Davis Polk

# SEC proposes expanded cyber oversight after Gensler signals more on the way

February 24, 2022 | Client Update | 4-minute read

**The SEC proposed new cybersecurity rules for investment advisers and investment companies that would require policies and procedures, annual reviews, reporting to the SEC, disclosures to investors, and recordkeeping. The rules would subject investment advisers and investment companies to increased enforcement risk.**

On February 9, 2022, the SEC proposed new rules that would impose significant new cybersecurity requirements for registered investment advisers and investment companies. The proposal has five core requirements:

- **Cybersecurity policies:** Registered investment advisers and investment companies would be required to adopt written cybersecurity policies "reasonably designed to address cybersecurity risks." Such policies would need to include risk assessments, controls to minimize user access risks, monitoring of information systems to prevent unauthorized access or use, threat and vulnerability detection and remediation, and incident response and recovery.
- **Annual reviews:** Advisers and investment companies would be required to review annually the effectiveness of these cybersecurity policies, including whether they reflect changes in cybersecurity risk, and prepare a written report. The report would describe the annual review, including the tests performed, and state whether there had been any incidents or material changes to the policies since the last report.
- **Reporting:** Advisers would be required to report significant cybersecurity incidents affecting the adviser or its clients to the SEC "promptly, but in no event more than 48 hours, after having a reasonable basis to conclude" that a significant cybersecurity incident has occurred or is occurring. Advisers may find it challenging to assess the extent of an incident, or whether one has occurred at all, in this tight timeframe. Reports also would have to be updated within 48 hours of becoming materially inaccurate.
- **Disclosures to investors:** Although reports to the SEC would be confidential,[1] the proposed rules would require advisers and funds to provide a less detailed disclosure in a publicly available section of Form ADV and fund registration statements.
- **Recordkeeping:** The proposed rules would require advisers and funds to maintain records of their cybersecurity policies and records related to the occurrence of any cybersecurity incident.

The proposed rules are written to cover all registered funds, although the SEC asked for comment about whether any funds should be exempt.

The SEC acknowledged that the cost of implementing these new obligations may ultimately be redirected to service providers and clients. The proposed rule would require registrants to include contractual provisions in their agreements with service providers to guarantee adherence to the required measures. In the end, however, the SEC acknowledged that "all of these costs may be passed on—in whole or in part—to clients and investors."

The proposed rules would impose potentially significant new enforcement risk. Advisers currently are subject to Reg S-

P and Reg S-ID, which generally require that they have reasonably designed policies and procedures to protect client information and detect and prevent identity theft. Our recent client update discussed several enforcement cases for violations of Reg S-P. The new rules would expand potential liability for having inadequate policies and procedures, including the multiple required sub-components, and would add new liability relating to annual reports, reporting incidents to the SEC, investor disclosures, and recordkeeping.

**Other cybersecurity rulemaking**

The proposed rules come less than two weeks after the SEC proposed rules to expand Reg ATS to include systems that trade Treasuries and other government securities. An intended consequence would be to bring such platforms with significant volume within the scope of Reg SCI, which imposes technology and security requirements on a limited set of SEC registrants that provide support for market infrastructure, such as stock exchanges, clearinghouses, self-regulatory organizations and similar institutions.

These proposals follow SEC Chair Gary Gensler's January 24 speech, in which he said that the "SEC [is] working to improve the overall cybersecurity posture and resiliency of the financial sector" and highlighted initiatives related to public companies, SEC registrants, and third-party service providers. He directed that SEC staff update guidance regarding public company cybersecurity disclosures that Commission issued in 2018. The SEC recently brought enforcement actions against two issuers, Pearson plc and First American Financial Corporation, for alleged disclosure failures.

Combined, the proposed rules, enforcement actions, expected future guidance, and additional potential rulemaking are significantly increasing the SEC's oversight of registrants' cybersecurity practices and the risk of liability for those firms when they suffer breaches, even though they usually will be in the posture of a victim of a sophisticated attack.

***If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.***


**Greg D. Andres**
+1 212 450 4724
greg.andres@davispolk.com

**Matthew J. Bacal**
+1 212 450 4790
matthew.bacal@davispolk.com

**Martine M. Beamon**
+1 212 450 4262
martine.beamon@davispolk.com

**Micah G. Block**
+1 650 752 2023
micah.block@davispolk.com

**Robert A. Cohen**
+1 202 962 7047
robert.cohen@davispolk.com

**Michael S. Hong**
+1 212 450 4048
michael.hong@davispolk.com

**Sarah E. Kim**
+1 212 450 4408
sarah.e.kim@davispolk.com

**Leor Landa**
+1 212 450 6160
leor.landa@davispolk.com

**Gregory S. Rowland**
+1 212 450 4930
gregory.rowland@davispolk.com


---



[1] The confidentiality of the reporting is one of the items the SEC specifically flagged for comment.