STRADLEY RONON

March 10, 2022

Client Alert | Investment Management

SEC Proposes New Rule for Fund and Adviser Cybersecurity Risk Management

On Feb. 9, 2022, the Securities and Exchange Commission (the SEC) proposed new cybersecurity and cyber reporting rules and amendments for investment advisers and investment companies.[1] According to the SEC, the proposed rules and amendments are intended to enhance cybersecurity preparedness and improve the resilience of investment advisers and investment companies against cybersecurity threats and attacks.

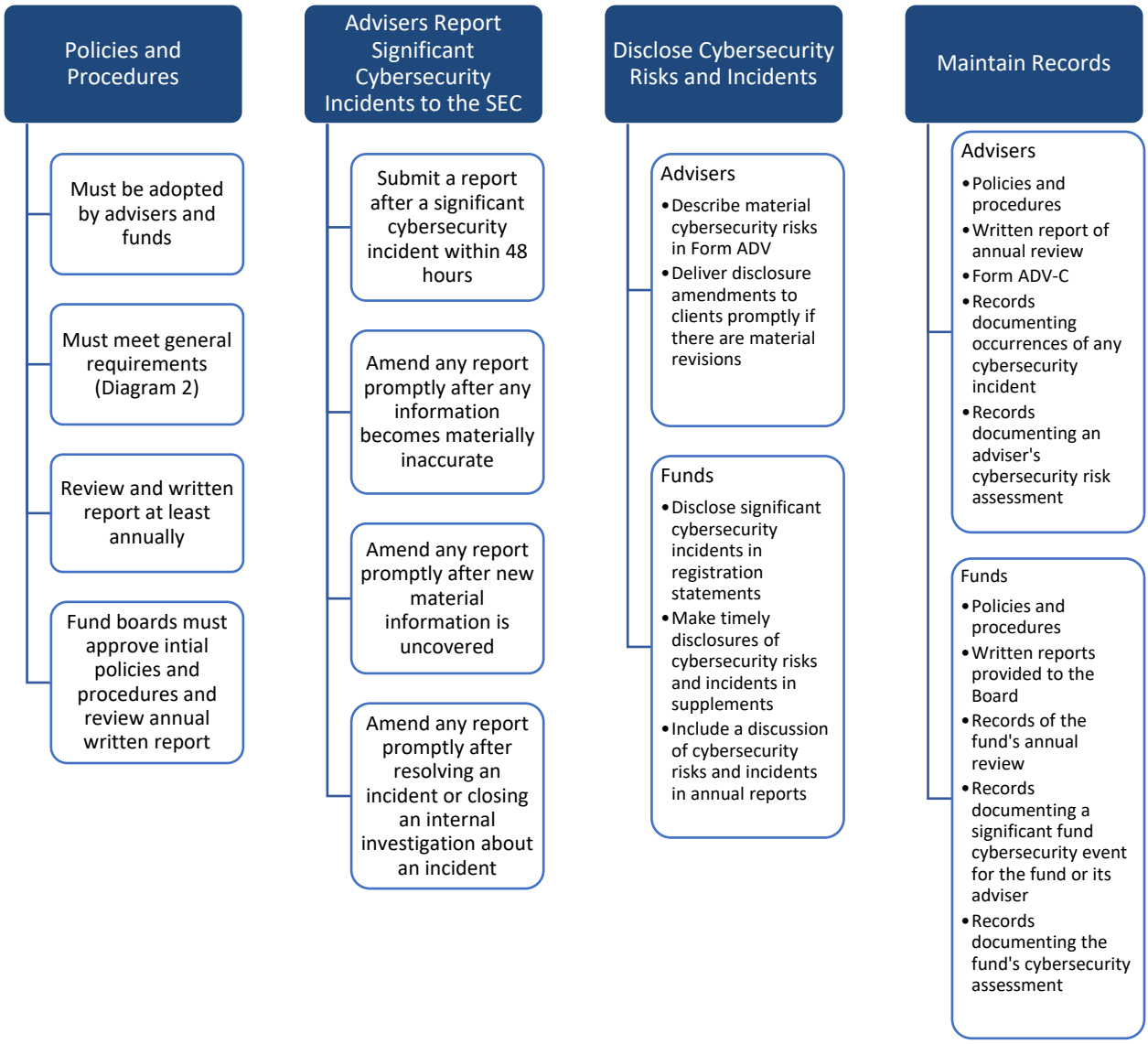
This Alert summarizes the Proposal and addresses some key observations and issues to consider throughout.

I. The Proposal

The SEC proposed new rules and amendments in four main areas: (1) cybersecurity risk management policies and procedures; (2) reporting of significant adviser and fund cybersecurity incidents; (3) disclosure of cybersecurity risks and incidents by funds and advisers to potential and existing investors; and (4) recordkeeping requirements. These proposed requirements are summarized in Diagram 1 and in the Sections below.

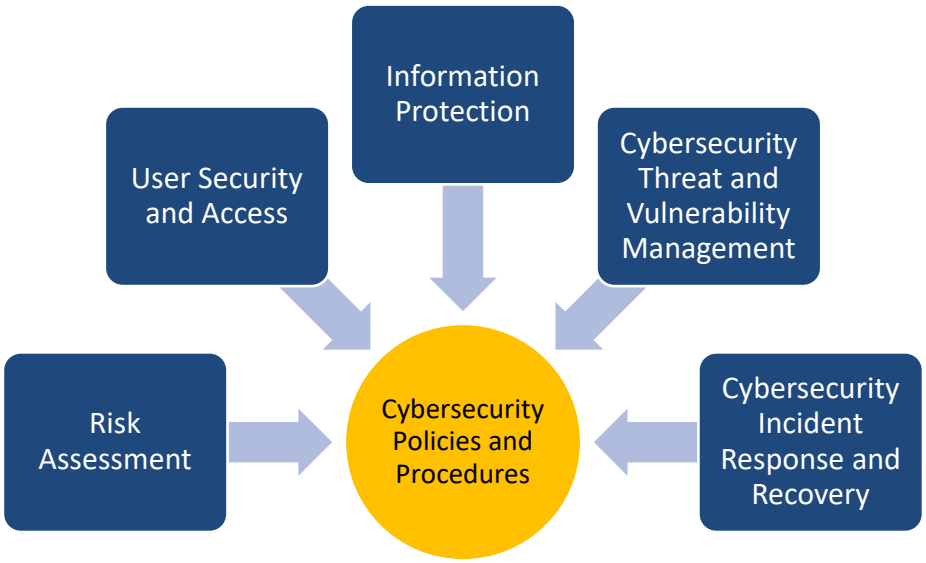
[1] Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, Release Nos. 33-11028; 34-94197; IA-5956; IC-34497 (Feb. 9, 2022) (the Proposal).

Diagram 1: SEC Proposed Cybersecurity Risk Management Requirements



A. Cybersecurity Risk Management Policies and Procedures. The proposed rules require certain general elements to be addressed in advisers' and funds' cybersecurity policies and procedures.[2] The five required elements are highlighted in Diagram 2. The SEC intends to permit firms some flexibility to tailor their policies and procedures based on the particular cybersecurity risk posed by each adviser's or fund's operations and business practices. Additionally, the Proposal would provide flexibility for the adviser and fund to determine in-house or external service providers to implement and oversee the effectiveness of the cybersecurity policies and procedures.

Diagram 2: Required Elements of Adviser and Fund Cybersecurity Policies and Procedures



i. Required Elements. The general requirements for these policies and procedures are discussed below.

1. Risk Assessment. The proposed rules would require periodic assessments, no less than annually, of cybersecurity risks, including (a) categorizing and prioritizing risks based on an inventory of the components of the adviser or fund information ("information") systems and information residing therein and (b) identifying service providers that receive, maintain or process information or are otherwise permitted access to information systems or any information residing therein. The proposed rules would also require written documentation of any risk assessments.

2. User Security and Access. The proposed rules would require controls designed to minimize user-related risks and prevent unauthorized access to information, including (a) requiring standards of behavior for individuals authorized access to information, (b) identifying and authenticating individual users with authentication measures that require users to present a combination of two or more credentials, (c) establishing procedures for timely distribution, replacement, and revocation of passwords and authentication methods, (d) restricting access to specific information systems solely to individuals requiring access to the systems and information as a

[2] These requirements are found in proposed new rule 38a-2 under the Investment Company Act and rule 206(4)-9 under the Investment Advisers Act.

necessity for performing their responsibilities and functions with the adviser or fund and (e) securing remote access technologies.

3. **Information Protection.** The proposed rules would require measures designed to monitor information systems and protect information from unauthorized access, based on a periodic assessment that takes into account (a) the sensitivity level and importance of information to business operations, (b) whether any information is personal information, (c) where and how information is accessed, stored and transmitted, (d) information systems access controls and malware protection and (e) the potential effect a cybersecurity incident involving information could have on the adviser or fund and its shareholders, including the ability to continue to provide services. The proposed rules would also require oversight of the service providers that receive, maintain or process information pursuant to a written contract between the adviser or fund and service providers that requires the service providers to implement and maintain appropriate cybersecurity risk management measures (i.e., a vendor management program).

4. **Threat and Vulnerability of Management.** The proposed rules would require measures to detect, mitigate and remediate any cybersecurity threats and vulnerabilities with respect to information systems and the information residing therein. Advisers and funds would generally be required to perform ongoing monitoring through measures such as comprehensive examinations and risk management processes.

5. **Cybersecurity Incident Response and Recovery.** The proposed rules would require measures to detect, respond to and recover from a cybersecurity incident,[3] including policies and procedures reasonably designed to ensure (a) continued operations of the adviser or fund, (b) the protection of information systems and the information residing therein, (c) external and internal cybersecurity incident information sharing and communications and (d) reporting of significant cybersecurity incidents. An incident response plan would also designate adviser or fund personnel to perform specific roles in the case of a cybersecurity incident. The proposed rules would also require written documentation of any cybersecurity incident, including the adviser's or fund's response to and recovery from such an incident.

[3] A "cybersecurity incident" is defined as an unauthorized occurrence on or conducted through an adviser's or fund's information systems that jeopardizes the confidentiality, integrity, or availability of an adviser's or fund's information systems or any information residing therein. Therefore, it seems that not all potential incidents would fall under this rule (e.g., not every phishing attempt would be a cybersecurity incident under the Proposal).

ii. **Annual Review and Required Written Reports.** The proposed rules would require advisers and funds to, at least annually, (1) review and assess the design and effectiveness of the cybersecurity policies and procedures, including whether they reflect changes in cybersecurity risk over the time period covered by the review and (2) prepare a written report that describes the annual review, assessment and any control tests performed, explain the results thereof, document any cybersecurity incident that occurred since the date of the last report, and discuss any material changes to the policies and procedures since the date of the last report. The written report would be prepared or overseen by the persons who administer the adviser's or fund's cybersecurity policies and procedures and should consider any risk assessments performed by the adviser or fund.

iii. **Fund Board Oversight.** Proposed rule 38a-2 would require a fund's board of directors, including a majority of its independent directors, to initially approve the fund's cybersecurity policies and procedures and review the written report on cybersecurity incidents and material changes to the fund's cybersecurity policies and procedures described above. Boards would also be required to consider what level of oversight of the fund's service providers is appropriate with respect to cybersecurity based on the fund's operations.

Key Observation

The Proposal imposes a number of specific obligations on fund boards, including approval of cybersecurity policies and procedures and review of an annual assessment of the cybersecurity program. In addition, the Proposal includes guidance suggesting that a board should review contracts and risk assessments of certain service providers with respect to cybersecurity. Despite these new obligations, we believe that fund directors should not be required to become cybersecurity experts and instead should continue to be able to serve in an oversight role, relying on others for assistance on these issues.

iv. **Recordkeeping.** The proposed rules generally would require that advisers and funds maintain copies of cybersecurity related records, including records documenting the occurrences of any cybersecurity incidents.

B. Reporting to SEC of Significant Cybersecurity Incidents. The Proposal includes a requirement that advisers would be required to report significant cybersecurity incidents to the SEC, including on behalf of a client that is a registered investment company, business development company or a private fund.[4] Proposed rule 204-6 and the related proposed Form ADV-C are described below.

i. Proposed Rule 204-6. Under proposed rule 204-6, any adviser registered or required to be registered with the SEC would be required to submit proposed Form ADV-C promptly, but in no event more than 48 hours, after having a reasonable basis to conclude that a significant adviser cybersecurity incident or a significant fund cybersecurity incident had occurred or is occurring. The SEC defines these incidents broadly (see callout box with definition below). Proposed rule 204-6 would also require advisers to amend any previously filed Form ADV-C promptly, but in no event more than 48 hours, after (a) information reported on the Form becomes materially inaccurate, (b) new material information about a previously reported incident is uncovered, and (c) resolving a previously reported incident or closing an internal investigation pertaining to a previously disclosed incident.

Definition of "Significant Cybersecurity Incident"

The Proposal defines a "significant adviser cybersecurity incident" and "significant fund cybersecurity incident" as a cybersecurity incident, or a group of related incidents, that significantly disrupts or degrades the ability of an adviser, a fund or a private fund, to maintain critical operations or leads to the unauthorized access or use of adviser or fund information, where the unauthorized access or use of such information results in:

- Substantial harm to the adviser or fund or
- Substantial harm to a client, or an investor in a fund or private fund, whose information was accessed.

[4] The Proposal in this regard is in some ways similar to cyber reporting requirements imposed by other federal regulators. For example, the Transportation Security Administration (the TSA) issued a security directive in May 2021 requiring pipeline owners or operators to report cybersecurity incidents within 12 hours and another in December 2021 that requires freight railroad owners or operators to report cybersecurity incidents within 24 hours. *See* TSA, Enhancing Pipeline Cybersecurity (May 28, 2021); TSA, Enhancing Rail Cybersecurity (Dec. 31, 2021).

ii. **Form ADV-C.** Proposed Form ADV-C would include both general and specific questions related to a significant cybersecurity incident, such as the nature and scope of the incident as well as whether any disclosure has been made to any clients and/or investors. The SEC does not intend to make Form ADV-C filings public.

Considerations for Form ADV-C
The proposed Form ADV-C would represent a significant change for the asset management industry. If adopted as proposed, to effectively plan for a future significant cybersecurity incident, industry participants would need to consider (among other things) the elements listed in Table 1 in their incident response planning:

Table 1: Form ADV-C Response Planning Considerations
▪ Designate those responsible for filing Form ADV-C and plan for access to the Investment Adviser Registration Depository (the IARD) in the event of a catastrophic event barring access to the firm's current systems.
▪ Identify those responsible for contact with the SEC.
▪ Identify third party resources which can be brought in quickly to provide relevant expertise.
▪ Address the 48-hour timeline for filing Form ADV-C and how the firm will supplement that filing as it learns additional information, including in situations where an investigation may be ongoing.
▪ The requirement to notify the SEC may also cause the adviser to reevaluate whether and how it engages with other law enforcement entities and government agencies.
▪ Develop guidance on whether and how to notify clients in the event of a significant cybersecurity incident.
▪ For fund advisers, developing an appropriate communication protocol with the fund Board in connection with the 48-hour time period.

C. **Disclosure of Cybersecurity Risks and Incidents.** The Proposal also includes amendments to 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 to address cybersecurity risks and incidents more directly. The specific amendments are detailed below.

i. **Proposed Amendments to Form ADV.** The proposed amendments to Form ADV Part 2A would include a new Item 20 entitled "Cybersecurity Risks and Incidents" that requires an adviser to describe in plain English the cybersecurity risks that could materially affect the advisory services that it offers; describe how it assesses, prioritizes, and addresses cybersecurity risks; and disclose any significant cybersecurity incidents that occurred within the last two years. In addition, the Proposal includes an amendment to rule 204-3(b) that would require an adviser to deliver interim brochure amendments to existing clients promptly if the adviser adds disclosure of a cybersecurity incident to its brochure or materially revises information already disclosed in the brochure about such an incident.

ii. **Proposed Amendments to Fund Disclosures**. The Proposal would require funds to provide prospective and current investors with disclosure about significant fund cybersecurity incidents that occurred in its last two fiscal years in their registration forms. The information required would include (a) the entity or entities affected, (b) when the incident was discovered and whether it is ongoing, (c) whether any data was stolen, altered, or accessed or used for any other unauthorized purpose, (d) the effect of the incident on the fund's operations and (e) whether the fund or service provider has remediated or is currently remediating the incident.

Funds would also be asked to consider cybersecurity when preparing risk disclosures in fund registration statements, such as whether cybersecurity is a principal risk of investing in the fund and should be reflected in the fund's prospectus. The SEC proposes specific guidance on making disclosure updates in fund supplements to make timely disclosure of cybersecurity risks and incidents.

In addition, funds would be asked to include in their annual reports to shareholders a discussion of cybersecurity risks and significant cybersecurity incidents, to the extent that these were factors that materially affected performance of the fund over the previous fiscal year.

Key Observation

The disclosure and SEC reporting requirements raise a number of potential concerns. For example, as described above, reporting to the SEC within 48 hours of a significant incident would create significant challenges for advisers. In addition, disclosure and reporting would be required for certain matters that do not result in investor harm. Furthermore, public disclosure may provide a roadmap to bad actors. If it adopts these rules, the SEC should adjust these requirements to reflect what we expect to be a variety of constructive and practical public comments in this regard.

II. Conclusion

Public comments on the Proposal are due 30 days after publication in the Federal Register, or April 11, 2022, whichever is later. It is likely that the industry will focus on a number of key issues in the Proposal during the comment period, including the key observations made above. Additionally, Commissioner Hester M. Pierce raised a number of important concerns in her dissenting statement.[5] The industry should carefully consider her statement in developing comments on the Proposal.

Finally, the SEC should recognize in any adopted rule that it must be flexible enough to fit different business models, adapt to changing cybersecurity threats, and appropriately recognize the burdens and resource demands that it will place on industry participants, in particular smaller firms.

Key Observation

The SEC has recently been aggressive on the enforcement front with respect to cybersecurity issues, using rules and authority that it already has. If adopted, these rules will provide additional tools to continue this trend, including with potential inadequate disclosure and policies and procedures cases.

For more information, contact:

David W. Grim
Partner
202.507.5164
dgrim@stradley.com

Peter Bogdasarian
Partner
202.419.8405
pbogdasarian@stradley.com

Jessica Patrick
Associate
202.419.8423
jpatrick@stradley.com

Geena Marzouca
Associate
202.507.6408
gmarzouca@stradley.com

[5] Hester M. Peirce, Commissioner, SEC, Statement on Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies (Feb. 9, 2022).