

April 11, 2022

*Submitted Electronically VIA SEC.gov.*

Vanessa Countryman  
Secretary  
Securities and Exchange Commission  
100 F Street, NE  
Washington, DC 20549-1090

Re: Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies (Release Nos. 33-11028; 34-94197; IA-5956; IC-34497; File No. S7-04-22)

Dear Ms. Countryman:

The law firm of Sullivan & Worcester LLP (“Sullivan”) respectfully submits the following comments to the Securities and Exchange Commission (the “Commission”) in response to the Commission’s proposed rules (the “Proposed Rules”) contained in *Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies* (the “Proposing Release”) under the Investment Advisers Act of 1940 (“Advisers Act”) and the Investment Company Act of 1940 (“Investment Company Act”). The Proposed Rules would require registered investment advisers and registered investment companies to adopt and implement written cybersecurity policies and procedures reasonably designed to address cybersecurity risks, require advisers to report significant cybersecurity incidents affecting the adviser to the Commission, require new disclosure concerning significant cybersecurity risks and cybersecurity incidents that affect advisers and investment companies and their clients and shareholders, and impose new recordkeeping requirements. For over sixty years, Sullivan has represented both large and small investment company complexes and business development companies (“Funds”), their boards of directors/trustees and independent directors/trustees (“Boards”), and their investment advisers (“Advisers”) with respect to regulatory matters under the Investment Company Act and other federal securities laws.

We commend the Commission on its efforts in developing the Proposed Rules. The Proposed Rules address many of the concerns raised over the years by Advisers, Funds, and Boards in connection with cybersecurity policies, procedures, and incidents. However, in our view, the Proposed Rules fail to strike the right balance between the need for enhanced cybersecurity protections and the Board’s traditional oversight role. We also believe the Proposed Rules do not properly allocate duties and responsibilities among the Board and Fund management in a manner that enables them to apply their respective competencies and expertise and use the resources available to them in a manner that is most appropriate given their respective roles.

We support an active and engaged role for Fund Boards when it comes to cybersecurity matters; however, we believe the Proposed Rules would place a heavy burden on Boards that would ultimately not add value to or further the stated goals of the Proposed Rules to enhance cybersecurity preparedness and improve investor confidence in the resiliency of Advisers and Funds against cybersecurity threats and

attacks. There are a number of areas that we believe require further consideration and clarification. We discuss these matters below.

*Approval of Adviser Cybersecurity Policies and Procedures* – The Proposed Rules would require a Fund’s Board, including a majority of the independent Board members, initially to approve the Adviser’s cybersecurity policies and procedures.<sup>1</sup>

We agree that Fund Boards should take an active role when it comes to the cybersecurity preparedness of their Funds. Staying current on the state of a Fund’s cybersecurity preparedness should include, at a minimum, regular updates and analysis from Fund management on the Adviser’s policies and procedures, infrastructure, cybersecurity risks and incidents, as the Proposed Rules provide. However, we believe the Proposed Rules misallocate responsibility when they require Fund Boards to initially approve the Adviser’s cybersecurity policies and procedures.

Cybersecurity policies and procedures are highly technical in nature and likely to be dependent on and tailored to the systems used by an Adviser and other service providers. It is unlikely that a Fund Board would have the detailed knowledge of the full scope of the Adviser’s business, risks and technical needs or the technical expertise to be able to meaningfully evaluate the Adviser’s cybersecurity policies and procedures. We note that Fund Boards contract with the Adviser and oversee the related services but do not supervise the day-to-day operations of the Adviser. Many Advisers have product offerings and lines of business unrelated to their Fund business which are not discussed in detail with the Board but would be implicated by any Adviser cybersecurity policies and procedures. Additionally, an Adviser that is part of a large financial services firm with brokerage, investment banking, commercial banking, or insurance operations will likely have enterprise-wide cybersecurity policies and procedures. Any changes to such policies and procedures proposed by a Fund Board likely would require amendments on an enterprise-wide basis and the application of changes to unrelated lines of business and operations.

In the Proposing Release the Commission notes that the Proposed Rules “would provide flexibility for the adviser and fund to determine the person or group of people who implement and oversee the effectiveness of its cybersecurity policies and procedures,”<sup>2</sup> and recognizes “that a cybersecurity expert may provide needed expertise and perspective to the annual review,”<sup>3</sup> showing how important the use of experts is in this process. Given the technical expertise and operational business knowledge required to assess cybersecurity policies and procedures, Fund Boards are not in a position to approve these policies and procedures. The Board’s traditional oversight role is inconsistent with evaluating the appropriateness of highly technical requirements related to operational considerations that Fund Boards do not normally oversee.

Accordingly, we recommend that the Commission not require a Fund’s Board to approve the cybersecurity policies and procedures of the Fund’s Adviser. A better approach is to require the Adviser to appoint an individual or entity to be responsible for its cybersecurity policies and procedures and have this individual or entity make regular periodic reports to the Fund Board, including in executive sessions, and to require prompt reporting to the Board of any cybersecurity incidents impacting the Fund and/or the

---

<sup>1</sup> See *Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies*, 87 FR 13524 (proposed March 9, 2022) (to be codified at 17 CFR Parts 230, 232, 239, 270, 274, 275, and 279).

<sup>2</sup> *Id.*

<sup>3</sup> *Id.*

Adviser. The sentiments expressed in the Derivatives Rule (Rule 18f-4 under the Investment Company Act), that the Board can take an active role in oversight without requiring the Board itself to directly approve policies and procedures, would be a more appropriate guide for the Commission.<sup>4</sup> Any policies and procedures approved by a Fund's Board relating to cybersecurity may more meaningfully include a cybersecurity communication policy which requires updates and notifications from Fund management and service providers of cybersecurity matters and might include a cybersecurity incident escalation process.

*Approval of Service Providers Cybersecurity Policies and Procedures* – In question 27,<sup>5</sup> the Proposing Release asks whether, as part of their oversight function, Fund Boards should also be required to approve the cybersecurity policies and procedures of certain of the Fund's service providers.

All of the concerns addressed above relating to the approval of Adviser cybersecurity policies and procedures are also applicable to the approval of Fund service providers' cybersecurity policies and procedures. However, when it comes to Fund service providers, there is an additional concern that Board members would be required to evaluate policies and procedures of entities with which the Board has limited direct contact. Moreover, the service providers' cybersecurity policies and procedures will likely be tailored to their own business, which may extend to banking, insurance, or other business lines.

Further, we are concerned that Fund Boards will have limited leverage or ability to influence or change the cybersecurity policies and procedures of a Fund's service providers. A large custodian bank, for example, may serve hundreds of Fund groups. The custodian bank cannot reasonably be expected to modify its cybersecurity policies and procedures at the request of one group of Funds.

More complex scenarios could occur when different Fund Boards provide conflicting advice to a service provider. For example, one Board could tie approval of a service provider's policies and procedures to an increase in dedicated cybersecurity staff, while another Board might ask for an increase in dedicated cybersecurity technology. A service provider with limited budget may only be able to satisfy one of these requests.

We note that many Advisers already evaluate Fund services providers' cybersecurity policies and procedures when initially engaging a service provider for a Fund and on a periodic basis going forward. Given the heightened focus on cybersecurity over the past few years, it has become commonplace for Fund Boards to receive periodic reports concerning Fund service providers' cybersecurity policies and procedures.

Ultimately, the service provider itself is more appropriately situated for determining best practices and deployment of resources for its cybersecurity needs than a Fund Board that may only be using limited aspects of the service provider's business.

There is also a need for clarity on what actions are required if a Fund Board cannot approve a service provider's cybersecurity policies and procedures or if it feels that aspects of the policies and procedures are inadequate or could be improved. It is unclear whether a Fund Board would be required to

---

<sup>4</sup> See 85 FR 83162 (2020).

<sup>5</sup> See Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, 87 FR 13524 (proposed March 9, 2022) (to be codified at 17 CFR Parts 230, 232, 239, 270, 274, 275, and 279).

change service providers in this event or whether there could be an opportunity for a Board to work with a service provider over time to develop a satisfactory policy.

We therefore recommend that the Commission not require the approval of the cybersecurity policies and procedures of Fund service providers.

*Should Boards have a Cybersecurity Committee* – In question 28,<sup>6</sup> the Proposing Release asks if a Fund’s Board, or some designee such as a sub-committee or cybersecurity expert, should have oversight over the Fund’s risk assessments of service providers.

As noted above, the Proposing Release routinely makes reference to flexibility and allowing for tailoring to the nature and scope of businesses and specific cybersecurity risks.<sup>7</sup> We support this goal and believe that it will especially benefit smaller Fund complexes and decrease their costs of compliance with the Proposed Rules.

However, adding specific requirements to the rule, such as requiring Fund Boards to have a cybersecurity expert or a specific committee, directly contradicts this goal and could significantly increase the burdens and costs of compliance, especially for smaller Fund complexes. We note that some Boards may wish to address cybersecurity as a full Board matter and others may wish to delegate this responsibility to a committee. These considerations are based on the facts, circumstances and dynamics of each Board and there are benefits to each approach. Proposed Item 106(c)(1) suggests that one or more specific Board members may be responsible for cybersecurity. We note that even if a committee structure is used, the decision-making and evaluation of cyber matters should be a full Board responsibility and, in any event, no specific members of the Board should be solely responsible for cybersecurity.

We believe that the Commission should generally leave these decisions to the discretion of Fund Boards as they are in the best position to assess the necessity and the cost-benefit tradeoff for their specific circumstances.

Accordingly, we would recommend that the Commission not mandate the establishment of cybersecurity committees or identify or regard any individual Board member as more or less responsible for cybersecurity.

*Whether the Board Approval Should be Based on a Specific Finding* – In question 29,<sup>8</sup> the Proposing Release asks for comments on whether the Commission should require Boards to base their approval of cybersecurity policies and procedures on any particular finding.

Our experience suggests that a broad finding such as the one suggested in the Proposing Release (“reasonably designed to prevent violations of the Federal securities laws”) would not add significant value. It is unlikely that a Fund Board would approve cybersecurity policies and procedures if the policies and procedures did not satisfy such a broad standard. However, if a narrow finding is used (such as “that the budget or staffing dedicated are sufficient” or “material risks have been identified and accounted for”) we believe this would unduly limit the flexibility of Funds and Advisers to tailor cybersecurity policies and

---

<sup>6</sup> *Id.*

<sup>7</sup> *Id.*

<sup>8</sup> *Id.*

procedures to their specific risks and circumstances. Further, Fund Boards are not in a position to assess entity-wide resources, particularly for larger enterprises. A narrow requirement could place too much focus on satisfying the narrower requirement when designing cybersecurity policies and procedures. Policies and procedures created under these restrictions may be less suited to a Fund's or Adviser's particular risks and circumstances than would otherwise have been made.

Therefore, we recommend that the Commission not require Fund Boards to approve cybersecurity policies and procedures on the basis of any particular finding.

*Comparison to Public Company Proposal* – There are some needed areas of clarity and comparison we would like to highlight given the close proximity between the announcements of the Proposed Rules and the public company proposal *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure* (the “Public Company Proposal”).

*Will Fund Boards be required to disclose their cybersecurity expertise?* The Public Company Proposal would amend Item 407 of Regulation S-K to require disclosure of whether any member of the registrant's Board has expertise in cybersecurity, and if so, the nature of such expertise.<sup>9</sup>

There are several negative consequences that could occur from requiring disclosure of the cybersecurity expertise of Board members. For example, there is a concern that such disclosure could suggest that any given Board member has greater or less responsibility for cyber oversight based on his or her experience. As a result, this may expose Board members to liability or reputational harm if a cybersecurity incident occurs. Additionally, this approach does not reflect a robust Board decision-making process where differing perspectives and areas of expertise combine dynamically to evaluate issues. Even the threat of litigation in this area could increase costs by leading to higher D&O/E&O insurance premiums.

Further, because of the potential liability or reputational harm this requirement might have a chilling effect on the recruitment of strong candidates, with or without cybersecurity experience, to serve on Fund Boards.

For these reasons, we recommend against requiring disclosure regarding the cybersecurity expertise of Fund Boards.

*Differences in Board treatment.* We note that the Public Company Proposal merely requires companies to disclose how the Board oversees cybersecurity governance but does not mandate the way in which the Board does so.

Unlike areas of particular relevance to Funds (*e.g.*, liquidity or derivatives risk management), we see no reason to apply a different standard to Funds than to public companies when it comes to cybersecurity risk management. The management of cybersecurity risks is equally important to Funds and public companies. We note that many Advisers to Funds are themselves public companies or are owned by public companies. This supports applying the same standard to Funds and public companies.

---

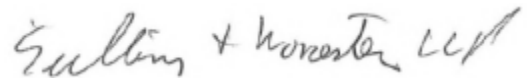
<sup>9</sup> See *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, 87 FR 16590 (proposed March 23, 2022) (to be codified at 17 CFR Parts 229, 232, 239, 240, and 249).

Further, as noted above, a less prescriptive rule would be more in line with the Proposed Rules' focus on flexibility and would allow Funds of varying sizes, particularly smaller Fund complexes, to adopt cybersecurity policies and procedures that are tailored to their specific circumstances with less costs and other burdens.

Given the emphasis on flexibility in the Proposed Rules, we encourage the Commission to take a similar approach of requiring disclosure of cybersecurity governance for Funds as they have taken in the Public Company Proposal or provide further clarity on the reason behind taking a different approach between the Public Company Proposal and the Proposed Rules.

We thank the Commission for its consideration of our comments with respect to the Proposed Rules. Please feel free to contact us if we can provide any additional assistance to you as you further evaluate these matters.

Sincerely,

A handwritten signature in cursive script that reads "Sullivan & Worcester LLP".

Sullivan & Worcester LLP