BCLP. Client Intelligent

Insights

SEC'S GENSLER: MAJOR CYBERSECURITY REGULATORY CHANGES ON THE HORIZON

Jan 31, 2022

SUMMARY

A significant expansion of rules relating to cybersecurity risks—particularly for the financial sector—is under consideration by the Securities and Exchange Commission (SEC).

In public remarks last week, SEC Chair Gary Gensler previewed a number of areas in which the SEC is looking to "broaden and deepen" its oversight of cybersecurity practices and risks. They range from a broad expansion of system integrity rules to changes involving the timing and delivery of privacy notices. Although new rules governing cybersecurity disclosures have been anticipated for months, Gensler's remarks indicate that the SEC's plans go well beyond disclosure rules and are far more ambitious.

Changes Likely for the Financial Sector and Its Service Providers

Extension of Reg SCI to "Large, Significant" Entities. One of the most far-reaching changes being considered involves broad expansion of the Regulation Systems Compliance and Integrity Rule (Reg SCI).

Reg SCI, adopted in November 2014, applies to entities that form the backbone of U.S. financial markets: self-regulatory organizations, including the securities and options exchanges, clearing agencies, FINRA, and the Municipal Securities Rulemaking Board (MSRB), as well as certain alternative trading systems (ATSs) and plan processors involved in distributing transaction and quotation information.

Reg SCI requires these covered entities to have policies and procedures in place to protect systems integral to key market functions: trading, clearance and settlement, order routing, market data, market regulation and surveillance. Reg SCI also requires covered entities to take corrective action and immediately notify the SEC if certain events occur. It further requires them to provide quarterly reports, conduct annual reviews and tests, and maintain books and records.

According to Gensler, the SEC is considering expanding Reg SCI to include "large, significant entities" such as market-makers, broker-dealers and Treasury trading platforms. The SEC took the first step just days after Gensler's speech and proposed new rules that would require ATSs that trade government securities to comply with Reg SCI.

The other "large, significant entities" that might become subject to Reg SCI remain to be seen. Large market-makers and broker-dealers will certainly be on the list, but other large entities supporting these market functions should be watching developments closely. Even if these entities already have sophisticated controls in place, the additional event notification, reporting, review and testing required by Reg SCI—all under the SEC's scrutiny—will present additional challenges.

Gensler also announced that the SEC is looking at ways "to deepen" Reg SCI to "shore up the cyber hygiene of important financial entities." He provided no further details, so it is not clear what the SEC is planning to do here. Perhaps specific technical safeguards will be required, such as encryption and multi-factor authentication, along with other such measures.

New Rules for Investment Companies, Investment Advisers and Broker-Dealers. Beyond Reg SCI, Gensler also announced that the SEC is considering new rules for investment funds, advisers and broker-dealers. Here, the SEC is focusing on ways to strengthen "cybersecurity hygiene and incident reporting." These changes would ensure entities continue to operate during significant incidents, provide clients and investors with better information, give the SEC "more insight into intermediaries' cyber risks," and create incentives to "improve cyber hygiene." Gensler offered no particulars but indicated that guidance was being drawn from the Cybersecurity and Infrastructure Security Agency (CISA) and "others." The "incentives" proposed to improve "cyber hygiene" will be of particular interest. They could range anywhere from safe harbors that encourage reporting to new attestation requirements with strict penalties.

Expanded Authority Over Financial Sector Service Providers. Another potentially far-reaching change being considered would give the SEC authority over third-party service providers that provide various administrative and technical services to financial sector registrants. Here, the SEC is reportedly considering "a variety of measures" such as requiring registrants to identify service providers that might pose cyber risks, and holding registrants accountable for service providers' cybersecurity measures.

Gensler, however, also expressed interest in a far more sweeping change: giving "market regulators" the same type of power over third-party service providers that bank regulators have under the Bank Service Company Act. That Act subjects third parties performing certain services for banks, (e.g., data processing, Internet banking and mobile banking services), to regulation and examination by the bank regulators to the same extent as the banks themselves. If enacted, such a law potentially would give the SEC authority over the systems and operations of cloud service providers and payment processors, to name a few.

Reg S-P Notifications. According to Gensler, the SEC is also looking at ways to "modernize and expand" Reg S-P. Currently, Reg S-P requires brokers, dealers, investment companies and advisers to provide privacy notices to customers and have written policies and procedures in place to safeguard customer information. The potential changes, Gensler explained, would relate to *how* notification is given to clients when their personal information has been accessed, as well as the "timing and substance of notifications currently required." Although not entirely clear, the SEC may be considering a new breach notification rule as well as updates to existing privacy notice forms.

New Disclosure Rules for Public Companies

Gensler also confirmed that the SEC is looking at new rules involving cybersecurity risk disclosures and practices that would be applicable to all public companies.

Cybersecurity Risk Disclosures. According to Gensler, the SEC is considering ways in which cybersecurity risk information can be presented by issuers in a "consistent, comparable, and decision-useful manner." The SEC also is examining "whether and how to update disclosures" when cybersecurity events have occurred. Although no specifics were provided, proposed mandatory disclosures for cybersecurity risks, along with guidance for assessing the materiality of cyber events, may be expected.

Cybersecurity Practices. The SEC is also apparently preparing recommendations around company practices with respect to "cybersecurity governance, strategy, and risk management." These issues have been the subject of SEC guidance, risk alerts and enforcement actions for the past several years. Look for proposed rules addressing internal controls for reporting cybersecurity risks and incidents and additional safeguards to protect customer information.

The SEC has staked out a very ambitious cybersecurity agenda for the months ahead. We'll be following developments and provide updates as they occur.

RELATED PRACTICE AREAS

- Securities Litigation and Enforcement
- Data Privacy & Security
- Financial Regulation Compliance & Investigations
- Securities & Corporate Governance

MEET THE TEAM

Lori Van Auken

New York
lori.vanauken@bclplaw.com
+1 212 541 2053
