Published on *The National Law Review* https://natlawreview.com

SEC Proposes Cybersecurity Regulations for Advisers and Funds

Article By:

Joseph C. Weinstein

Sean L. McGrane

Kristin L. Bryan

Following recent comments by the Chair of the Securities and Exchange Commission (SEC) on cybersecurity policy, this week a divided SEC proposed new rules related to cybersecurity for registered investment advisers ("advisers"), investment companies and business development companies ("funds"). Citing the growing threat of malicious cyber actors, the SEC's proposal emphasizes that cybersecurity incidents may cause harm to clients of advisers and funds, as well as to the operation and reputation of the financial markets generally. With respect to the need for new regulations, the SEC observes that certain advisers and funds still lack robust cybersecurity practices and that current regulations—such as the Advisers Act compliance rule and Regulation S-ID—only indirectly address cybersecurity for advisers and funds. The SEC's proposal includes four areas of new rules specific to cybersecurity:

1. **Adoption of Written Cybersecurity Policies and Procedures**

The first set of proposed rules (206(4)-9 and 38a-2) would require advisers and funds to adopt and implement written policies and procedures "reasonably designed to address cybersecurity risks." The rules enumerate general elements that written policies and procedures would be required to address—including cybersecurity risk assessments, user access controls, sensitivity levels of firm information, and cybersecurity incident detection—but the rules would allow advisers and funds to tailor their cybersecurity policies and procedures based on their circumstances and sophistication. The proposed rule would require that the written cybersecurity policies and procedures be approved initially by the adviser or fund's board of directors. In addition, advisers and funds would be required to 1) annually review the effectiveness of their policies and procedures and 2) provide a written report to their board of directors describing the review and any cybersecurity incidents and assessments since the previous report.

2. **Confidential Reporting by Advisers of Cybersecurity Incidents to the SEC**

The proposal includes a new rule (204-6) requiring advisers to file a report with the SEC when a "significant cybersecurity incident" occurs at the adviser or clients of the adviser. As to what constitutes a "significant" incident, the proposed rule defines "significant adviser cybersecurity incident" to include cybersecurity incidents that result in substantial harm to the adviser or to the adviser's client whose information was accessed. As for timing, the adviser would be required to file the report "promptly, but in no event more than 48 hours, after having a reasonable basis to conclude" that a cybersecurity incident has occurred or is occurring. The adviser would also be required to amend previous reports within 48 hours after obtaining new material information or if a previous report becomes materially inaccurate.

3. Public Disclosure of Cybersecurity Incidents and Risks

The SEC also proposes amendments to certain forms for advisers (ADV Part 2A) and funds (N-1A, N-2, N-3, N-4, N-6, N-8B-2, and S-6) that are given to current or prospective clients. For advisers, the amended "brochure" form would require firms to include both a description of cybersecurity incidents over the past two fiscal years and a description of how the adviser addresses material cybersecurity risks. In addition, advisers would be required (under proposed rule 204-3(b)(4)) to "promptly" provide interim brochure amendments or supplements to existing clients if the adviser makes a material revision about a cybersecurity incident. Similarly, funds would be required to disclose in their registrations statements "any significant fund cybersecurity incident that has occurred in its last two fiscal years" in a certain machine-readable format.

4. Recordkeeping Obligations

Lastly, the proposed rules (204-2(a)(17)(i), (iv)–(vii) and 38a-2(e)) would require funds and advisers to maintain certain records related to the above cybersecurity rules. Among other things, funds and advisers would need to maintain, for at least five years, 1) their written cybersecurity policies and procedures, 2) reports provided to the board of directors about the review of cybersecurity policies and procedures, 3) records relating to the occurrence of any cybersecurity incident.

The proposed rules are open to public comment and may be revised before an eventual SEC vote for final approval. In the meantime, we expect the SEC to continue to push cybersecurity policy. In his statement accompanying the proposal, SEC Chair Gary Gensler reiterated that he has asked the SEC to make cybersecurity-related recommendations with respect to broker-dealers, Regulation SCI, Regulation S-P, and third-party service providers. And a day prior to the proposal, a bipartisan group of U.S. Senators urged the SEC in a letter to propose cybersecurity disclosure requirements for public companies and financial sector registrants. In other words, there may be much more to come.

James Brennan also contributed to this article.

National Law Review, Volume XII, Number 42

funds