



July 28, 2022

Ms. Vanessa Countryman, Secretary  
U.S. Securities and Exchange Commission  
100 F Street, NE  
Washington, DC 20549-1091

Re: Proposed Cybersecurity Risk Management Program Rule; File No. S7-04-22

Dear Ms. Countryman:

The Investment Company Institute<sup>1</sup> is writing to supplement our April comment letter<sup>2</sup> on the Commission's proposed cybersecurity risk management rules for funds and advisers.<sup>3</sup> We urge the Commission to revise proposed subsection 38a-2(a)(3)(ii), which would require funds,<sup>4</sup> to execute a written contract with each service provider that has access to a fund's information or information systems ("information-handling service providers") in which the service provider agrees to implement and maintain appropriate measures, including the practices described in

---

<sup>1</sup> The Investment Company Institute (ICI) is the leading association representing regulated investment funds. ICI's mission is to strengthen the foundation of the asset management industry for the ultimate benefit of the long-term individual investor. Its members include mutual funds, exchange-traded funds (ETFs), closed-end funds, and unit investment trusts (UITs) in the United States. Its members manage total assets of \$29.6 trillion in the United States, serving more than 100 million investors, and an additional \$9.3 trillion in assets outside the United States. ICI has offices in Washington, DC, Brussels, London, and Hong Kong and carries out its international work through [ICI Global](#).

<sup>2</sup> Letter to Vanessa A. Countryman, Secretary, US Securities and Exchange Commission from Susan M. Olson, General Counsel, Investment Company Institute (April 11, 2022), available at <https://www.sec.gov/comments/s7-04-22/s70422-20123076-279408.pdf>

<sup>3</sup> *Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies*, SEC Release Nos. 33-11028, 34-94197, IA-5956, and IC-34497; File No. S7-04-22 (February 9, 2022) (Release), available at <https://www.sec.gov/rules/proposed/2022/33-11028.pdf>. The proposed rule defines funds as registered investment companies and business development companies.

<sup>4</sup> The cybersecurity program rule proposal for investment advisers (Rule 204-6) includes the same problematic requirement for investment advisers and their information-handling service providers. Our comments should be read as also applying to the same requirement in that proposed rule.

paragraphs (a)(1), (a)(2), (a)(3)(i), (a)(4), and (a)(5) of Rule 38a-2 (the “SPC subsection” or “subsection”).

The SPC subsection risks severely compromising the ability of funds to continue to conduct business with critical service providers. Many information-handling service providers will be unwilling or unable to enter into a written contract with the required provisions. At the same time, this element of the rule is unnecessary. If a fund breaches its obligations to maintain the security of its information under Rule 38a-2, the Commission can proceed against the fund, irrespective of the language in the fund’s contract with a service provider. In addition, the Commission can proceed against service providers for aiding and abetting a violation by the fund, irrespective of the language in the contract.<sup>5</sup>

We therefore urge the Commission to revise the written contract requirement to avoid adversely impacting funds’ cybersecurity risk management programs by impeding arrangements with critical service providers. The Commission can revise the subsection in a way that both addresses our concerns and furthers the Commission’s objectives to assure funds have robust and comprehensive cybersecurity programs.<sup>6</sup> We recommend that the Commission revise the subsection as follows:

**§ 270.38a-2 Cybersecurity policies and procedures of certain investment companies.**

(a) *Cybersecurity policies and procedures.* Each fund must adopt and implement written policies and procedures that are reasonably designed to address cybersecurity risks, including policies and procedures that:

\* \* \*

(3) *Information protection.*

\* \* \*

(ii) Require oversight of service providers that receive, maintain, or process fund information, or are otherwise permitted to access fund information systems and any fund information residing therein. ~~and through that oversight document that such service providers, pursuant to a written contract between the fund and any such service provider, are required to implement and maintain appropriate measures, including the practices described in paragraphs (a)(1), (a)(2), (a)(3)(i), (a)(4), and (a)(5) of this~~

---

<sup>5</sup> See Gemini Fund Services, LLC, 4847 SEC (Jan. 22, 2018); see also Apex Fund Services (US), Inc., 4429 SEC (June 16, 2016) (where the Commission pursued enforcement against fund administrators for causing liability).

<sup>6</sup> In our April comment letter, we recommended that the Commission issue cybersecurity rules for other SEC registrants, particularly broker-dealers and transfer agents.

~~section, that are~~ Such oversight shall be designed to protect fund information and fund systems. With respect to any service provider that is registered with and regulated by the Commission, such fund shall take reasonable steps to ensure that such service provider implements and maintains appropriate measures to protect the fund's information or systems, as applicable, including the practices described in paragraphs (a)(1), (a)(2), (a)(3)(i), (a)(4), and (a)(5) of this section.

### **The SPC Subsection Will Adversely Impact Funds' Ability to Engage Service Providers and Conduct Business**

Proposed subsection 38a-2(a)(3)(ii) would require funds to have the specified written contract with each service provider that has access to the fund's information or information systems. The terms "fund information," "fund information systems," and "personal information" are broadly defined in the rule.<sup>7</sup> Consequently, the breadth and effect of this provision will be substantial, sweeping hundreds, if not thousands, of service providers into the contract requirement, including firms that are not subject to Commission regulation and have customers and clients not subject to Commission regulation. Plain English suggests a wide array of firms will be information-handling service providers including firms traditionally engaged in providing services to the financial services industry such as transfer agents, custodians, banks, financial intermediaries, clearing firms, attorneys, accountants, etc. – along with telecommunications firms (*e.g.*, AT&T, Verizon, Comcast, Sprint), cloud providers (*e.g.*, AWS, Microsoft Azure), firms that service, maintain and repair office machinery and technology (*e.g.*, printers, scanners, copiers, computers, networks), print shops, and a variety of consultants, vendors, and third-party experts.<sup>8</sup>

The Release is silent on what the Commission expects funds to do when, in attempting to comply with the contract requirement, their service providers refuse to revise their existing agreements or do business with funds. We have serious concerns that there may not be alternative providers to supply many of these services.

---

<sup>7</sup> Proposed Rule 38a-2(f) provides, in part.: (1) "fund information" means any electronic information related to the fund's business, including personal information, received, maintained, created, or processed by the fund; (2) "fund information systems" means the information resources owned or used by the fund, 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 fund information to maintain or support the fund's operations; and (3) "personal information" means any information that can be used, alone or in conjunction with any other information, to identify an individual, such as name, date of birth, place of birth, telephone number, street address, mother's maiden name, Social Security number, driver's license number, electronic mail address, account number, account password, biometric records or other nonpublic authentication information. Release at 199.

<sup>8</sup> In many cases, it will be impractical and too complex to agree to these measures. For example, service providers, like telecommunication and internet providers, will be unable to distinguish which information flowing through their systems or utilizing their services is "fund information."

Ms. Vanessa A. Countryman  
July 28, 2022  
Page 4 of 4

### **The SPC Subsection is Unnecessary to Ensure Comprehensive Cybersecurity Programs**

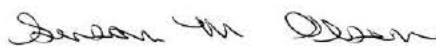
Proposed Rule 38a-2 is intended to ensure that funds adopt and implement comprehensive cybersecurity programs. The requirements of subsection 38a-2(a)(3)(ii) are not necessary to fulfill the Commission's goal. As recognized by the Commission, funds have long taken seriously their obligation to protect their systems and the confidentiality of their non-public information against threats, including cybersecurity threats. Funds spend considerable resources protecting their systems and information from intrusions. Funds have agreements with service providers with provisions that the fund believes are necessary for its business operations and, at a minimum, to ensure its compliance with the Federal securities laws. The subsection will not provide additional protection to funds' information and systems.

We urge the Commission to focus on the effectiveness of funds' cybersecurity programs. It is the obligation and responsibility of each fund to oversee, negotiate, and manage these relationships. If it fails to do so, the Commission can proceed against the fund and its service providers, irrespective of any contract language.<sup>9</sup> But, in any event, it is neither necessary nor appropriate for the Commission to require funds to impose SEC rule provisions on funds' information-handling service providers.

### **Conclusion**

The Institute urges the Commission to design any final rule to avoid adversely impacting funds' cybersecurity programs. We believe our recommended changes would avoid the deleterious circumstances we describe, while, at the same time, better accomplish the protections the Commission intends under the rule. We thank you for your attention to this very important matter.

Sincerely,



Susan M. Olson, General Counsel

cc: The Honorable Gary Gensler  
The Honorable Hester M. Peirce  
The Honorable Caroline A. Crenshaw  
The Honorable Mark T. Uyeda  
The Honorable Jaime Lizárraga  
Division Director William Birdthistle  
Division Deputy Director Sarah ten Sietoff

---

<sup>9</sup> See note 5, *supra*.