SULLIVAN & CROMWELL LLP

S&C memo

February 18, 2022

# SEC Proposes New Cybersecurity Risk Management Rules for Investment Advisers and Investment Companies

## Proposed Rules and Amendments Are Aimed at Enhancing Cybersecurity Preparedness and Improving Resilience Against Cybersecurity Risks

### SUMMARY

On February 9, 2022, the Securities and Exchange Commission (the "SEC") voted 3 to 1 (Commissioner Peirce dissenting[1]) to propose cybersecurity risk management rules and amendments for registered investment advisers, registered investment companies and business development companies (the "proposal").[2] The proposed rules and amendments are designed to reduce cybersecurity risks to clients and investors and enhance the SEC's ability to oversee advisers and funds. As proposed, the rules would require SEC-registered advisers and funds to adopt and implement written policies and procedures reasonably designed to address cybersecurity risks and registered advisers to confidentially report significant cybersecurity incidents to the SEC through a new Form ADV-C. In addition, the proposed rules would improve SEC-registered adviser and fund disclosures related to cybersecurity risks and incidents.

The SEC is seeking comment from the public on the proposal. Consistent with Chair Gensler's approach on several other recent rulemaking initiatives, the comment deadline is accelerated, with comments due on April 11, 2022 or 30 days after the proposal is published in the Federal Register, whichever is later.

### BACKGROUND

The SEC states in the Release that advisers and funds "increasingly depend on technology for critical business operations."[3] At the same time, "cyber threat actors have grown more sophisticated," putting advisers and funds at a significant risk of suffering financial, operational, legal and reputational harm.[4] The

SEC has expressed concern that some advisers and funds have not implemented reasonably designed cybersecurity programs to address these increasingly complex and damaging threats. Accordingly, the proposal is designed to "promote a more comprehensive framework to address cybersecurity risks for advisers and funds," thereby reducing the risk that advisers and funds would not be able to maintain critical operations when confronted with a significant cybersecurity incident, to give clients and investors superior information and to give the SEC greater ability to conduct more comprehensive oversight of cybersecurity risks and incidents.[5]

## OVERVIEW OF THE CYBERSECURITY PROPOSAL

### Cybersecurity Risk Management Rules

Proposed new rules 206(4)-9 under the Investment Advisers Act and 38a-2 under the Investment Company Act would require registered investment advisers and registered investment companies and business development companies (collectively, "funds") to adopt and implement policies and procedures that are reasonably designed to address cybersecurity risks. Specifically, the proposal would require advisers and funds to address the following general elements in their policies and procedures:[6]

- **Risk Assessment**, including assessing, categorizing, prioritizing, and drafting written documentation of the cybersecurity risks associated with their information systems and the information residing therein;
- **User Security and Access**, including implementing controls designed to minimize user-related risks and prevent unauthorized access to information and systems;
- **Information Protection** involving monitoring information systems and protecting information from unauthorized access or use;
- **Threat and Vulnerability Management** to detect, mitigate and remediate cybersecurity threats and vulnerabilities; and
- **Cybersecurity Incident Response and Recovery** to detect, respond to and recover from cybersecurity incidents.

In the Release, the SEC emphasizes that cybersecurity programs should have clear incident response plans to ensure continued operational capability, data protection and critical system recovery during cybersecurity incidents.[7] To these ends, the SEC suggests maintaining physical copies of incident response plans and backing up data as ways to promote prompt system recovery and mitigate the consequences of cybersecurity incidents. Incident response plans should designate adviser or fund personnel with requisite cybersecurity expertise to perform specific roles during an incident, including coordinating with outside experts as needed and keeping the appropriate individuals informed. Incident response plans should also include a clear escalation protocol to ensure that these individuals, such as senior officers and legal compliance personnel, receive necessary information on a timely basis.[8] In addition, under the proposed rules and amendments, advisers and funds would have to report significant cybersecurity incidents to the SEC, as well as their clients and investors, as discussed further below.

### Annual Review and Required Written Report

In addition, the proposal would require an adviser or fund to review and assess the design and effectiveness of its cybersecurity policies and procedures, including whether they reflect changes in cybersecurity risk over the time period covered by the review. The adviser or fund must then prepare a written report describing its review and assessment at least annually, including any control tests performed, explain the results thereof, document any cybersecurity incidents that occurred since the last report and discuss any material changes to its cybersecurity policies and procedures. The report should be prepared or overseen by the persons who administer the adviser's or fund's cybersecurity program.[9]

### Role and Obligations of Fund Boards

Proposed rule 38a-2 would require a fund's board of directors, including a majority of the independent directors, to approve the fund's initial cybersecurity policies and procedures, and to review the written report described above. The SEC believes the proposed rules would "facilitate the board's oversight of the fund's cybersecurity program and provide accountability for the administration of the program," and "would be consistent with a board's duty to oversee other aspects of the management and operations of a fund."[10] The SEC notes that board oversight "should not be a passive activity" and "the requirements for the board to initially approve the fund's cybersecurity policies and procedures and thereafter to review the required written reports are designed to assist directors in understanding a fund's cybersecurity risk management policies and procedures, as well as the risks they are designed to address."[11] In addition, the SEC notes that fund directors, especially independent directors, may satisfy their duties with respect to the initial approval by reviewing summaries of the cybersecurity program that include the salient features of the program and provide directors with an understanding of the program's operation and administration. The proposal states that when considering whether to approve the procedures and policies, the directors of a fund may wish to consider the fund's exposure to cybersecurity risks, including those of its service providers, and any recent threats or incidents to which the fund may have been subject. Fund directors are expected to ask questions and seek relevant information regarding the effectiveness of the fund's cybersecurity program and its implementation, and whether the fund has adequate resources with respect to cybersecurity matters, including access to cybersecurity expertise. The SEC envisions that this fund director review of the written reports would involve specific inquiries about cybersecurity risks arising from the program and any incidents that have occurred. Boards should also consider their level of oversight of the fund's service providers in relation to cybersecurity risks.[12]

### Reporting of Significant Cybersecurity Incidents to the Commission

The proposal would require advisers to report "significant adviser cybersecurity incidents" and "significant fund cybersecurity incidents" to the SEC on proposed Form ADV-C promptly, and in any case within 48 hours, after having a reasonable basis to believe such an incident has occurred or is occurring.[13] A "significant adviser cybersecurity incident" would be defined as "a cybersecurity incident, or a group of

related cybersecurity 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."[14] Similarly, a "significant fund cybersecurity incident" would be defined as "a cybersecurity incident, or a group of related cybersecurity incidents, that significantly disrupts or degrades the fund's ability to maintain critical operations, or leads to the unauthorized access or use of fund information, where the unauthorized access or use of such information results in substantial harm to the fund or to an investor whose information was accessed."[15]

Accordingly, in addition to requiring an adviser to report significant cybersecurity incidents for itself and its private fund clients, an adviser would also have to report significant fund cybersecurity incidents for its registered fund and business development company clients.[16] In order to assist the adviser in reporting a significant fund cybersecurity incident, a fund's cybersecurity policies and procedures would also be required to address these proposed notification requirements on Form ADV-C, which generally should address communications between the administrator of the fund's cybersecurity policies and the advisers about cybersecurity incidents.

Advisers would also be required to promptly amend Form ADV-C, and in no event more than 48 hours after (1) any previously reported information has become materially inaccurate, (2) discovering new material information pertaining to a previously reported incident or (3) resolving a previously reported incident or closing any internal investigation pertaining to such an incident.[17]

Form ADV-C, which advisers would file electronically through the Investment Adviser Registration Depository platform, contains both general and specific questions related to the significant cybersecurity incident, such as the details about the nature and scope of the incident, whether law enforcement or any government agency other than the SEC has been notified and whether the incident is covered under a cybersecurity insurance policy. The SEC believes that collecting information about significant cybersecurity incidents in the structured format of Form ADV-C would enhance its ability to carry out its risk-based examination program, assess trends in cybersecurity incidents across the industry and better protect investors from any patterned cybersecurity threats.

### Disclosure of Cybersecurity Risks and Incidents

The proposed amendments would require the disclosure of cybersecurity risks and incidents to investors and other market participants by modifying 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. Specifically, the proposed amendments would require the adviser to describe cybersecurity risks that could materially affect the advisory services offered, and how the adviser assesses, prioritizes, and addresses cybersecurity risks created by the nature and scope of its business.

In addition, advisers would be required to provide a description of any cybersecurity incident that has occurred within the last two fiscal years that has significantly disrupted or degraded its ability to maintain critical operations, or has led to the unauthorized access or use of adviser information, resulting in substantial harm to the adviser or its clients. Funds would be required to include a description of any significant fund cybersecurity incidents that have occurred in the last two fiscal years in the funds' registration statements, tagged in a structured data language. The SEC notes that these changes would also give the SEC greater insight into cybersecurity risks that affect advisers and funds, enhancing oversight for compliance with the policies and procedures that would be required under the other proposed cybersecurity management rules.[18]

### Recordkeeping

The SEC's proposed rules would also propose new recordkeeping requirements. Advisers would be required to maintain: (1) a copy of their cybersecurity policies and procedures that are in effect or were in effect at any time within the past five years, (2) a copy of the adviser's written report documenting annual review of its cybersecurity policies and procedures for the last five years, (3) a copy of any Form ADV-C filed in the last five years, (4) records documenting the occurrence of any cybersecurity incident in the last five years, and (5) records documenting an adviser's cybersecurity risk assessment in the last five years.[19]

Similarly, a fund would be required to maintain: (1) a copy of its cybersecurity policies and procedures that are in effect, or at any time within the last five years were in effect; (2) copies of written reports provided to its board; (3) records documenting the fund's annual review of its cybersecurity policies and procedures; (4) any report of a significant fund cybersecurity incident provided to the SEC by its adviser; (5) records documenting the occurrence of any cybersecurity incident, including any records related to any response and recovery from such an incident; and (6) records documenting the fund's cybersecurity risk assessment.[20]

## IMPLICATIONS

Although many advisers and funds consider cybersecurity risks in developing their compliance policies and procedures required under the Investment Advisers Act and Investment Company Act, the proposal represents the first time that advisers and funds would expressly be obligated to adopt cybersecurity-related policies and procedures. The proposal affirms Chair Gensler's commitment to looking at ways the SEC can play a more robust role in addressing cybersecurity risks.[21] We believe the following elements of the proposal are particularly noteworthy:

- **Benchmarking Cybersecurity Best Practices.** The general elements advisers and funds would be required to address under the proposed rules, namely (1) risk assessment, (2) user security and access, (3) information protection, (4) threat and vulnerability management and (5) cybersecurity incident response and recovery, can be read as benchmarking best practices. This aligns with

other regulatory guidance in the cybersecurity space, such as the New York State Department of Financial Services' minimum access elements.[22]

- **Guidance for Fund Boards.** The Release explicitly discusses directors' roles in addressing cybersecurity risks for the funds they oversee. The proposed rules would require board involvement in cybersecurity risk management and the Release discusses particular ways directors can discharge their duties to oversee the fund's cybersecurity risk management program. The guidance provided in the Release regarding the active role fund boards are required to play in the oversight of cybersecurity risk management will be familiar, following the general framework of the guidance provided to fund boards in other recent SEC rulemakings, including Use of Derivatives by Registered Investment Companies and Business Development Companies and Good Faith Determinations of Fair Value.[23]

* * *

## ENDNOTES

1 Commissioner Peirce commented that for those advisers and funds that have not already implemented cybersecurity programs under the existing regulatory framework, "guidance might be more helpful than a rule." Commissioner Hester M. Peirce, Statement on Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies (Feb. 9, 2022), *available at* https://www.sec.gov/news/statement/peirce-statement-cybersecurity-risk-management-020922.

2 Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, SEC Release Nos. 33-11028; 34-94197; IA-5956; IC-34497 (Feb. 9, 2022) (the "Release"). *See also*, SEC Fact Sheet: Cybersecurity Risk Management (Feb. 9, 2022), *available at* https://www.sec.gov/files/33-11028-fact-sheet.pdf.

3 Release at 6.

4 *Id*. at 6-7.

5 *Id*. at 14-15.

6 The SEC notes that given the number and varying characteristics of advisers and funds, firms may need to tailor their cybersecurity policies based on their individual facts and circumstances. Therefore, the proposed rules give advisers and funds flexibility to address the outlined general elements relative to the individual cybersecurity risks of each firm. *Id.* at 17.

7 *Id*. at 33.

8 *Id*. at 34.

9 *Id*. at 39.

10 *Id.* at 41.

11 *Id.* at 41.

12 *Id*. at 42.

13 A "cybersecurity incident" would be defined as "an unauthorized occurrence on or conducted through [an adviser's or a fund's] information systems that jeopardizes the confidentiality, integrity, or availability of [an adviser's or a fund's] information systems or any [adviser or fund] information residing therein." *Id.* at 216, 236.

14 *Id.* at 231–32.

15 *Id.* at 217.

16 The SEC requests comments on how it should address funds that are internally managed. *Id.* at 52.

17 *Id.* at 231.

18 *Id.* at 60.

19 *Id.* at 229–30.

20 *Id.* at 215–16. Records would have to be maintained for at least five years after the provision of the report, the first two years in an easily accessible place.

21 Chair Gensler has commented that "cyber risks have implications for the financial sector, investors, issuers and the economy at large" and that "the SEC has a role to play," along with other government agencies and the private sector. Chair Gary Gensler, Speech on Cybersecurity and Securities Laws, Northwestern Pritzker School of Law's Annual Securities Regulation Institute (Jan.

## ENDNOTES (CONTINUED)

24, 2022), *available at* https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124.

[22] "DFS must have access, at a minimum, to documentation including the affiliate's cybersecurity policies and procedures, risk assessments, penetration testing and vulnerability assessment results, and any third party audits that relate to the adopted portions of the cybersecurity program of the affiliate." Adoption of an Affiliate's Cybersecurity Program, New York State Department of Financial Services Industry Guidance Letter (Oct. 22, 2021), *available at* https://www.dfs.ny.gov/industry_guidance/industry_letters/il20211022_affiliates_cybersecurity_program.

[23] *See, e.g.*, SEC Adopts New Derivatives Framework for Registered Investment Companies and Business Development Companies, Sullivan & Cromwell Memo (December 23, 2020), *available at* https://www.sullcrom.com/files/upload/sc-publication-sec-adopts-new-derivatives-framework-for-registered-investment-companies-business-development-companies.pdf, and SEC Adopts New Rule to Modernize Fund Valuation Framework, Sullivan & Cromwell Memo (December 14, 2020), *available at* https://www.sullcrom.com/files/upload/sc-publication-sec-adopts-new-rule-modernize-fund-valuation-framework.pdf.

## ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

## CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers, or to any Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.