WILLKIE FARR & GALLAGHER LLP

CLIENT ALERT

SEC Proposes Cybersecurity Rules and Amendments for Registered Investment Advisers, Registered Investment Companies and BDCs

February 18, 2022

AUTHORS

James E. Anderson | James R. Burns | Elizabeth P. Gray | Neesa Patel Sood
Richard M. Borden | Richard F. Jackson | Nicholas Chanin | John F. Rupp

On February 9, 2022, the Securities and Exchange Commission (the "SEC" or the "Commission") voted 3-1 to propose rules related to cybersecurity risk management for registered investment advisers ("investment advisers"), and registered investment companies and business development companies ("funds"), as well as amendments to certain rules that govern adviser and fund disclosures (the "Proposal").[1] The Proposal is the latest in a series of actions taken by the SEC and its staff focusing on cybersecurity risk management, most recently including two Risk Alerts issued in 2020 by the Division of Examinations (formerly known as the Office of Compliance Inspections and Examinations or OCIE)[2] and a

[1] *See* Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, Securities Exchange Act of 1934 (the "Exchange Act") Release No. 94197 (Feb. 9, 2022), available here (the "Proposing Release").

[2] *See* Cybersecurity: Safeguarding Accounts against Credential Compromise, OCIE Risk Alert (Sept. 15, 2020), available here; Cybersecurity: Ransomware Alert, OCIE Risk Alert (July 10, 2020), available here.

series of SEC enforcement actions, which resulted in a total of $750,000 in civil money penalties for failure to secure personal investor information.[3]

At the Commission's open meeting in connection with the Proposal, SEC Chair Gary Gensler commented that "[t]he proposed rules and amendments are designed to enhance cybersecurity preparedness and could improve investor confidence in the resiliency of advisers and funds against cybersecurity threats and attacks." The Proposal would require: (i) investment advisers and funds to adopt and implement written policies and procedures that are reasonably designed to address cybersecurity risks; (ii) investment advisers to report significant cybersecurity incidents, including those affecting clients that are funds, to the SEC on proposed Form ADV-C; and (iii) investment advisers and funds to provide clients and investors with disclosure related to cybersecurity risks and incidents. As discussed below, however, the Proposal provides only vague guidance to affected firms as to how they should go about implementing its complicated provisions while seeming to disregard well-established cybersecurity standards and frameworks.

Current Regulatory Framework

The SEC generally has viewed investment advisers' obligations relating to cybersecurity through the lens of an adviser's fiduciary duty to clients, which derives in part from Section 206 of the Investment Advisers Act of 1940 (the "Advisers Act"). Thus, investment advisers, as fiduciaries, are required to act in the best interest of their clients at all times.[4] Investment advisers owe their clients a duty of care and a duty of loyalty.

In addition to these general principles, the SEC has adopted a number of rules that are used indirectly to address cybersecurity concerns associated with investment advisers and funds. For example, Rule 206(4)-7 under the Advisers Act requires investment advisers to adopt and implement written policies and procedures reasonably designed to prevent violations of the Advisers Act. Since cybersecurity incidents could create significant operational disruptions and losses to clients and investors, investment advisers often consider the cybersecurity risks created by their particular circumstances when developing their compliance policies and procedures.

Similarly, Rule 38a-1 under the Investment Company Act of 1940 (the "Investment Company Act") requires funds to adopt and implement written policies and procedures reasonably designed to prevent violations of the Federal securities laws by

[3] *See* In the Matter of Cetera Advisor Networks LLC, Exchange Act Release No. 92800 (Aug. 30, 2021), available here; In the Matter of Cambridge Investment Research, Inc., Exchange Act Release No. 92806 (Aug. 30, 2021), available here; In the Matter of KMS Financial Services, Inc., Exchange Act Release No. 92807 (Aug. 30, 2021), available here.

[4] *See SEC v. Capital Gains Research Bureau, Inc.,* 375 U.S. 180, 194 (163); *see also* Commission Interpretation Regarding Standard of Conduct for Investment Advisers, Advisers Act Release No. 5248 (June 5, 2019), available here.

the fund. Funds often take into account any specific cybersecurity risks they face when developing their compliance policies and procedures required by Rule 38a-1 under the Investment Company Act.

Regulation S-P, adopted in 2000 and amended in 2004, addresses cybersecurity concerns relating to personal financial information of certain advisory clients and fund investors by requiring investment advisers and funds to, among other things, adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information.[5] These policies and procedures must be reasonably designed to protect the security and confidentiality of customer records and information against (i) any anticipated threats or hazards, and (ii) unauthorized access to, or use of, customer records or information that could result in a substantial harm or inconvenience to any customer.

In addition, Regulation S-ID requires certain investment advisers and funds to develop and implement a written identity theft program.[6] A Regulation S-ID program must, among other things, include reasonable policies and procedures to identify and detect relevant red flags, as well as respond appropriately to red flags so as to prevent and mitigate identify theft.

Implications of the Proposal

Separate from the specifics of the Proposal, broader potential implications of the Proposal if it were to be adopted as proposed are significant. The Proposal generally takes a step in the right direction to improve cybersecurity for investment advisers and funds. However, despite vague references to existing cybersecurity standards and frameworks,[7] the Proposal appears to depart from both current financial services cybersecurity regulation and from existing standards and frameworks. Many investment advisers and funds have already adopted such standards, which are prevalent in the cybersecurity industry.[8] It is puzzling that the SEC does not even reference the Financial Services Sector Coordinating Council ("FSSCC") Cybersecurity Profile—a cybersecurity framework that references SEC, Federal Reserve Board, Commodity Futures Trading Commission and international regulations and guidance (the "FSSCC Framework"). The FSSCC Framework maps the regulatory requirements and guidance to widely used standards. The FSSCC Framework was developed over the course of two years by a consortium of financial services stakeholders that included the SEC.[9]

---

5 *See* 17 C.F.R. 248.30(a); Disposal of Consumer Report Information, Exchange Act Release No. 50781 (Dec. 2, 2004), available here; Privacy of Consumer Financial Information ("Regulation S-P"), Exchange Act Release No. 42974 (Nov. 13, 2000), available here.

6 *See* 17 C.F.R. 248.201; Identity Theft Red Flags Rules, Exchange Act Release No. 34-69359 (May 20, 2013), available here.

7 *See, e.g.*, Proposing Release at n.24 (noting that funds and advisers "may" wish to consult such resources).

8 Examples of widely used cybersecurity standards include the ISO/IEC 27000:2018 Family of Standards ("ISO 27000"); the National Institute of Standards and Technology ("NIST") Special Publication 800-53 Rev. 5 ("NIST 800-53"); and COBIT 2019 from ISACA.

9 The current FSSCC Framework is available here.

Prior SEC regulations have relied on industry standards and frameworks. Regulation Systems Compliance and Integrity ("Regulation SCI"), adopted by the SEC in 2014, directly refers regulated firms, such as certain exchanges, clearing agencies and others ("SCI entities") to industry standards. Rule 1001(a)(1) requires SCI entities to establish, maintain, and enforce certain written policies and procedures. Sub-paragraph (4) of Rule 1001(a) provides that "such policies and procedures shall be deemed to be reasonably designed if they are consistent with current SCI industry standards, which shall be comprised of information technology practices that are widely available to information technology professionals in the financial sector and issued by an authoritative body that is a U.S. governmental entity or agency, association of U.S. governmental entities or agencies, or widely recognized organization." The SEC also released detailed staff guidance as to how SCI entities could make use of such industry standards in developing the required policies and procedures.[10] The guidance identifies the publications the SEC staff believes are appropriate reference documents for various domains (*e.g.,* information security and networking).

The SEC's approach also is at odds with the approach taken by the Federal Reserve Board through the Federal Financial Institutions Examination Council (the "FFIEC"). The Federal Reserve Board utilizes a detailed audit Handbook[11] that is aligned with NIST 800-53. Additionally, many advisers and funds are already complying with cybersecurity regulations promulgated by other federal and state regulators (*e.g.*, the New York Department of Financial Services Cybersecurity Regulations).

By failing to reference existing standards and frameworks, and not providing detailed audit guidance, the Proposal introduces uncertainty as to whether the existing and widely accepted cybersecurity standards would satisfy the Proposal, or how the Proposal will interact with competing compliance obligations. Investment advisers and funds that make good faith efforts to comply will not know whether those efforts will actually result in compliance with the proposed rules. This uncertainty increases the cost of compliance and—absent clear and detailed guidelines from the SEC—introduces the risk of inadvertent non-compliance and does not necessarily improve cybersecurity. Moreover, by proposing the Advisers Act cybersecurity risk management rule as an antifraud rule under Section 206 of the Advisers Act, the Proposal unfairly magnifies potential negative consequences to an investment adviser for failing to navigate this uncertainty successfully.

For the Proposal to be truly effective, the SEC should either publish thoughtful, comprehensive, and clear compliance and audit guidance or adopt the standards and framework already widely accepted in the cybersecurity industry. If the SEC intends to increase requirements or depart from existing standards, that intention should be stated much more clearly. The absence of constructive guidance by the SEC and the failure to adhere to the FSSCC Framework could leave the Proposal vulnerable to challenge under Section 706(2)(A) of the Administrative Procedure Act as being arbitrary.

[10] *See* Staff Guidance on Current SCI Industry Standards (Nov. 19, 2014), available here.

[11] The Handbook consists of several individual IT booklets published by the FFIEC and are available here.

The Proposed Rules and Amendments

Cybersecurity Risk Management Policies and Procedures

The Commission proposes to adopt Rule 206(4)-9 under the Advisers Act and Rule 38a-2 under the Investment Company Act (collectively, the "proposed cybersecurity risk management rules"), requiring investment advisers and funds, respectively, to adopt and implement written policies and procedures addressing certain required elements. In addition, the cybersecurity policies and procedures would be subject to review at least annually that is documented in a written report. Further, proposed Rule 38a-2 would require a fund's board of directors, including a majority of its independent directors, initially to approve the fund's cybersecurity policies and procedures, as well as to review the annual report on and material changes to the fund's cybersecurity policies and procedures. Apart from the board oversight reflected in proposed Rule 38a-2, the two proposed cybersecurity risk management rules are generally identical.

Required Elements of Investment Advisers' and Funds' Policies and Procedures

The proposed cybersecurity risk management rules enumerate five general elements that must be addressed: (i) cybersecurity risk assessment, (ii) user security and unauthorized access, (iii) information protection, (iv) cybersecurity threat and vulnerability management, and (v) cybersecurity incident response and recovery.

Cybersecurity Risk Assessment. The proposed cybersecurity risk management rules would require advisers and funds periodically to assess, categorize, prioritize, and draft written documentation of, the cybersecurity risks[12] associated with their information systems[13] and the information residing therein. The proposed cybersecurity risk management rules would require advisers and funds, when conducting this risk assessment, to:

- Categorize and prioritize cybersecurity risks based on an inventory of the components of their information systems, the information residing therein, and the potential effect of a cybersecurity incident on the advisers and funds;[14] and

[12] The Commission proposes to define "Cybersecurity risk" as the "financial, operational, legal, reputational, and other adverse consequences that could stem from cybersecurity incidents, threats, and vulnerabilities." Note, the defined terms for the proposed cybersecurity risk management rules are contained in, respectively, proposed Rule 206(4)-9(b) and Rule 38a-2(f).

[13] The Commission proposes to define "Adviser information system" as "information resources owned or used by the adviser, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of adviser information to maintain or support the adviser's operations." The Proposing Release indicates that such proposed defined terms for advisers and funds will be the same in most instances (*e.g.,* "fund information system").

[14] The Commission proposes to define "cybersecurity incident" 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 system residing therein."

- Identify the service providers that receive, maintain or process adviser or fund information, or that are permitted to access their information systems and the information residing therein, and assess the cybersecurity risks associated with the use of these service providers.

The proposed cybersecurity risk management rules would require written documentation of any such risk assessment. The risk assessment should generally inform senior officers of the cybersecurity risks specific to the firm and support responses to such risks by identifying threats to information systems that, if compromised, could result in significant cybersecurity incidents. Cybersecurity programs should be reasonably designed to ensure their operational capability, including resiliency and capacity of information systems, when confronted with a cybersecurity incident.

The Proposal here introduces highly complex concepts, such as risk prioritization based on a comprehensive systems assessment, without any real guidance from the SEC as to the expectation on how this should be achieved. The vast majority of current cybersecurity assessments are conducted by cybersecurity professionals trained to assess using ISO 27000, NIST 800-53, or the SANS Institute Top 25.[15] Such assessments are designed to assist information security and information technology organizations to better protect themselves, not for compliance in the manner that the Proposal contemplates. For large investment advisers and funds, this will be a highly complex requirement. For smaller investment advisers and funds, the resources necessary to design and deliver a risk assessment meeting these criteria, both internal and external, may not be available for a reasonable cost, if at all. It should be noted that NIST has published an entire Special Publication devoted to risk assessments,[16] including the testing of the effectiveness of controls, which is discussed in the *Annual Review and Required Written Reports* section below.

User Security and Unauthorized Access. The proposed cybersecurity risk management rules would require controls designed to minimize user-related risks and prevent the unauthorized access to information and systems, including:

- Requiring standards of behavior for individuals authorized to access information systems and relevant information residing therein, such as an acceptable use policy;

- Identifying and authenticating users, including implementing authentication measures that require users to present a combination of two or more credentials for access verification;

- Establishing procedures for the timely distribution, replacement, and revocation of passwords or methods of authentication;

[15] *See* SANS Institute Top 25, available here.

[16] *See* NIST Special Publication 800-53A, Rev. 5, Assessing Security and Privacy Controls in Information Systems and Organizations, available here.

- Restricting access to specific information systems or components thereof and information residing therein solely to individuals requiring access to such systems and information as is necessary for them to perform their responsibilities and functions on behalf of the investment adviser or fund; and

- Securing remote access technologies used to interface with information systems.

The Proposing Release suggests that, given the increase in remote access and telework, requiring such measures is a necessary component of robust and comprehensive cybersecurity policies and procedures.[17]

Information Protection. The proposed cybersecurity risk management rules would require investment advisers and funds to monitor information systems and protect information from unauthorized access or use, based on a periodic assessment of their information systems and the information that resides on the systems. The proposed rules require consideration of:

- The sensitivity level and importance of the information to the adviser's or the fund's business operations;

- Whether the information includes personal information (*i.e.*, information that can be used to identify an individual or other non-public information about a client's account);

- Where and how the information is accessed, stored and transmitted, including the monitoring of the information in transmission;

- Information systems access controls and malware protection; and

- The potential effect of a cybersecurity incident involving adviser or fund information on the entity and its clients or investors, including the ability for the entity to continue providing services.

This provision, again, has the SEC introducing complex requirements—sophisticated network monitoring and data loss prevention—without detailed guidance. For example, the SEC does not make clear whether it would require endpoint detection and response, or if firms should deploy managed detection and response. Similarly, the SEC does not indicate whether deployment of data loss prevention systems is required, and if required, whether certain actions by users must be blocked, or if detection and reporting would be acceptable. Stating that it should be based on the risk assessment leaves firms that desire to comply with no clarity on whether the choices they make will be considered acceptable, with the risk of being accused of an antifraud violation if they fail to choose the SEC's as yet unannounced preferred course.

The proposed rules also provide that the administrators of an investment adviser's or a fund's cybersecurity policies and procedures, whether they are in-house or a third party, must be empowered to make decisions and escalate issues to

[17] *See* Proposing Release at 25–26.

senior officers as necessary.[18] This element also requires the oversight of service providers that receive, maintain, or process adviser or fund information, or are otherwise permitted to access the information systems and information residing therein. Investment advisers and funds would be required to document that such service providers, pursuant to a written contract, are required to implement and maintain appropriate measures, including the practices described above, that are designed to protect adviser and fund information systems and information residing therein. There are many ways to manage third-party risk. Contractual provisions provide one path, but may not be easily obtained or enforced. Certain aspects of the proposed cybersecurity risk management rules may drive investment advisers and funds away from third parties that enable more effective protections than on-premise adviser and fund operations, but who are not willing to accept certain contractual risks or regulatory obligations. If the SEC is too proscriptive in this area, it may in fact unintentionally increase cybersecurity risk in the financial services markets.

Cybersecurity Threat and Vulnerability Management. The proposed cybersecurity risk management rules would require investment advisers and funds to detect, mitigate, and remediate cybersecurity threats and vulnerabilities with respect to their information systems. In general, once a threat or vulnerability is identified, investment advisers and funds should consider how to mitigate and remediate the threat or vulnerability, with a view towards minimizing the window of opportunity for attackers to exploit vulnerable hardware and software.

Cybersecurity Incident Response and Recovery. The proposed cybersecurity risk management rules would require advisers and funds to have measures to detect, respond to, and recover from a cybersecurity incident, including policies and procedures that are reasonably designed to ensure:

- Continued operations;
- The protection of the information systems and the information residing therein;
- External and internal cybersecurity incident information-sharing and communications; and
- Reporting of significant cybersecurity incidents to the Commission.

In addition, the proposed cybersecurity risk management rules would require written documentation of any cybersecurity incident, including the investment adviser's or the fund's response to and recovery from such an incident.

Given the prevalence of ransomware, this aspect of the Proposal, and the lack of guidance, is of significant concern. Disaster recovery is significantly more technically complicated than the risk assessment. Even organizations with the most sophisticated disaster recovery programs struggle with this. It is of the utmost importance that the proposed rules provide clarity as to the SEC's expectations, especially as the rules would apply to entities ranging from some of the

[18] *Id.*at 19.

largest in the world to much smaller organizations, often without the levels of sophistication that may (or may not) be required. Leaving this to the risk assessment, and determining what is considered reasonable after a cybersecurity incident, is not only unfair to the regulated entities, but also will not achieve the SEC's goals. Further, the Proposal seems to emphasize the use of redundant services or service providers to reduce the risk of operational disruption from a cybersecurity incident. While redundant services may indeed reduce the risk of operational disruption, such redundancy is both expensive and complicated to implement (perhaps prohibitively so for smaller firms), and in fact may increase the risk of information compromise by spreading firms' information through additional systems, exposing that information to additional attack vectors.

Annual Review and Required Written Reports

The proposed cybersecurity risk management rules would require investment advisers and funds to review their cybersecurity policies and procedures no less than annually. Such annual reviews would require investment advisers and funds to:

- 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;[19] and
- Prepare a written report describing the annual review, which would have to, at a minimum:
    - Describe the annual review, assessment, and any control tests performed;
    - Explain the results of the control tests;
    - Document any cybersecurity incident that occurred since the last annual report; and
    - Discuss any material changes to the cybersecurity policies and procedures since the last annual report.

The Proposing Release notes that the annual review requirement is designed to require investment advisers and funds to evaluate whether their policies and procedures continue to work as designed and whether changes are needed to assure their continued effectiveness.[20]

[19] As noted previously, there are existing standards and detailed regulatory guidance relating to cybersecurity and privacy risk assessment. If such standards are not used, new audit regimes will need to be developed.

[20] *See* Proposing Release at 39.

Fund Board Oversight

Proposed Rule 38a-2 would require a fund's board of directors, including a majority of its independent directors, initially to approve the fund's cybersecurity policies and procedures as well as to review the annual written report on and material changes to cybersecurity policies and procedures detailed above. The Proposing Release notes that board oversight should not be a passive role, and the requirements proposed here 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.[21] This aspect of the Proposal appears to change the role of the fund's board from oversight of management to stepping into the shoes of management. The concept that the SEC further proposed of direct oversight by the board of cybersecurity issues connected with vendor contracts takes this even further.[22]

Reporting of Significant Cybersecurity Incidents to the Commission

The Proposal includes new reporting requirements for investment advisers. Proposed Rule 204-6 under the Advisers Act would require investment advisers to file a report with the SEC on proposed Form ADV-C within 48 hours after having a reasonable basis to conclude that a significant adviser cybersecurity incident or a significant fund cybersecurity incident has occurred or is occurring.[23] Form ADV-C also would need to be amended if any previously reported information about a significant cybersecurity incident becomes materially inaccurate or if the adviser discovers new material information related to an incident. The proposed reporting rule would also require investment advisers to file a final Form ADV-C amendment after the resolution of any significant cybersecurity incident or after closing any internal investigation related to a previously disclosed incident. The form would be filed electronically through the Investment Adviser Registration Depository system.

By requiring these reports to be prepared and filed with the SEC within 48 hours, the Proposal does not appear to consider the fact that the personnel best positioned to prepare and file the reports are the very people who would be working to identify and respond to such incidents. The SEC should consider whether, on balance, it is necessary to impose such a strict reporting requirement on investment advisers and their personnel that could potentially force them to take time away from dealing with an incident before it becomes a crisis.

---

[21] *Id.* at 41.

[22] *Id.* at 42–43.

[23] Proposed Rule 204-6(b) would define a "significant adviser 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." This proposed definition is substantially the same for a "significant fund cybersecurity incident" for funds.

Proposed Form ADV-C would provide information regarding a significant cybersecurity incident in a structured format through a series of check-the-box and fill-in-the-blank questions. Proposed Form ADV-C would elicit the following information:

- Whether the investment adviser is reporting a significant adviser cybersecurity incident or a significant fund cybersecurity incident (or both);
- The approximate date of the incident's occurrence and discovery;
- Whether the incident is ongoing;
- Whether law enforcement or a government agency has been notified;
- Any actions and planned actions to recover from the incident;
- Whether any data was stolen, altered, or accessed, or used for any unauthorized purpose;
- Whether the incident has been disclosed to clients or investors; and
- Whether the incident is covered under a cybersecurity insurance policy.

Disclosure of Cybersecurity Risks and Incidents

The Proposal includes amendments to registration forms used by investment advisers and funds to require the disclosure of cybersecurity risks and incidents to their investors and other market participants. For investment advisers, the Proposal would amend Form ADV Part 2A by adding new Item 20, which would require investment advisers to describe, in plain English, cybersecurity risks that could materially affect the advisory services they offer and how they assess, prioritize, and address cybersecurity risks created by the nature and scope of their business. The SEC stated in the Proposing Release that a cybersecurity risk, regardless of whether it has led to a significant cybersecurity incident, would be material to an adviser's advisory relationship with its clients if there were a substantial likelihood that a reasonable client would consider the information important based on the total mix of facts and information.[24] Proposed Item 20 would also require investment advisers to describe any cybersecurity incidents that occurred within the last two fiscal years that have significantly disrupted or degraded the adviser's ability to maintain critical operations, or that have led to the unauthorized access or use of adviser information, resulting in substantial harm to the adviser or clients.

[24] Proposing Release at 61.

The Proposal would amend rule 204-3(b) under the Advisers Act to require an investment 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 its brochure.

For funds, the Proposal would amend Form N-1A, Form N-2, Form N-3, Form N-4, Form N-6, Form N-8B-2, and Form S-6 to require funds to provide prospective and current investors with disclosure about any significant cybersecurity incidents that have occurred in the last two fiscal years. The proposed amendments would require funds to tag the new information using a structured data language (Inline eXtensible Business Reporting Language, or Inline XBRL). A fund would be required to describe each significant cybersecurity incident, including the following information to the extent known:

- The entity or entities affected;
- When the incident was discovered and whether it is ongoing;
- Whether any data was stolen, altered, or accessed or used for any other unauthorized purpose;
- The effect of the incident on the fund's operations; and
- Whether the fund or service provider has remediated or is currently remediating the incident.

Funds would be required to update their prospectuses upon the occurrence of a significant cybersecurity event by filing a supplement with the SEC. The SEC also stated in the Proposing Release that funds should generally include in their annual reports to shareholders a discussion of cybersecurity risks and significant fund cybersecurity incidents, to the extent that these were factors that materially affected performance of the fund over the past fiscal year.[25]

The Proposal does not appear to take into account the fact that cybersecurity risk assessments are not designed to provide the types of information called for in the proposed disclosure provisions. This is an area where the SEC should consider providing clear guidance, so that an investment adviser or fund that makes a good faith effort to make proper disclosure of cybersecurity risks can know with a degree of certainty that they are meeting the SEC's expectations.

Recordkeeping

The Proposal includes several proposed amendments to the books and records requirements under the Advisers Act. Under the Proposal, an investment adviser would be required to maintain:

[25] *Id.* at 67.

- A copy of its cybersecurity policies and procedures that are in effect, or at any time within the past five years were in effect;
- A copy of its written report documenting the annual review of its cybersecurity policies and procedures in the last five years;
- A copy of any Form ADV-C, and any amendments thereto, filed by the adviser in the past five years;
- Records documenting the occurrence of any cybersecurity incident, including any records related to any response and recovery from such an incident, in the last five years; and
- Records documenting any risk assessment conducted pursuant to its cybersecurity policies and procedures in the last five years.

Proposed Rule 38a-2 would require that a fund maintain:

- A copy of its cybersecurity policies and procedures that are in effect, or at any time within the past five years were in effect, in an easily accessible place;
- Copies of written reports provided to its board of directors for at least five years, the first two in an easily accessible place;
- Records documenting the fund's annual review of its cybersecurity policies and procedures for at least five years, the first two in an easily accessible place;
- Any report of a significant fund cybersecurity incident provided to the Commission by its adviser for at least five years, the first two in an easily accessible place;
- Records documenting the occurrence of any cybersecurity incident, including any records related to any response and recovery from such an incident, for at least five years, the first two in an easily accessible place; and
- Records documenting the fund's cybersecurity risk assessment for five years, the first two in an easily accessible place.

Comment Period

Comments on the Proposal are due 30 days after the publication of the Proposing Release in the Federal Register or 60 days after the publication of the Proposing Release on the SEC's website (*i.e.*, April 11, 2022), whichever is longer.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

James E. Anderson
202 303 1114
janderson@willkie.com

James R. Burns
202 303 1241
jburns@willkie.com

Elizabeth P. Gray
202 303 1207
egray@willkie.com

Neesa Patel Sood
202 303 1232
nsood@willkie.com

Richard M. Borden
212 728 3872
rborden@willkie.com

Richard F. Jackson
202 303 1121
rfjackson@willkie.com

Nicholas Chanin
202 303 1164
nchanin@willkie.com

John F. Rupp
202 303 1020
jrupp@willkie.com