

SEC Chair: Sweeping New Cybersecurity Rules Are Coming Soon

February 8, 2022

On Monday, January 24, 2022, in a [speech](#) at the Northwestern University Pritzker School of Law annual Securities Regulation Institute conference, Gary Gensler, Chair of the U.S. Securities and Exchange Commission (SEC), announced that he has asked SEC staff to provide sweeping rulemaking recommendations to modernize and expand the agency's rules relating to cybersecurity.¹ Stressing that cybersecurity is a matter of national security, Chair Gensler signaled that new guidance or proposed rules would enhance or expand public company cybersecurity programs and risk disclosures; cybersecurity program requirements and breach notification obligations for SEC regulated entities under Reg S-P; and the scope of registrants covered under Regulation Systems Compliance and Integrity (Reg SCI). He also signaled the SEC's continued focus on enforcement and cooperation with other law enforcement agencies.²

These SEC rules could broadly affect cybersecurity requirements across the U.S. securities markets, including for public securities issuers, SEC registrants (such as broker-dealers, investment advisers, investment companies, self-regulatory organizations (SROs), and alternative trading systems (ATs)), and service providers to issuers and SEC-registered entities.

Given the potential scope and reach of the new rules, firms should monitor these developments and begin to consider how they may wish to comment on the SEC's proposals and advocate with the agency to ensure that the SEC adopts final rules that are well informed, are harmonious with other relevant and well-developed cybersecurity compliance regimes, and will not impose inappropriate costs and compliance burdens. Below, we summarize the areas of SEC focus and identify related considerations, including certain guidance and best practices regarding existing SEC cybersecurity requirements.

Public Companies and Service Providers

Public companies currently must disclose material cybersecurity incidents. For example, SEC guidance from 2018 emphasizes that there is a range of factors that may affect whether an incident should be disclosed to investors beyond the bottom-line financial costs to respond to the incident. However, Chair Gensler highlighted that disclosure regimes evolve over time and stated that he has asked the staff to make recommendations related to public companies' cybersecurity practices and cyber risk disclosures as well as disclosures that must be made once cyber events have occurred. Reflecting on the wide range of disclosure practices around cyber risks and incidents, Chair Gensler stressed the need to ensure that cyber-related disclosures are "presented in a consistent, comparable, and decision-useful

manner.”

Chair Gensler also stressed the importance of proper disclosure regimes for non-public-company service providers — including, for example, cloud companies, investor reporting systems and providers, and data analytics. He has asked the staff to make recommendations for how to address cybersecurity risk that comes from service providers — which could include reporting requirements that hold companies accountable for certain of their service providers’ cybersecurity measures. The impending emphasis on supply chain risk is not a surprise, however, in light of the SEC’s numerous information requests in 2021 connected to the Solar Winds vulnerability.

Chair Gensler’s most recent speech and any forthcoming SEC proposals or guidance may also signal the SEC’s continued focus on cyberenforcement. In May 2021, at a speech at the 2021 Financial Industry Regulatory Authority (FINRA) annual conference, for example, Chair Gensler emphasized that the SEC (as well as FINRA) should be ready to bring more cases related to cyber.³ In June 2021, the SEC settled charges against First American Title Insurance Company, which had alleged improper disclosures related to a cybersecurity vulnerability because senior executives were not provided all available and relevant information and First American’s information security personnel had identified and failed to remediate the vulnerability months earlier.⁴ In August 2021, the SEC settled charges with Pearson plc, which had alleged that Pearson did not patch a known critical vulnerability and issued a public statement concerning a data incident that did not accurately disclose the scope of affected data.⁵

Best Practices for Public Companies

- **Consider OCIE Cybersecurity and Resiliency Practices:** In 2020, the Office of Compliance Inspections and Examinations (OCIE) published exam observations that discuss several industry practices, including governance and risk management; access rights and controls; data loss prevention; mobile security; incident response and resiliency; vendor management; and training and awareness.⁶ Companies should familiarize themselves with the SEC’s view of best practices and trends of industry failures when considering programmatic risk assessments and project prioritization.
- **Embrace Commission Statement and Guidance on Public Company Disclosures:** While the SEC will likely update this 2018 guidance, public companies should establish reporting processes to support risk disclosures, which should “enable companies to identify cybersecurity risks and incidents assess and analyze their impact on a company’s business evaluate the significance associated with such risks and incidents provide for open communications between technical experts and disclosure advisers and make timely disclosures regarding such risks and incidents.”⁷
- **Stay Up to Date on SEC Alerts Related to Cybersecurity:** For instance, in 2020 the Division of Examinations published three alerts related to cybersecurity (OCIE Cybersecurity and Resiliency Practices; Ransomware Alert; and Safeguarding Client Accounts against Credential Compromise).⁸
- **Establish and Implement Proper Policies and Procedures:** The orders against First American and Pearson highlight the importance of maintaining policies and procedures for the reporting of security incidents and patching as well as the proper training of personnel under these policies and procedures.

- **Assess All Public Statements:** As the SEC is focused on communications that may affect investor decision-making, companies should ensure that legal and IT review all public statements concerning cyberevents or cybersecurity.
- **Conduct Third-Party Diligence on Third Parties:** The SEC's interest in service parties is not new, as the SEC announced in 2021 an investigation into companies affected by the cyberattack of SolarWinds Corp.'s software.⁹ In this context, companies should consider reviewing the "Vendor Management" section of the OCIE Cybersecurity and Resiliency Practices observations.

SROs and ATSS Covered by Regulation Systems Compliance and Integrity

In addition to SEC regulations that apply to public companies regarding cybersecurity, the agency's Reg SCI regime under the Securities Exchange Act imposes capacity, integrity, resiliency, and security requirements on the systems of certain SEC registrants that act as key intermediaries in the U.S. financial markets. Specifically, Reg SCI applies to clearing agencies, national securities exchanges that are SROs under the Securities Exchange Act, and certain ATSS operated by broker-dealers that meet specified securities volume thresholds.¹⁰ The highly prescriptive requirements that Reg SCI imposes on covered SCI entities regarding systems' capacity, integrity, resiliency, availability, and security are pervasive, onerous, and costly.

The headline from Chair Gensler's speech regarding Reg SCI is that the SEC will again consider expanding it to cover other entities not currently covered, including broker-dealers that are large market makers and other categories of broker-dealers. When Reg SCI was proposed, the SEC solicited comment on whether it should cover more categories of broker-dealers besides certain ATS operators and whether it should also cover such entities as SEC-registered transfer agents and investment advisers.¹¹ But the SEC declined to go that far when it adopted Reg SCI. In the aftermath of 2021 market volatility relating to meme stock trading, however, and given the increasingly important role played by some broker-dealers that operate as over-the-counter (OTC) market makers, the SEC appears poised to revisit whether those broker-dealer market participants and potentially others may have to comply with Reg SCI.¹²

The intersection of cybersecurity and U.S. national security arises under Reg SCI as well. One area of Reg SCI compliance that recently has been a focus for the SEC and Reg SCI entities is the use of cloud services and related national security concerns that may be raised if the availability zones used in such services are not entirely located within the United States. Because the SEC's adopting release for Reg SCI and related SEC staff guidance does not specifically address the use of cloud services, this is an area that may be ripe for further SEC rulemaking or guidance. The SEC may also consider updating its guidance on industry best practices, which SCI entities must follow, from the existing guidance that the SEC staff provided in 2014.¹³

Investment Companies, Investment Advisers, and Broker-Dealers

Beyond potential expansion of Reg SCI to apply to more types of SEC registrants, Chair Gensler also stated that the agency will focus modernizing rules for investment companies, investment advisers, and broker-dealers to reduce cybersecurity risks, focusing on "cybersecurity hygiene and incident reporting." Specifically regarding cybersecurity hygiene and incident reporting, he noted that the agency will focus on new regulations that could reduce the risk that investment companies, investment advisers, and

broker-dealers would not be able to maintain critical operational capability during a significant cybersecurity incident. He noted that an additional goal could be the implementation of regulations that would provide the SEC with more information and insights regarding cyber risks at these firms.

SEC Reg S-P requires SEC-registered investment companies, investment advisers, and broker-dealers to protect customer records and information. The SEC may consider several revisions to this regulation. Namely, Chair Gensler indicated that the SEC will review how customers and clients receive notices regarding cyberevents when their data has been accessed, and he stated that amendments to Reg S-P could alter the timing and substance of required notifications.

Subsequent to Chair Gensler's speech, the SEC provided public notice that at an upcoming open meeting it will consider whether to propose new rules to address cybersecurity risk management for registered investment advisers and investment companies as well as related amendments to rules regarding adviser and fund disclosures.¹⁴

On February 9, 2022, the SEC voted to propose rules for registered investment advisers and funds, titled as the Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies.¹⁵ The proposed rules includes requirements that advisers and funds: implement written policies and procedures designed to address cybersecurity risks; report significant cybersecurity incidents to the SEC on a proposed form; and, maintain, make, and retain certain cybersecurity-related books and records. A public comment period will follow.

Service Providers

In what may have the most far-reaching implications in Chair Gensler's speech regarding the SEC's cybersecurity regulations, he stated that the SEC staff will investigate ways in which the agency could further address cybersecurity risks that stem from service providers to public securities issuers and SEC registrants. In particular, he noted that the ways U.S. banking regulators already directly regulate and supervise service providers to banks under the Bank Service Company Act could provide a model for similar SEC regulations. Chair Gensler named an array of financial sector service providers that play critical roles and, presumably, could be subject to future regulatory action including investor reporting systems and providers, middle-office service providers, fund administrators, index providers, custodians, data analytics, trading and order management, and pricing and other data services, among others.

Direct regulation and supervision of these and potentially other types of service providers would be a new paradigm in much of the SEC's current approach to relationships between regulated entities and their service providers. For example, Reg SCI contemplates that covered entities may receive services from third parties or even contract with a third party to operate SCI systems on their behalf.¹⁶ However, the SCI entity remains responsible for having appropriate processes and requirements in place to ensure that it is able to satisfy the requirements of Reg SCI, and the SEC does not gain direct supervisory authority over the third party by virtue of the outsourcing.

¹ Chair Gary Gensler, *Cybersecurity and Securities Laws*, SEC (Jan. 24, 2022), <https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124>.

² As an example of this focus on interagency coordination, in December 2021, the Department of Justice announced that it had coordinated with the SEC to investigate and extradite a group of Russians that

hacked into the computer networks of vendors used by public companies to submit filings to the SEC. See *Russian National Extradited for Role in Hacking and Illegal Trading Scheme*, DOJ (Dec. 20, 2021), <https://www.justice.gov/usao-ma/pr/russian-national-extradited-role-hacking-and-illegal-trading-scheme>.

³ Chair Gary Gensler, *Remarks at 2021 FINRA Annual Conference*, SEC (May 20, 2021), <https://www.sec.gov/news/speech/gensler-finra-conference>.

⁴ See Alan Raul et al., *SEC Announces Settled Charges Against First American for Cybersecurity Disclosure Controls Failures – Lessons Learned*, SIDLEY DATA MATTERS (June 24, 2021), <https://datamatters.sidley.com/sec-announces-settled-charges-against-first-american-for-cybersecurity-disclosure-controls-failures-lessons-learned>.

⁵ See Alan Raul et al., *SEC Continues Focus on Cybersecurity Disclosure Failures, Announces Settled Charges Against Pearson plc*, SIDLEY DATA MATTERS (Aug. 30, 2021), <https://datamatters.sidley.com/sec-continues-focus-on-cybersecurity-disclosure-failures-announces-settled-charges-against-pearson-plc>.

⁶ *Cybersecurity and Resiliency Observations*, SEC (Jan. 27, 2020), available at <https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf>.

⁷ 17 CFR Parts 229 and 249 (Feb. 26, 2018), available at <https://www.sec.gov/rules/interp/2018/33-10459.pdf>.

⁸ See, e.g., Division of Examinations Announcements, available at <https://www.sec.gov/exams/announcements>.

⁹ See *In the Matter of Certain Cybersecurity-Related Events (HO-14225) FAQs*, SEC (June 25, 2021), <https://www.sec.gov/enforce/certain-cybersecurity-related-events-faqs>.

¹⁰ Reg SCI also applies to the securities information processors that produce consolidated market data for NMS securities, including competing consolidators under the SEC's new market data infrastructure rules once implemented. For more information, please see Sidley's client alert on the SEC's market data infrastructure rules available [here](#).

¹¹ See Securities Exchange Act Release No. 73639 (November 19, 2014), 79 FR 72252 (December 5, 2014), <https://www.govinfo.gov/content/pkg/FR-2014-12-05/pdf/2014-27767.pdf>.

¹² For example, the SEC staff found that although executions appeared to shift more toward exchanges as volatility increased in January 2021, 80% of OTC volume occurred against OTC market makers rather than ATSs and 88% of that volume against just three market makers. See SEC Staff Report on Equity and Options Market Structure Conditions in Early 2021 at 35-37 (Oct. 14, 2021), <https://www.sec.gov/files/staff-report-equity-options-market-struction-conditions-early-2021.pdf>. OTC market makers therefore may have been more important sources of liquidity than ATSs and therefore in greater need enhanced cyber and operational protections pursuant to Reg SCI.

¹³ See SEC Staff Guidance on Current SCI Industry Standards (Nov. 19, 2014), <https://www.sec.gov/rules/final/2014/staff-guidance-current-sci-industry-standards.pdf>.

¹⁴ See SEC Open Meeting Agenda (February 9, 2022), <https://www.sec.gov/os/agenda-open-020922>.

¹⁵ SEC Proposes Cybersecurity Risk Management Rules and Amendments for Registered Investment Advisers and Funds, SEC (Feb. 9, 2022), <https://www.sec.gov/news/press-release/2022-20>.

¹⁶ See SEC Staff Responses to Frequently Asked Questions Concerning Reg SCI. Question 2.03 (Updated August 21, 2019), <https://www.sec.gov/divisions/marketreg/regulation-sci-faq.shtml>.

CONTACTS

If you have any questions regarding this Sidley Update, please contact the Sidley lawyer with whom you usually work, or

Andrew P. Blake , Partner	+1 202 736 8977, ablake@sidley.com
Colleen Theresa Brown , Partner	+1 202 736 8465, ctbrown@sidley.com
Andrew J. Sioson , Partner	+1 202 736 8351, asioson@sidley.com
Charles A. Sommers , Partner	+1 202 736 8125, csommers@sidley.com
Sasha Hondagneu-Messner , Managing Associate	+1 212 839 5403, shondagneumessner@sidley.com

Attorney Advertising—Sidley Austin LLP is a global law firm. Our addresses and contact information can be found at www.sidley.com/en/locations/offices.

Sidley provides this information as a service to clients and other friends for educational purposes only. It should not be construed or relied on as legal advice or to create a lawyer-client relationship. Readers should not act upon this information without seeking advice from professional advisers. Sidley and Sidley Austin refer to Sidley Austin LLP and affiliated partnerships as explained at www.sidley.com/disclaimer.

© Sidley Austin LLP