

## [Securities Regulation Daily Wrap Up, TOP STORY—Gensler outlines plans to update cyber rules, \(Jan. 24, 2022\)](#)

Securities Regulation Daily Wrap Up

[Click to open document in a browser](#)

By Mark S. Nelson, J.D.

SEC Chair Gensler suggested in a conference keynote speech that public company cyber disclosure rules could be on the agency's radar screen, although a later panel discussion mulled the agency's authorities for some of Gensler's proposals.

SEC Chair Gary Gensler mapped out the agency's plans for freshening and expanding regulations that govern market participants' cybersecurity hygiene and public company cyber disclosures in his Alan B. Levenson Keynote Address to a virtual audience at the 49th Annual Securities Regulation Institute hosted by Northwestern Pritzker School of Law. Gensler also engaged in a short Q&A following his [remarks](#) that emphasized climate change and virtual currencies in addition to cybersecurity. A later panel discussion that included ex-SEC officials discussed at length the prospects for renewed SEC activity on cybersecurity.

**Regulations SCI, S-P, and more.** Gensler offered an expansive view of where the SEC's cybersecurity regulations might go in future rulemakings. Specifically, Gensler's remarks tended to cluster around possible amendments to Regulation Systems Compliance and Integrity (SCI), Regulation S-P, public company cyber disclosures, and accountability for third-party service providers. By way of background, cybersecurity already appears twice on the SEC's Fall 2021 Unified Agenda of Regulatory and Deregulatory Actions, once regarding a [proposal to enhance issuer disclosures](#) regarding cybersecurity risk and related governance, and a second time regarding a [proposal to enhance fund and investment adviser disclosures and governance](#). Also, Gensler noted that the Commission will consider re-proposing rules that would include Treasury trading platforms within Regulation SCI at a January 26, 2022 [open meeting](#) (See [2020 proposal](#)).

With respect to [Regulation SCI](#), Gensler said he wants the SEC to consider "broaden[ing] and deepen[ing]" the current regulation. He noted that Regulation SCI was rolled out in 2014 and that much has happened in the intervening years that merits consideration of a rules refresh. Specifically, Gensler suggested that Regulation SCI could be applied to entities not currently within its ambit, such as large market-makers and broker-dealers.

Regulation SCI superseded the SEC's prior voluntary Automation Review Policy (ARP) and applies to "SCI Entities," including: (i) SCI self-regulatory organizations; (ii) SCI alternative trading systems; (iii) plan processors; and (iv) exempt clearing agencies subject to the ARP.

In the case of funds, advisers, and broker-dealers currently not subject to Regulation SCI, Gensler said that he has asked SEC staff for recommendations on how these actors' cybersecurity hygiene and incident reporting could be improved.

Regulation S-P addresses consumer financial information and the safeguarding of personal information. Here, Gensler suggested a future rules refresh could involve the ways in which customers and clients are notified about cyber events involving their data and the timing and substance of notices required under Regulation S-P.

If amendments to Regulation SCI and Regulation S-P can be considered low-hanging fruit, regulations that would require more specific public company cyber disclosures and that would impose a degree of accountability for cyber risks posed by companies' third-party service providers may present the agency with greater regulatory challenges.

With respect to public company disclosures, Gensler suggested two possible areas for revisions to current rules. First, Gensler said he had asked SEC staff to make a recommendation on public companies' cybersecurity practices and cyber risk disclosures, which he said could include how these companies address

cybersecurity governance, strategy, and risk management. Second, Gensler said he had asked SEC staff for a recommendation on whether and how to update companies' disclosures to investors when cyber events have occurred.

"A lot of issuers already provide cyber risk disclosure to investors," said Gensler. "I think companies and investors alike would benefit if this information were presented in a consistent, comparable, and decision-useful manner."

Although Gensler did not mention it, Congress has proposed legislation, especially on the governance component, that would require public companies to state that they have cybersecurity expertise on their boards or, if they lack such expertise, explain what other steps they have taken by those who evaluate board candidates to address oversight of the company's cybersecurity risks (See the Cybersecurity Disclosure Act ([S. 808](#)), sponsored by Sen. Jack Reed (D-RI), which has also been included as Title VIII of the Corporate Governance Improvement and Investor Protection Act ([H.R. 1187](#)), sponsored by Rep. Juan Vargas (D-Calif), and which narrowly passed the House by a vote of 215-214).

Lastly, Gensler offered a preview of where SEC regulations might go regarding third-party service providers. Service providers have always been considered by cybersecurity experts to be a potential backdoor risk, as exemplified by the recent SolarWinds software breach. For Gensler, however, the SEC may consider requiring that some registrants identify risky service providers. Gensler also floated the possibility of imposing accountability on registrants for service providers' cybersecurity measures as they relate to access and investor information.

**Gensler Q&A session.** While Gensler's formal remarks focused on cybersecurity, a brief post-speech Q&A session moderated by Thomas Kim, Institute Chair and partner at Gibson, Dunn & Crutcher LLP emphasized climate change and virtual currencies without breaking new ground but also the timing of any new cybersecurity rules. On climate change, Gensler said the SEC would issue a rule proposal when it is ready. He also reiterated his prior observations going back to his confirmation hearing and several earlier speeches that he believes investors want to know about how companies consider climate change and that investors could benefit from consistent and comparable public company disclosures.

Gensler also was asked about virtual currencies. He said the SEC has issued lots of guidance on when tokens are securities and reiterated that his immediate predecessor, Jay Clayton, had viewed the agency's approach to virtual currencies in much the same way. Specifically, Gensler said the investment contract approach to dealing with digital assets that may be securities has been written into the law since the 1930s and has been interpreted by the Supreme Court.

As for cybersecurity, Gensler was non-committal on an exact time frame for any rule revisions but he appeared to suggest that Regulation SCI and related issues were under review.

**Ex-SEC officials and cybersecurity.** The first conference panel after Gensler's keynote address consisted of a group of recent ex-SEC officials and was moderated by former SEC Commissioner Robert Jackson Jr., now the Pierrepont Family Professor of Law, Co-Director of the Institute for Corporate Governance and Finance, and Director of the Program of Corporate Law and Policy at New York University School of Law.

Jackson opened the discussion by asking the panel about Gensler's cybersecurity remarks. Former SEC Chair Mary Jo White, under whose tenure Regulation SCI was adopted, said there is nothing more important than cybersecurity. She noted that Gensler had carefully assigned the possible rulemaking topics to buckets and that the public company bucket was among the last he addressed. According to White, the public company space may be a heavier lift if the SEC was to prescribe mandatory disclosure requirements, although White said it was not entirely clear that was the direction Gensler was suggesting the SEC would go.

Stephanie Avakian, former Co-Director of the SEC's Enforcement Division and now a partner at Wilmer Cutler Pickering Hale and Dorr LLP, suggested that Gensler did not lean in on public company cybersecurity disclosures. She also said that the SEC recently has done a lot of messaging on public company cybersecurity disclosures via selected enforcement matters, such as those involving [First American Financial Corporation](#) and

[Pearson plc](#), the former focused on inadequate disclosure controls and procedures, and the latter focused on material misstatements. Avakian noted that before the First American and Pearson matters, there was the SEC's \$35 million settlement with [Altaba Inc./Yahoo! Inc.](#) regarding the two-year delay by Yahoo! in disclosing in its SEC filings the fact that a major cybersecurity breach had already occurred.

William Hinman, Senior Advisor at Simpson Thacher & Bartlett and a former director of the SEC's Division of Corporation Finance, suggested that the SEC's cybersecurity efforts would continue to look at disclosure controls and procedures issues. He also said the SEC may focus on the timing of when cybersecurity breaches are reported. On this latter point, Hinman raised the question of whether such report would be a Form 8-K event.

Hinman's remark about Form 8-K drew a response from moderator Jackson, who in 2018 both [voted](#) for (albeit "reluctantly" because he believed it did not go far enough) the Commission's [interpretive guidance](#) on cybersecurity disclosures and gave a speech in which he presented his own study on how frequently companies disclose cybersecurity breaches via Form 8-K. Said Jackson of the [study results](#) published a few weeks after adoption of the interpretive guidance: "My staff and I compiled evidence on data breaches in 2017 that were reported to state and local regulators, as well as to the press. After removing minor breaches from our dataset, what we found surprised us: of 82 cybersecurity incidents at public companies in 2017, only four companies chose to file an 8-[K] disclosing the breach to their investors. In other words, in 2017, companies that suffered data breaches chose not to file an 8-K more than 97% of the time."

Former SEC Commissioner Troy Paredes, Founder of Paredes Strategies and co-author of Loss, Seligman and Paredes, *Securities Regulation*, a Wolters Kluwer Legal & Regulatory U.S. publication, said generally that disclosure can change what companies do substantively. But more specifically, Paredes remarked that Gensler's suggestion that third-party services providers could fall within the scope of future SEC cybersecurity rules had caught his attention. Paredes said two questions would arise if the Commission were to pursue such rules: (1) what would be the practicality of the rules? and (2) what are the limits of the SEC's authority? Paredes said the second question would likely become a key issue.

MainStory: TopStory BrokerDealers ClearanceSettlement CorporateGovernance CyberPrivacyFeed  
DataSecurity DirectorsOfficers Enforcement ExchangesMarketRegulation FedTracker Securities  
FinancialIntermediaries GCNNews InvestmentAdvisers InvestorEducation PublicCompanyReportingDisclosure  
RiskManagement SECNewsSpeeches