

Cybersecurity Risk Management



The Securities and Exchange Commission proposed new cybersecurity risk management rules and amendments to enhance cybersecurity preparedness and improve the resilience of investment advisers and investment companies against cybersecurity threats and attacks.

Specifically, the proposal would:

- Require advisers and funds to adopt and implement written policies and procedures that are reasonably designed to address cybersecurity risks;
- Require advisers to report significant cybersecurity incidents to the Commission on proposed Form ADV-C;
- Enhance adviser and fund disclosures related to cybersecurity risks and incidents; and
- Require advisers and funds to maintain, make, and retain certain cybersecurity-related books and records.

Background

Advisers and funds play an important role in our financial markets and increasingly depend on technology for critical business operations. Advisers and funds are exposed to and rely on a broad array of interconnected systems and networks, both directly and through service providers such as custodians, brokers, dealers, pricing services, and other technology vendors. As a result, they face numerous cybersecurity risks and may experience cybersecurity incidents that can cause or be exacerbated by critical system or process failures.

The proposed rules and amendments are designed to address concerns about advisers' and funds' cybersecurity preparedness and reduce cybersecurity-related risks to clients and investors; improve adviser and fund disclosures about their cybersecurity risks and incidents; and enhance the Commission's ability to assess systemic risks and oversee advisers and funds.

Proposed Amendments

Cybersecurity Risk Management Rules

The proposal includes new rule 206(4)-9 under the Advisers Act and new rule 38a-2 under the Investment Company Act (collectively, the "proposed cybersecurity risk management rules"). The proposed cybersecurity risk management rules would require advisers and funds to adopt and implement policies and procedures that are reasonably designed to address cybersecurity risks. The proposed rules list certain general elements that advisers

and funds would be required to address in their cybersecurity policies and procedures to help address operational and other risks that could harm advisory clients and fund investors or lead to the unauthorized access to or use of adviser or fund information, including the personal information of their clients or investors.

Reporting of Significant Cybersecurity Incidents

The proposal includes a reporting requirement under new rule 204-6 that would require advisers to report significant cybersecurity incidents to the Commission, including on behalf of a fund or private fund client, by submitting a new Form ADV-C. These confidential reports would bolster the efficiency and effectiveness of the Commission's efforts to protect investors by helping the Commission monitor and evaluate the effects of a cybersecurity incident on an adviser and its clients, as well as assess the potential systemic risks affecting financial markets more broadly.

Disclosure of Cybersecurity Risks and Incidents

Currently, advisers provide disclosures to their prospective and current clients on Form ADV's narrative brochure, or Part 2A, which is publicly available and one of the primary client-facing disclosure documents used by advisers. Form ADV Part 2A contains information about the investment adviser's business practices, fees, risks, conflicts of interest, and disciplinary information. The proposal would amend Form ADV Part 2A to require disclosure of cybersecurity risks and incidents to an adviser's clients and prospective clients.

Like advisers, funds also would be required to provide prospective and current investors with cybersecurity-related disclosures. Specifically, the proposed amendments would require a description of any significant fund cybersecurity incidents that have occurred in the last two fiscal years in funds' registration statements, tagged in a structured data language. The proposal includes amendments to Form N-1A, Form N-2, Form N-3, Form N-4, Form N-6, Form N-8B-2, and Form S-6.

Recordkeeping

Rule 204-2, the books and records rule under the Advisers Act, sets forth requirements for maintaining, making, and retaining books and records relating to an adviser's investment advisory business. The proposal would amend this rule to require advisers to maintain certain records related to the proposed cybersecurity risk management rules and the occurrence of cybersecurity incidents.

Similarly, proposed rule 38a-2 under the Investment Company Act would require that a fund maintain copies of its cybersecurity policies and procedures and other related records specified under the proposed rule.

Additional Information:

The public comment period will remain open for 60 days following publication of the proposing release on the SEC's website or 30 days following publication of the proposing release in the Federal Register, whichever period is longer.