Data Privacy and Cybersecurity
Investigations, Compliance, and Defense
Securities Litigation and Enforcement
Markets and Trading

Securities and Exchange Commission Chair Emphasizes SEC's Role in Cybersecurity and Suggests Additional Cybersecurity Regulations are on the Horizon

By: Charles D. Riely, Shoba Pillay, Gregory M. Boyle, and Karolina L. Bartosik

In a speech to the Securities Regulation Institute conference last week, Chair Gary Gensler signaled the SEC may implement more stringent cybersecurity regulations, and in the meantime, would work to enforce existing requirements. Since taking office in 2021, Mr. Gensler has often referred to the need for the SEC to be a "cop on the beat" to root out misconduct and address potential risk to investors.[1] It has become increasingly clear that Mr. Gensler views addressing cybersecurity risk and misconduct as an important part of this work. In 2021, the SEC brought several actions against financial services firms or public companies that allegedly failed to heed their obligations under the federal securities law.[2] Mr. Gensler focused on the role the SEC should play in a collaborative effort across federal agencies and the private sector to promote robust cybersecurity. Here are some key takeaways from Mr. Gensler's comments.

Defining the SEC's Role in "Team Cyber"

Mr. Gensler framed cybersecurity as critical to a strong financial system and overall economic stability, especially as the financial sector has "become increasingly embedded with society's critical infrastructure."[3] He described a technological landscape that includes "the interconnectedness of our networks, the use of predictive data analytics, and the insatiable desire for data."[4] The SEC's role within this context is to "improve the overall cybersecurity posture and resiliency of the financial sector" in collaboration with other government entities Mr. Gensler named, including the Federal Bureau of Investigation and the Cybersecurity and Infrastructure Security Agency.[5] However, the private sector has a significant role to play in strengthening cybersecurity. To make this point, Mr. Gensler quoted President Biden's August 2021 remarks on cybersecurity that "most of our critical infrastructure is owned and operated by the private sector, and the federal government can't meet this challenge alone."[6] Mr. Gensler emphasized that the SEC was an important part of "Team Cyber" and has "a key role as the regulator of the capital markets with regard to SEC registrants—ranging from exchanges and brokers to advisers and public issuers" and used his speech to outline potential changes.

Additional Disclosure Obligations for Public Companies

Mr. Gensler suggested new regulations on public companies' disclosure obligations may be forthcoming. Currently, SEC guidelines indicate a public company must disclose certain cybersecurity risks and incidents depending on "the potential materiality of any identified risk and, in the case of incidents, the importance of any compromised information and of the impact of the incident on the company's operations."[7] A public company must also disclose "the most significant factors that make investments in the company's securities speculative or risky," which may include cybersecurity risks and incidents.[8] Although Mr. Gensler recognized that many public companies "already provide cyber risk disclosure to investors," he believes that "companies and investors alike would benefit if this

information were presented in a consistent, comparable, and decision-useful manner."[9] Thus, the SEC may be poised to regulate the ways in which cybersecurity disclosures are made.

While noting the need for new rules, Mr. Gensler also emphasized that the SEC would continue to bring enforcement actions under existing law where companies failed to disclose all material facts related to a cyber incident or risk. He said, "Make no mistake: Public companies already have certain obligations when it comes to cybersecurity disclosures." Mr. Gensler emphasized that "[i]f customer data is stolen, if a company paid ransomware, that may be material to investors" and would need to be disclosed. He added, "As recent cases show, failure to make accurate disclosures of cybersecurity incidents and risks can result in enforcement actions."[10]

Expected Changes to Reg SCI and Reg S-P

Throughout his speech, Mr. Gensler also indicated a desire to extend existing regulations to apply more broadly. As part of this message, he indicated the possible "broadening and deepening" of the Regulation Systems Compliance and Integrity (Reg SCI) rule to apply to market intermediaries, such as broker-dealers and investment advisors.[11] Reg SCI currently applies to financial sector registrants, such as exchanges and clearinghouses, mandating that covered entities "have sound technology programs, business continuity [and disaster recovery] plans, testing protocols, data backups," and specific recordkeeping practices.[12] Mr. Gensler likewise suggested bolstering rules on cybersecurity hygiene and incident reporting. He spoke only generally about the form these rules would take, but he noted that potential reform could "reduce the risk that these registrants couldn't maintain critical operational capability during a significant cybersecurity incident."[13] Mr. Gensler spoke more specifically on financial sector registrants' responsibility towards clients and customers relating to data privacy, suggesting that the SEC may alter the timing and substance of notifications mandated by the Privacy of Consumer Financial Information rule (Regulation S-P), which requires registered broker-dealers, investment companies, and investment advisers protect customer data and provide customers with privacy policy notifications.[14]

New Regulation for Service Providers

Mr. Gensler suggested the SEC will address cybersecurity risk related to service providers. As Mr. Gensler emphasized, service providers "go far beyond the cloud" and "can include 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."[15] Additional regulations in this area could include holding financial sector registrants "accountable for service providers' cybersecurity measures with respect to protecting against inappropriate access and investor information."[16]

As was clear throughout the speech, Mr. Gensler views addressing cybersecurity risk as an important part of the SEC's mission. Thus, while we expect the new regulations that Mr. Gensler emphasized during his speech, we also expect the SEC to continue to bring enforcement actions under existing law.

Jenner & Block will continue to monitor the regulatory landscape surrounding the SEC and cybersecurity.

Contact Us

Charles D. Riely
criely@jenner.com | Download V-Card

Shoba Pillay
spillay@jenner.com | Download V-Card

Gregory M. Boyle
gboyle@jenner.com | Download V-Card

Karolina L. Bartosik
kbartosik@jenner.com | Download V-Card

Meet Our Data Privacy and Cybersecurity Team

Meet Our Investigations, Compliance, and Defense Team

Meet Our Securities Litigation and Enforcement Team

Meet Our Markets and Trading Team

Practice Leaders

David Bitkower
Co-Chair, Data Privacy and Cybersecurity and Investigations, Compliance, and Defense
dbitkower@jenner.com
Download V-Card

Madeleine V. Findley
Co-Chair, Data Privacy and Cybersecurity
mfindley@jenner.com
Download V-Card

Anthony S. Barkow
Co-Chair, Investigations, Compliance, and Defense
abarkow@jenner.com
Download V-Card

Christine Braamskamp
Co-Chair, Investigations, Compliance, and Defense
cbraamskamp@jenner.com
Download V-Card

Brandon D. Fox
Co-Chair, Investigations, Compliance, and Defense
bfox@jenner.com
Download V-Card

Erin R. Schrantz
Co-Chair, Investigations, Compliance, and Defense
eschrantz@jenner.com
Download V-Card

Stephen L. Ascher
Co-Chair, Securities Litigation and Enforcement
sascher@jenner.com
Download V-Card

Howard S. Suskin
Co-Chair, Securities Litigation and Enforcement
hsuskin@jenner.com
Download V-Card

Gregory M. Boyle
Co-Chair, Markets and Trading
gboyle@jenner.com
Download V-Card

Vincent E. Lazar
Co-Chair, Markets and Trading
vlazar@jenner.com
Download V-Card

---

[1] Gary Gensler, Chairman, Sec. & Exch. Comm'n, Remarks at the Securities Enforcement Forum (Nov. 4, 2021) (transcript available at https://www.sec.gov/news/speech/gensler-securities-enforcement-forum-20211104)

[2] *See, e.g., SEC Charges Issuer with Cybersecurity Disclosure Controls Failures*, U.S. Sec. & Exch. Comm'n (June 15, 2021), https://www.sec.gov/news/press-release/2021-102; *SEC Charges Pearson plc for Misleading Investors about Cyber Breach*, U.S. Sec. & Exch. Comm'n (Aug. 16, 2021), https://www.sec.gov/news/press-release/2021-154.

[3] Gary Gensler, Chairman, Sec. & Exch. Comm'n, Speech at the Northwestern Pritzker School of Law Securities Regulation Institute Conference (Jan. 24, 2022) (transcript available at https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124#_ftn17) [hereinafter Gensler, Speech at Securities Regulation Institute Conference].

[4] *Id.*

[5] *Id.*

[6] President Joe Biden, Remarks on Collectively Improving the Nation's Cybersecurity (Aug. 25, 2021) (transcript available at https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/08/25/remarks-by-president-biden-on-collectively-improving-the-nations-cybersecurity/).

[7] 17 C.F.R. § 229, 249 (2018) (available at https://www.sec.gov/rules/interp/2018/33-10459.pdf).

[8] *Id.*

[9] *Id.*

[10] Gensler, Speech at Securities Regulation Institute Conference.

[11] 17 C.F.R. § 240, 242, 249 (2015) (available at https://www.sec.gov/rules/final/2014/34-73639.pdf).

[12] Gensler, Speech at Securities Regulation Institute Conference.

[13] *Id.*

[14] 17 C.F.R. § 248 (2000) (available at https://www.sec.gov/rules/final/34-42974.htm).

[15] Gensler, Speech at Securities Regulation Institute Conference.

[16] *Id.*