 60 days following publication in the Federal Register.

For more information, please contact Matt Miller, Steve Stein, or Mike Sullivan.

Contact the author:

Amy Matsuo
Principal and National Leader
Regulatory Insights
amatsuo@kpmg.com