

Newly Proposed SEC Cybersecurity Risk Management Rules and Amendments for Registered Investment Advisers and Funds

March 4, 2022

On February 9, 2022, the U.S. Securities and Exchange Commission (SEC) proposed sweeping [rules](#) that would require registered advisers and funds to implement written policies and procedures designed to address cybersecurity risks, report significant cybersecurity incidents to the SEC using a proposed form, and keep enumerated cybersecurity-related books and records.

Key takeaways from the SEC's release, titled "Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies and Business Development Companies" (the Proposed Rules):

- 1. Cybersecurity Risk Management Rules:** The Proposed Rules would require registered advisers and funds (including SEC-registered business development companies) to implement and maintain policies and procedures to address cybersecurity risks, including risk assessments; controls designed to minimize user-related risks and prevent unauthorized access to information and systems; periodic assessments of information systems and the information stored on such systems; threat and vulnerability management; incident response and recovery; annual review and required written reports; and recordkeeping.
- 2. Reporting of Significant Cybersecurity Incidents:** The Proposed Rules would require registered advisers promptly to report significant cybersecurity incidents under new rule 304-6 by submitting new Form ADV-C. Specifically, advisers would file a report "48 hours after having a reasonable basis to conclude that a significant adviser cybersecurity incident or a significant fund cybersecurity incident occurred or is occurring." The SEC defined a significant cybersecurity incident as one that "significantly disrupts or degrades the adviser's ability, or the ability of a private fund client of the adviser, to maintain critical operations, or leads to the unauthorized access or use of adviser information, where the unauthorized access or use of such information results in: (1) substantial harm to the adviser, or (2) substantial harm to a client, or an investor in a private fund, whose information was accessed."
- 3. Disclosure of Cybersecurity Risks and Incidents:** The SEC's amendments would require registered advisers and funds to disclose cybersecurity matters in Form ADV Part 2A for advisers and Forms N-1A, N-2, N-3, N-4, N-6, N-8B-2, and S-6 for funds.

4. **Fund Boards:** Registered fund boards would have specific duties under the Proposed Rule for funds. Following a required initial approval of a fund's cybersecurity policies and procedures, fund directors over time would review reports on cyberincidents and material changes to policies and procedures. Echoing language used in other SEC releases, the SEC adds that "Board oversight should not be a passive activity."

The SEC established a public comment period as the later of April 11, 2022 (60 days after the SEC issued its release), or 30 days after the *Federal Register* publishes the Proposed Release. The SEC's proposing release seeks comment on more than 60 detailed issues.

Commissioner Hester Peirce [published a statement](#) dissenting to the Proposed Rules. Commissioner Peirce said that she disagrees with framing the Proposed Rules for advisers as antifraud under the Advisers Act, stating that the fraudulent and deceptive acts covered in the Proposing Rules are "not ones in which the adviser is the perpetrator, but the victim." To further make her point, Commissioner Peirce recited language from the Proposed Rule that would make it "unlawful for any investment adviser registered or required to be registered ... to provide investment advice to clients unless the adviser adopts and implements written policies and procedures that are reasonably designed to address the adviser's cybersecurity risks" She then observed that if the rule is read literally, should an adviser not follow these rules, any investment advice it provides to clients is illegal — what she described as an "extreme" penalty with "no apparent logical connection." Commissioner Peirce also discussed the current cybersecurity protections in place, such as Regulation S-P and Regulation S-ID, and recommended that the SEC issue guidance as opposed to a rule.

Other initial reactions to the Proposed Rules have been mixed. Some observers question the need for the rules; some ask whether they are too specific and risk becoming dated; and many are concerned that the proposed real-time and after-the-fact reporting of cybersecurity incidents will have unintended consequences including distraction of time and resources from actual response at that critical moment and even signaling of vulnerabilities to bad actors.

These Proposed Rules may not be the only upcoming SEC cybersecurity regulation. During a [speech on January 24, 2022](#), Chair Gary Gensler signaled that there may be forthcoming guidance related to public companies' cybersecurity programs and risk disclosures. For information related to current best practices related to cybersecurity, see [Sidley's recent blog post](#) on the topic or contact a member of the Sidley team.

CONTACTS

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

Colleen Theresa Brown , Partner	+1 202 736 8465, ctbrown@sidley.com
Jay G. Baris , Senior Counsel	+1 212 839 8600, jbaris@sidley.com
Nathan J. Greene , Partner	+1 212 839 8673, ngreene@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