KPMG

Regulatory Alert

Regulatory Insights

January 2022

Cybersecurity: SEC Reg SCI Proposal, Future Considerations

SEC is expected to issue climate, human capital, and cyber risk governance disclosure requirements this year. In a clear indication of activity in the cyber area, the SEC has denoted key areas of upcoming focus that address strengthening the "cyber hygiene" of SEC registrants (practices to maintain the security of devices, networks, and data) and improving the timing and content of cyber incident notifications and disclosures to clients, investors, and the SEC. Proposals to amend Reg SCI would extend requirements intended to protect the resiliency of technology infrastructures (including business continuity plans, testing protocols, data backups, incident reporting) to reach an expanded number of registrants. Notably, Chair Gensler is considering how to expand oversight of the cyber risks posed by certain service providers, calling out the federal banking regulators oversight model as an example; the federal banking regulators recently finalized cyber incident notification rules that cover both banking entities and certain of their service providers.

The Biden Administration, citing "persistent and increasingly sophisticated cyber campaigns", has called for government-wide improvements to national cybersecurity defenses. To this end, the SEC announced a number of planned actions.

Reg SCI

The SEC proposed amendments to Regulation Systems Compliance and Integrity (Reg SCI - a rule intended to strengthen the resiliency of technology infrastructure in the U.S. securities markets) that would expand the applicability of the rule to alternative trading systems (ATSs) that meet certain trading volume thresholds (as defined in the rule) with respect to U.S. Treasury Securities and/or Agency Securities. The amendments, which were first proposed in 2020, are included as part of a larger proposed rule that would expand the definition of an "exchange" under Regulation ATS and bring Treasury market platforms with "significant volume" within the regulatory framework.

Entities subject to Reg SCI are required to:

- Establish, maintain, and enforce written policies and procedures reasonably designed to ensure that key automated systems have levels of capacity, integrity, resiliency, availability, and security adequate to maintain their operational capability and promote the maintenance of fair and orderly markets.
- Take appropriate corrective action when systems issues occur, provide certain notifications and reports to the SEC regarding systems problems and systems changes, inform members and participants about systems issues, conduct business continuity and disaster recovery testing, conduct annual reviews of their automated systems, including penetration testing, and make and keep certain books and records.

Additional Steps

In addition to the Reg SCI and Reg ATS proposal, SEC Chair Gensler, speaking to the Securities Regulation Institute, provided several insights on the direction of

other rule proposals that are currently under consideration to "improve the overall cybersecurity posture and resiliency of the financial sector," including:

- ***Funds, Advisers, Broker-Dealers***. Building on current requirements, the SEC is considering proposals to strengthen these registrants' cybersecurity hygiene and incident reporting with an eye to giving clients and investors better information, incentivizing cyber hygiene improvements, and providing the SEC with more insight into cyber risks.
- ***Data privacy***. Updates to Regulation S-P could "modernize and expand" the rule. Key features being considered include the timing and substance of customer and client notifications regarding cyber events and data breaches.
- ***Disclosure requirements***. Updates to public company disclosures would be two-fold.
  - *Cyber events*. SEC staff is considering how to update disclosures to investors when a cyber event has occurred; Chair Gensler stressed accuracy and materiality to investors as pertinent issues.
  - *Practices and risks*. SEC staff is considering disclosures related to cybersecurity practices (such as governance, strategy, and risk management) and cyber risk. Chair Gensler added that companies and investors would benefit from these disclosures being presented in a "consistent, comparable, and decision-useful manner." (*Note:* The SEC's Fall 2021 Regulatory Agenda lists a proposed rulemaking expected to be released in the second quarter of 2022 covering enhanced disclosure for cybersecurity risk and related governance.)
- ***Service providers***. Chair Gensler noted that banking agencies directly regulate and supervise certain bank's third-party service providers through statutory authority, and it may be useful to provide similar authorities to market regulators. (*See related KPMG Regulatory Alert on Cyber incident notifications, here*.) SEC staff is currently considering potential measures to address cybersecurity risk from service providers, including:
  - Requiring certain registrants to identify service providers that could pose such risks.
  - Holding registrants accountable for service providers' cybersecurity measures with respect to protecting against inappropriate access and investor information.

Please refer to:

- Press Release: SEC Proposes Amendments to Include Significant Treasury Markets Platforms Within Regulations ATS/SCI
- SEC Speech: Cybersecurity and Securities Laws
- KPMG Regulatory Alert | Cyber incident notifications

For additional information, please contact Matt Miller or Mike Sullivan.

Contact the author:

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

kpmg.com/socialmedia