

## SEC Announces Proposed Cybersecurity Rules for Advisers and Funds

February 22, 2022 Kit Addleman, Tim Newman, Carrington Giammittorio

**PRACTICES** Investment Management, Fund Formation and Management, Privacy and Cybersecurity

On February 9, the Securities and Exchange Commission [announced](#) proposed new rules related to cybersecurity risk management for registered investment advisers, registered investment companies, and funds.<sup>1</sup> In addition to enhancing the requirements for cybersecurity risk and incident disclosures, the proposed rules would introduce three new obligations for advisers and funds:

- Adoption and implementation of written policies and procedures that are reasonably designed to address cybersecurity risks;
- Reporting of significant cybersecurity incidents to the Commission on a new, proposed Form ADV-C; and
- Maintenance and retention of certain cybersecurity-related books and records.

**First**, proposed new rules 206(4)-9 under the Advisers Act and 38a-2 under the Investment Company Act would require all advisers and funds—regardless of type or size—to “implement cybersecurity hygiene and protection measures.” The proposed rules for advisers and funds would require rule 206(4)-9 policies and procedures be tailored to the business and to include the following mandatory elements: (i) periodic assessment and prioritization of risks, (ii) user security and access controls, (iii) periodic assessment and monitoring of information systems, (iv) detection and mitigation of cybersecurity threats and vulnerabilities, and (v) measures to detect, respond to, and recover from cybersecurity incidents.

Many of these mandatory elements correspond to the best practices for managing cybersecurity risk that the Commission’s Office of Compliance Inspections and Examinations (“OCIE”) published in January of 2020.<sup>2</sup> They also seem designed to reinforce and remedy the most common exam deficiencies identified by OCIE in connection with the Safeguards Rule, which requires registrants to adopt written policies and procedures reasonably designed to ensure the protection of customer information.<sup>3</sup> Under new proposed rules 206(4)-9 and 38a-2, advisers and funds would have to review their cybersecurity policies and procedures at least annually.

**Second**, proposed new rule 204-6 under the Advisers Act would introduce a new Form ADV-C. Advisers who experience a cybersecurity incident would be required to confidentially report the incident to the Commission using the proposed Form ADV-C within 48 hours of “having a reasonable basis to conclude” that a qualifying cybersecurity incident had occurred. Advisers would be required to report not only on behalf of itself, but also on behalf of any client that is a registered investment company, business development company, or private fund.

Under proposed rule 204-6, the Commission would define a “significant” cybersecurity incident as “a cybersecurity incident, or a group of related incidents, 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.” In simple terms, an incident would need to be reported if it leads to significant disruption to critical operations or unauthorized access or use of information that results in substantial harm to either the adviser or client.

Advisers would also have an ongoing obligation to timely supplement any Form ADV-C when new information about a previously reported incident is discovered. In order to facilitate timely compliance with these reporting requirements, the Commission notes in the proposing release that the new rule 206(4)-9 “must address the proposed notification requirement to the Commission on Form ADV-C.”

***Third***, the proposed rulemaking would amend the applicable books and records rules<sup>4</sup> to require advisers and funds to maintain the following records related to cybersecurity risk management and incidents: (i) a copy of their cybersecurity policies and procedures (formulated pursuant to proposed rule 206(4)-9) in effect at any time within the last five years; (2) a copy of written reports documenting the annual review of its cybersecurity policies and procedures; (3) a copy of any Form ADV-C filed in the last five years or, in the case of funds, a copy of any Form ADV-C filed by its adviser; (4) records documenting the occurrence of any cybersecurity incident in the last five years; and (5) records documenting the adviser or fund’s cybersecurity risk assessment. The proposed amendment would require advisers and funds to maintain these records for five years.

***Finally***, the Commission’s proposal would amend Form ADV Part 2A to require disclosure of material cybersecurity risks and incidents to an adviser’s clients and prospective clients. Funds would also be required to disclose this information on their registration forms. These amendments would more closely align advisers’ and funds’ public disclosure obligations with that of public companies.

The public comment period runs 60 days following the publication of the proposed rules on the SEC’s website or 30 days following the publication of the proposed rules in the Federal Register, whichever is longer. Following the comment period, the Commission will vote on a final rule.

For more information on the Commission’s proposed cybersecurity rulemaking or the Commission’s ongoing focus on cybersecurity matters, please contact one of the following Haynes Boone lawyers.

---

<sup>1</sup> <https://www.sec.gov/rules/proposed/2022/33-11028.pdf>

<sup>2</sup> [OCIE Cybersecurity and Resiliency Observations](#) (Jan. 27, 2020)

<sup>3</sup> [Investment Adviser and Broker-Dealer Compliance Issues Related to Regulation S-P—Privacy Notices and Safeguard Policies](#) (Apr. 16, 2019)

<sup>4</sup> Rule 204-2 under the Advisers Act and rule 38a-2 under the Investment Company Act.