IDC Independent Directors Council

Promoting Excellence in Fund Governance

April 11, 2022

Ms. Vanessa A. Countryman
Secretary
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-1090

Re: *Cybersecurity Risk Management Rule Proposal; File No. S7-04-22*

Dear Ms. Countryman:

The Independent Directors Council[1] appreciates the opportunity to comment on the Securities and Exchange Commission's proposed cybersecurity risk management rules for registered funds.[2] Cybersecurity risk management is a critical focus area across many industries, including for registered funds. As the Release notes, "[c]ybersecurity threat intelligence surveys consistently find the financial sector to be one of—if not the most—attacked industry, and remediation costs for such incidents can be substantial."[3]

Fund boards have a keen interest in cybersecurity matters as part of their general oversight responsibilities regarding risk management for the benefit of funds and their shareholders. Among other things, fund independent directors have a demonstrated interest in addressing information security risk management, as well as educational resources to support their understanding of this important area. Therefore, IDC strongly supports director oversight of cybersecurity preparedness and resilience.

---

[1] The Independent Directors Council (IDC) serves the US-registered fund independent director community by advancing the education, communication, and public policy priorities of fund independent directors, and promoting public understanding of their role. IDC's activities are led by a Governing Council of independent directors of Investment Company Institute (ICI) member funds. ICI's members manage total assets of $31 trillion in the United States, serving more than 100 million US shareholders, and $10 trillion in assets in other jurisdictions. There are approximately 1,600 independent directors of ICI-member funds. The views expressed by IDC in this letter do not purport to reflect the views of all fund independent directors.

[2] *See* Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, SEC Release No. IC-34497 (February 9, 2022) ("Release").

[3] Release at p. 71.

The Commission is proposing new Rule 38a-2 under Section 38 of the Investment Company Act of 1940 (Investment Company Act), which would require funds to adopt and implement policies and procedures that are reasonably designed to address cybersecurity risks.[4] In our view, the breadth and effectiveness of Rule 38a-1 (the fund compliance program rule) provides a sufficient regulatory basis to address cybersecurity risk management for registered funds. At the same time, the interests of funds and their advisers are generally aligned in their efforts to prepare for, monitor, and respond to potential information security breaches.

Nevertheless, IDC supports the Commission's proposed cybersecurity risk management rule, provided that:

- Funds retain flexibility in implementing the rule—particularly smaller funds;
- The scope of fund boards' responsibilities under the rule is consistent with their general oversight responsibilities as boards of directors, rather than the day-to-day responsibilities of a fund's manager and other service providers; and
- Fund boards may have the option to rely on cybersecurity risk management certifications supplied by the fund's principal service providers.

These recommendations are described below.

I. Overview of Proposal

Proposed Rule 38a-2 would require funds to adopt and implement written cybersecurity policies and procedures.[5] Among other things, funds would be required to identify and oversee any service providers that receive, maintain, or process fund information or are otherwise permitted to access their information systems and any information residing therein.[6] In addition, proposed Rule 38a-2 would require fund boards, including a majority of the independent directors, initially to approve the fund's cybersecurity policies and procedures that are reasonably designed to address a fund's cybersecurity risks.[7] Thereafter, boards would be required to review an annual report regarding the fund's assessment of its cybersecurity policies and procedures.[8]

The Release explains that, under proposed Rule 38a-2, fund boards should "consider what level of oversight of the fund's service providers is appropriate with respect to cybersecurity based on the fund's

[4] Release at p. 1.

[5] Release at p. 118.

[6] Release at p. 118.

[7] Release at p. 37.

[8] Release at p. 37.

operations."[9] In that regard, boards may consider the contracts and risk assessments (or summaries thereof) of any service providers that receive, maintain, or process fund information, or that are permitted to access their information systems, including the information residing therein and the cybersecurity risks they present.[10]

II. Relevance of Rule 38a-1

Rule 38a 1 under the Investment Company Act establishes the compliance oversight framework for fund boards. Adopted in 2004, Rule 38a-1 requires funds to adopt and implement written policies and procedures reasonably designed to prevent violations of the federal securities laws by the fund, including policies and procedures that provide for the oversight of compliance by certain "named service providers" (*e.g.*, a fund's investment adviser, principal underwriter, administrator, and transfer agent).[11] The board may satisfy its obligation to approve a fund's compliance policies and procedures by reviewing summaries of them.[12] The rule also requires funds to review the adequacy of the policies and procedures and the effectiveness of their implementation at least annually.[13]

In our view, the Commission could have utilized the framework established in Rule 38a-1 to ensure that funds address cybersecurity risks in their processes and procedures. As the Commission recognized, "all but the smallest funds likely take into account cybersecurity risks when developing their compliance policies and procedures under [Rule 38a-1]."[14] To the extent the Commission believes a separate rule for cybersecurity risk management is necessary, we believe that the approach should incorporate the following recommendations.

III. Recommendations

A. Flexibility in Implementation

The Release appropriately recognizes that "there is not a one size-fits all approach to addressing cybersecurity risks,"[15] and the proposed cybersecurity risk management rule should "allow firms to tailor their cybersecurity policies and procedures to fit the nature and scope of their business and

---

[9] Release at p. 38.

[10] Release at p. 38.

[11] Release at p. 10.

[12] Release at p. 37, n.52.

[13]Release at p. 10, n.13.

[14] Release at p. 76.

[15] Release at p. 14.

address their individual cybersecurity risks."[16] We agree and recommend that any adopting release expressly allow for flexibility in implementation.

This is particularly important considering the level of resources that is required to establish an effective cybersecurity risk management program that complies with the requirements contained in the rule proposal, as well as the "number and varying characteristics (*e.g.*, size, business, and sophistication) of advisers and funds."[17] In particular, small funds may have limited resources to develop or enhance cybersecurity programs,[18] and the cost of complying with an extensive set of rules and procedures could be prohibitive.[19] While cybersecurity risk management should be a priority for all funds, the Commission's rule should expressly allow funds to tailor their programs based on the funds' business operations, considering the complexity and attendant cybersecurity risks.

IDC also recommends that the Commission preserve flexibility in board reporting. Proposed Rule 38a-2 would require a fund board, including a majority of its independent directors, to review and initially approve the policies and procedures on cybersecurity risk management, and to review the written report on cybersecurity incidents and material changes to the fund's cybersecurity policies and procedures that, as described above, would be required to be prepared at least annually.[20] We support this board reporting approach, as it does not appear to contain granular reporting requirements that are overly prescriptive. We anticipate that advisers and other service providers will update fund boards in a timely manner in the event of a significant cybersecurity event impacting the fund and its shareholders.[21]

B. Scope of Fund Boards' Role

1. Board Oversight of Service Providers

It is well established that the role of fund directors is to represent the interests of the fund and its shareholders through independent oversight, rather than through day to day management of the fund

[16] Release at p. 14.

[17] Release at p. 16.

[18] Release at p. 162.

[19] Release at p. 90, n.190. Recognizing these distinctions, the Commission has requested comments on whether the Rule should allow for some flexibility. Release at p. 15.

[20] Release at p. 37.

[21] We note that, depending on the circumstances, advisers may have limited knowledge of the nature and scope of cyber threats and incidents in the first instance. Their level of awareness may evolve rapidly while, at the same time, they are engaged in remediation efforts. As such, it appears unreasonable to require advisers to notify the Commission no more than 48 hours after they have a reasonable basis to conclude that a "significant cyber incident" has occurred at the adviser or a fund it advises.

or its adviser.[22] Consistent with Rule 38a 1, IDC assumes that boards may delegate the day-to day management of cybersecurity risk to the fund's adviser or administrator, subject to board oversight. As such, while directors are not required to possess cybersecurity expertise and experience to fulfill their oversight role, they would exercise oversight consistent with their fiduciary responsibilities over service providers that have such expertise and experience.

That said, it is unclear how boards might oversee the cybersecurity risk management of certain large service providers involved in the day to day business of the fund that, for example, provide email platforms, office software, customer relationship management systems, cloud applications, and other broadly-available technology solutions.[23] IDC recommends that board oversight of a fund's cybersecurity risk management be limited to the fund's principal service providers, such as the fund's investment adviser, principal underwriter, administrator, and transfer agent. Oversight of these service providers would provide a more effective and realistic means of assessing risk to a fund and its shareholders, rather than through the review of contractual terms with, for instance, a cloud service provider.

2. Independent Director Approval of Policies and Procedures

We support the proposed requirement that a fund board, including a majority of its independent directors, review and initially approve the fund's policies and procedures on cybersecurity risk.[24] Beyond the initial establishment of policies and procedures and material amendments thereto, we generally do not view cybersecurity risk management as an activity that presents a perceived (or actual) conflict of interest between a fund and its investment adviser. As noted above, the interests of the fund and the adviser are generally aligned in efforts made to prepare for, monitor, and respond to potential information security breaches. Protecting and preserving fund and shareholder information is the common, critical objective.

C. Option to Rely on Third-Party Certifications

IDC recommends that the Commission clarify in the adopting release that, in fulfilling their oversight responsibilities, fund boards may have the option to rely upon third party reviews or certifications provided or supplied by the fund's principal service providers regarding such service providers' cybersecurity risk programs. As the Commission has observed, cyber threats and actors are increasingly

---

[22] *See* Division of Investment Management, Securities and Exchange Commission, Protecting Investors: A Half Century of Investment Company Regulation, 266 (1992), *available at* http://www.sec.gov/divisions/investment/ guidance/icreg50-92.pdf (Red Book).

[23] Release at p. 88. A fund or funds may very well lack sufficient bargaining power to compel certain service providers to make changes to their cybersecurity risk management programs.

[24] Release at p. 37.

becoming sophisticated.[25] Highly specialized and equally sophisticated cybersecurity strategies are often required to address and mitigate such risks. In our view, affirming the ability of fund boards to rely upon such reviews or certifications may be more meaningful to boards than requiring boards to review vendor-specific contractual terms or detailed descriptions of specialized technology solutions.

This approach may address some difficulties associated with board oversight of large service providers of broadly used technology services, as well as principal service providers that carry out significant and important activities across many fund complexes, such as transfer agents and custodians. An industry-level process involving third-party certifications might be an effective and efficient way to proceed in a manner that is consistent with the contours of the board's oversight role. [26]

* * *

IDC appreciates the opportunity to comment on the Commission's cybersecurity risk management rule proposal. IDC supports director oversight of fund cybersecurity preparedness and resilience. We also support the Commission's efforts to develop a comprehensive cybersecurity risk management rule, provided it is consistent with the recommendations set forth above.

If you have any questions regarding our letter or would like additional information, please contact Nicole Baker, IDC Associate Counsel, at [redacted] or me at [redacted].

Sincerely,

/s/ Thomas T. Kim

Thomas T. Kim
Managing Director
Independent Directors Council

cc: Gary Gensler, Chair, Securities and Exchange Commission
Allison Herren Lee, Commissioner, Securities and Exchange Commission
Hester M. Peirce, Commissioner, Securities and Exchange Commission
Caroline A. Crenshaw, Commissioner, Securities and Exchange Commission

[25] Release at p. 6.

[26] Release at p. 106.