INVESTMENT COMPANY INSTITUTE

1401 H Street, NW, Washington, DC 20005-2148, USA
202/326-5800 www.ici.org

April 11, 2022

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

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

Dear Ms. Countryman:

The Investment Company Institute[1] appreciates the opportunity to provide its comments on the proposal by the U.S. Securities Exchange Commission (the Commission or SEC) to require registered investment companies and investment advisers to adopt and implement written cybersecurity risk programs.[2] As proposed, such programs must include policies and procedures that are reasonably designed to address the registrant's cybersecurity risks. The proposal would also impose disclosure, reporting, and recordkeeping requirements on funds and advisers.

We are pleased that the Commission has proposed rules that would require registrants to have formal programs designed to address cybersecurity risks. Currently, the only information security requirement applicable to SEC registrants is in Section 248.30 of

[1] 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, and UCITS and similar funds offered to investors in Europe, Asia and other jurisdictions. Its members manage total assets of $31.0 trillion in the United States, serving more than 100 million investors, and an additional $10.0 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.

[2] *See 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).

Regulation S-P, which "requires registrants to adopt policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information." In light of the proliferation of cyber risks since this provision was adopted in 2002, we believe it is appropriate for the Commission to impose greater rigor on registrants' information security and support the Commission's adoption of appropriate rules in this area.

Executive Summary

While the Institute supports the Commission's proposal, we recommend various revisions to the proposal to ensure that it provides registrants the flexibility necessary to implement such programs in a way that both (1) does not disrupt their current cybersecurity policies, procedures, and processes and (2) enables such programs to mature and evolve to address new cybersecurity risks and vulnerabilities and changes in technologies.

As discussed in detail in this letter, the Institute:

- Supports adoption of the elements that would be required to be included in registrants' cybersecurity policies and procedures;
- Recommends expanding the scope of the proposal to include all SEC registrants, including broker-dealers and transfer agents;
- Opposes applying the rule to service providers that are not subject to the Commission's regulatory authority;
- Recommends narrowing the scope of service providers covered by the rules to exclude those that present little risk to the fund or adviser and those whose cybersecurity practices are already subject to government oversight;
- Consistent with Rule 38a-1 and the annual review process, urges the Commission to expressly provide registrants flexibility in how they conduct annual reviews of their program under this proposed rule;
- Supports board oversight of funds' and advisers' programs while recognizing fund boards are not cybersecurity experts;
- Recommends that the Commission clarify that the proposed recordkeeping requirements will only apply prospectively;
- Urges that the definitions for "cybersecurity threat" and "significant cybersecurity incident" be revised to target those threats and incidents impacting a fund's or adviser's ability to maintain critical operations or protect information;
- Opposes requiring public disclosure of a fund's or adviser's cybersecurity incidents;

- Opposes the imposition of these requirements under Section 206 of the Investment Advisers Act as the failure to have such a program should not be considered fraud;

- Opposes the adoption of Form ADV-C or any electronic or paper form to notify the Commission of significant cybersecurity incidents;

- Opposes using a form or other means of electronic filing to provide the Commission notice of significant cybersecurity incidents;

- Opposes requiring information on remediation, disclosures, and cyber insurance be included in any notice provided to the Commission of significant cybersecurity incidents;

- Urges a 24-36 month compliance period to better facilitate and ensure an effective and orderly implementation; and

- Due to the complexity of the issues raised by the proposal, urges that the Commission be prepared and willing to provide necessary guidance to registrants once the rules are adopted.

1. The Importance of Effective Information Security

The importance of, and necessity for, effective information security increases with each passing day as bad actors – including nation states[3]– remain intent on penetrating systems of financial institutions to access or exfiltrate their data. As noted in the Release, advisers and funds

> . . . face numerous cybersecurity risks and may experience cybersecurity incidents that can cause, or be exacerbated by, critical system or process failures. . . . At the same time, cyber threat actors have grown more sophisticated and may target advisers and funds, putting them at risk of suffering significant financial, operational, legal, and reputational harm. Cybersecurity incidents affecting advisers and their funds also can cause substantial harm to their clients and investors.[4]

[3] As we learned from the recent SolarWinds breach, cyber compromises are not limited to the private sector. The recent SolarWinds breach "allowed the threat actor to breach several federal agencies networks that used the software." *See Federal Response to SolarWinds and Microsoft Exchange Incidents,* GAO-22-104746 (January 2002). According to the GAO, "The federal government later confirmed the threat actor to be the Russian Foreign Intelligence Service." According to the SEC's Inspector General, "in the wake of the SolarWinds compromise, in FY 2021 [the SEC] initiated and completed a special review of the SEC's initial response and compliance with CISA Emergency Directive 21-01, *Mitigate SolarWinds Orion Code Compromise* (dated December 13, 2020) and supplemental guidance." *See* Memorandum from Carl W. Hoecker, SEC Inspector General, to Gary Gensler, SEC Chair (October 8, 2021) (SEC Inspector General Memo).

[4] Release at pp. 6-7.

Members of the Institute have long taken seriously their obligation to protect their systems and the confidentiality of their non-public information against *any* type of threat – including cybersecurity threats. This is not surprising as our members' brands and success as a business are highly dependent upon investor confidence. Cybersecurity attacks or incidents could easily and quickly erode or destroy such confidence.

We are pleased that, when the SEC held its Cybersecurity Roundtable in 2014, Roundtable participants described the financial services sector of the economy, including the asset management industry, as "way ahead of the rest of our nation's cybersecurity."[5] According to Roundtable participant Larry Zelvin, who was then Director, National Cybersecurity and Communications Integration Center, U.S. Department of Homeland Security:

> As you look at the 16 critical infrastructures, finance probably wins the cybersecurity threat award. . . . So you are a massive target, and you're a target for two reasons in my mind. First is because you're where the money is. The second one is that you also represent our nation. There was a time when nations used to focus on their militaries. They would focus potentially on commerce overseas. Now they can focus on the commerce within your own nation.
>
> [T]he financial sector . . . is way ahead of the rest of our nation's cybersecurity, reason being is – is you're getting attacked a lot. I'd encourage you on the information sharing we get there to share that information not only with the people you work with in business both nationally and internationally, but also with government because we have a lot of work to do with a number of sectors that you rely upon for your businesses *that we need to benefit from your experience.*[6]

Mr. Zelvin also as stated that, with respect to cybersecurity, the financial services sector is "doing extraordinary work. It's highly impressive."[7]

The Release echoes comments from the Roundtable when it states:

> The financial services sector has . . . been at the forefront of digitization *and now represents one of the most digitally mature sectors of the*

---

[5] *See Cybersecurity Roundtable Transcript* at p. 13.

[6] *Id.* at pp. 12-13. [Emphasis added.]

[7] *Id*. at p. 19.

> *economy. Not surprisingly, it is also one of the biggest spending on cybersecurity measures.*[8]

When asked at the Roundtable, "what the SEC should do in this space"—*i.e.,* to address cybersecurity concerns in the financial services industry – the panelists' responses included the following:

> . . . the SEC should provide principle-based guidance and avoid any attempt to issue prescriptive rules as it relates to cybersecurity controls. Simply for the reason we've talked about so many times is the constantly changing threat landscape. Any prescriptive rules would be outdated potentially by the time they were written and by the time they were put into place.
>
> * * *
>
> I think all of us are so unique that trying to put anything more prescriptive into place would be extremely difficult. And I think at the end of the day it probably wouldn't have the desired effect.
>
> * * *
>
> [I] agree with a lot of what's been said. The experts I talked to – their number one thing was please resist the urge to impose rigid or prescriptive requirements.[9]

Participants in the Roundtable also strongly recommended that, in taking any steps to address cybersecurity concerns, all federal regulators of financial institutions work collaboratively on these issues and "actually talk to each other"[10] to avoid conflicting regulations and requirements.

As the Commission considers adopting its proposed rules, we share and echo these recommendations. We urge the Commission to recognize the experiences and observations of these experts, the work of colleagues in the federal government that regulate the financial services sector, and the success our industry has had – in the absence of regulatory requirements – in maintaining effective information security programs. Much is at stake so it is critical that the Commission act responsibly and utilize the expertise of stakeholders. The Commission must ensure that any rules it adopts in this area align with existing federal regulations imposed on financial

---

[8] Release at p. 79. [Emphasis added.]

[9] *Cybersecurity Roundtable Transcript* at pp. 91-92. These comments were made in response to a question by the panel moderator, David Grim, who, at the time was the Deputy Director in the SEC's Division of Investment Management.

[10] *Id*. at p. 93.

institutions. Further, it is essential that the Commission avoid imposing overly prescriptive requirements that would disrupt registrants' long-standing information security programs or fail to provide needed flexibility to respond to new and changing threats.

2. The Commission's Previous Efforts to Regulate Information Security

The current proposal is not the Commission's first attempt to adopt rules to regulate registrants' information security since it adopted Regulation S-P in 2000.[11] In March 2008, the Commission proposed amendments to Regulation S-P to require SEC registrants to develop, implement, and maintain a comprehensive information security program.[12] While the Institute supported the Commission revising Regulation S-P to impose more rigorous information security requirements,[13] our comment letter recommended that, in lieu of adopting the rules as proposed, the Commission revise its proposal to better align its requirements with those of the Interagency Guidelines Establishing Information Security Standards (Interagency Guidelines).[14]

The Interagency Guidelines were adopted in February 2001 by the Department of the Treasury, the Federal Reserve System, and other federal regulators of banking institutions. We supported such alignment because it would facilitate compliance with the SEC's requirements by those SEC registrants that are subject to such other regulators' jurisdiction and it would avoid such registrants having to reconcile their existing information security programs with new SEC rules.[15] As discussed in more detail below, we again recommend the SEC revise its proposal to align its requirements with those of the Interagency Guidelines. It would be counterproductive and disruptive to do otherwise. Those Guidelines have now been in place for over twenty years – more than two decades. The requirements are, and have long been, well embedded in financial institutions and they

---

[11] *See Privacy of Consumer Financial Information,* SEC Release Nos. 34-42974, IC-24543, and IA-1883 (June 27, 2000). Section 248.30 of Regulation S-P requires registrants to safeguard customer records and information.

[12] *See Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information,* Release No. 34-57427 and IA-2712, 73 FED. REG. 13692 (March 13, 2008) (the SEC's 2008 Proposal). Following the comment period, no further action was taken on this proposal. Importantly, the scope of SEC's 2008 proposal would have included brokers, dealers, and transfer agents.

[13] *See* Letter from Tamara K. Salmon, Senior Associate Counsel, ICI, to Ms. Nancy M. Morris, Secretary, U.S. Securities and Exchange Commission, dated May 2, 2008 (the Institute's 2008 Letter).

[14] 66 FED. REG. 8616 (Feb. 1, 2001).

[15] As noted above, at the time of our recommendation in 2008, the Interagency Guidelines had been in place for at least seven years.

have withstood the test of time. This, in part, is due to the federal banking regulators revising them as necessary to ensure their continued effectiveness.[16]

3. The Commission's Current Proposal is Too Limited in Scope

The Commission has proposed to adopt rules under Section 38 of the Investment Company Act of 1940 (ICA) and Section 206 of the Investment Advisers Act (Advisers Act) to require registered investment companies and investment advisers, respectively, to adopt, implement, and maintain information security programs.[17] Noticeably, and surprisingly, missing from the Commission's proposal are rules under the Securities Act of 1934 requiring brokers, dealers, and transfer agents to have cybersecurity risk programs. These are firms over which the SEC has jurisdiction. Because there is no mention of these registrants in the Release, we are uncertain as to the Commission's rationale in excluding these registrants from the proposal.

We note that all of the arguments and rationale motivating the Commission to propose rules requiring registered investment companies and investment advisers to have such programs holds true for SEC registrants like brokers, dealers, and transfer agents. Indeed, in discussing how advisers and funds "depend on technology for critical business operations," the Release observes that "[a]dvisers and funds are exposed to, and rely on, a broad array of interconnected systems and networks, both directly and through service providers, *such as custodians, brokers, dealers,* pricing services, and other technology vendors."[18] While custodians would be subject to the Interagency Guidelines, we are not aware of *any* rules requiring brokers and dealers or transfer agents to have information security programs along the lines of what the Commission has proposed for registered investment companies and advisers. And yet, they are SEC registrants and part of the "interconnected systems" that are, in part, the basis for the Commission's proposal.

3.1 Broker-Dealers Should be Within Scope

While historically, many mutual fund investors purchased their fund shares directly from the fund through the fund's transfer agent, today many, if not most, investors purchase their shares through a broker-dealer. When that happens, in addition to effecting the trade, it is common for the broker-dealer, *not the fund company's transfer agent and not the fund*,

---

[16] For example, effective April 1, 2022, the federal banking regulators adopted a new rule imposing an incident notification requirement on banking organizations. This new rule requires banking institutions to notify their primary federal regulator of certain computer security incidents. *See Computer-Security Incident Notification Requirements of Banking Organizations and Their Bank Service Providers,* 12 CFR Parts 53, 225, and 304 (November 23, 2021).

[17] As discussed in more detail under Section 6, below, the Institute opposes citing the SEC's antifraud authority in proposing rules to require investment advisers to have information security programs.

[18] Release at p. 6.

to maintain the records relating to the investor's mutual fund transactions.[19] To most effectively advance and support the Commission's interest in protecting mutual fund investors from the "substantial harm" caused by cybersecurity incidents,[20] broker-dealers should be within the scope of the Commission's proposed rules.
According to FINRA's 2019 Annual Report (the latest available), in 2019, FINRA's technology looked across markets to detect potential fraud, and there were, on average, 71.5 billion market events processed through this technology *every day.*[21] We presume that the "events" FINRA monitors involve transactions processed by its members through systems that are part of the "interconnected systems and networks" referenced in the Release. No doubt, many of these transactions involve the purchase or sale of mutual fund shares held in brokerage accounts.[22]

Since the Commission's proposal, in large part, is intended to protect mutual fund investors, it is anomalous that the rules will fail to extend these protections to investors who are customers of a broker-dealer. If FINRA's rules required its members to have information security programs in place, investors might have some assurance that they are protected from cyber incidents occurring at broker-dealers. But this is not the case.

According to FINRA's website (www.finra.org) (as of the date of this letter), "FINRA Rules Related to Cybersecurity" consists of Rule 3110 (Supervision), 3120 (Supervisory Control System), Rule 4530(b) (Reporting Requirements), and Supplementary Material 4530.01 (Reporting of Firms' Conclusions of Violation). *None* of these rules mentions cybersecurity or information security nor do they impose any requirements on broker-dealers related to these topics.[23] Under the heading of "SEC Rules Related to Cybersecurity," FINRA's website lists the following: 248.201-202 (Regulation S-ID: Identity Theft Red Flags), 248.1-100 (Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information), and 240.17a-4(f), relating to recordkeeping. Again, none of these SEC rules

---

[19] *See Transfer Agent Regulations,* Release No. 34-76743 (December 22, 2015) (2015 Transfer Agency Release) at p. 161. [Emphasis added.]

[20] Release at p. 7.

[21] *See 2019 FINRA Annual Financial Report* (FINRA) at p. 3.

[22] While many investors purchase mutual funds shares through investment professionals, including broker-dealers, retail investors purchase closed-end funds and ETF shares, which are listed on an exchange or traded in the over-the-counter market, through a broker-dealer. *See*, ICI Fact Book, 2021, Chapter 7 (characteristics of mutual fund owners and where investors own mutual funds), available at https://www.icifactbook.org/21_fb_ch7.html#mfinvestors.

[23] FINRA Supplementary Material 4530.01, which supplements the requirement in Rule 4530 that requires FINRA members to report violations of law to FINRA, clarifies that a FINRA member must report "only conduct that has widespread or potential widespread impact to the member or its customers or to the markets, or conduct that arises from a material failure of the member's systems, policies or practices involving numerous customers, multiple errors, or significant dollar amounts."

require broker-dealers to have information security programs along the lines of what the SEC is proposing for funds and advisers.

To address this omission and ensure that all SEC registrants are required to establish, implement, and maintain an information security or cybersecurity risk program, we urge the Commission to impose upon brokers and dealers regulatory requirements substantively identical to those it proposes for investment companies and investment advisers. This recommendation is consistent with the approach the SEC took in its 2008 Proposal, which would have applied to broker-dealers. For reasons not explained in the Release, the SEC's current proposal is limited and surprisingly departs from the approach in the 2008 Proposal.

3.2 Transfer Agents Should be Within Scope

As externally managed organizations, mutual funds and other investment companies typically have no employees and are reliant upon a variety of external entities to conduct business. Every mutual fund has a transfer agent. The role of a mutual fund's transfer agent is explained in the Institute's annual *Fact Book* as follows:

> Mutual funds and their shareholders rely on the services of transfer agents to maintain records of shareholder accounts; calculate and distribute dividends and capital gains; and prepare and mail shareholder account statements, federal income tax information, and other shareholder notices. Some transfer agents also prepare and mail statements confirming shareholder transactions and account balances. Additionally, they may maintain customer service departments, including call centers, to respond to shareholder inquiries.[24]

In its 2015 proposal to reform the transfer agent rules under the Securities Exchange Act of 1934, the Commission discussed in detail the role of transfer agents to mutual funds and the services they provide to mutual funds and mutual fund shareholders. After recognizing that the complexity of recordkeeping for mutual fund shares has increased significantly over the last several decades, that release notes:

> As a result, Mutual Fund Transfer Agents have made significant investments in technology advancements to manage more frequent and diverse transaction processing and shareholder communications through different channels. The industry also has relied heavily on the automation developed through [National Securities Clearing

[24] *See* Appendix A, *2021 Investment Company Fact Book* (ICI).

> Corporation] for processing and settling mutual fund transactions and exchanging and reconciling customer account information.[25]

Indeed, it is the systems of transfer agents – and not the systems of the fund or its adviser – that process shareholders' transactions and maintain shareholder records. If a mutual fund's shareholder records were breached or compromised, such breach or compromise *would occur on the transfer agent's systems and impact the information it holds and not that of the mutual fund or its investment adviser.* This being the case, if the Commission is interested, in part, in protecting mutual fund shareholders from the harm a cybersecurity event may cause to a shareholder or investor, transfer agents' systems must be in scope of the proposal.

While we recognize that the Commission's proposal includes provisions relating to an investment company's "service providers," any service providers regulated by the Commission should be expressly within the proposal's scope. Seeking to subject such firms to SEC regulation indirectly by the SEC requiring registered investment companies or their advisers that hire them to bring them within scope is not the appropriate or most effective way to achieve the Commission's goals.[26]

As proposed by the Commission, if a transfer agent suffers a cybersecurity incident based on its failure to have an information security program reasonably designed to protect the shareholder data it holds and the systems it uses, *it is the investment company or its investment adviser that would be in violation of the rules and <u>not</u> the transfer agent.* This seems wholly inappropriate and misplaced especially since it is the SEC that registers, regulates, examines, and can sanction transfer agents. It makes no sense that the Commission would not subject such registrants to direct regulation. Accordingly, we urge that the Commission's proposal be revised to bring transfer agents within its scope.

4. Revising Elements of Proposed Rule 38a-2 to Provide Flexibility and Consistency

There is much about the Commission's proposal that we support. We support the SEC requiring registrants to adopt, implement, and maintain cybersecurity risk management programs. We support the SEC adopting rules to define the structural elements of those programs consistent with the NIST framework. We support the Commission providing registrants the flexibility necessary to tailor their programs based on the registrant's business operations, including its complexity and attendant cybersecurity risks. We support requiring the regular review of such programs and reporting on them to a fund's board. We support ensuring the SEC receives notice of certain significant cyber events impacting a registrant. And we

---

[25] Transfer Agency Release at pp. 162-164.

[26] *See* Section 4.1.3.2 *et seq.* for our recommendations relating to the proposal's treatment of service providers.

support requiring registrants to maintain records relating to their programs. As is always the case, "the devil is in the detail."

As discussed in this section, we recommend that the Commission revise some of the proposed rules to provide registrants greater flexibility in designing and implementing their programs. This approach will also ensure that funds' and advisers' existing cybersecurity risk programs, including any that are governed by the Interagency Guidelines, are not disrupted or otherwise adversely impacted by adoption of the SEC's new rules.[27]

We additionally recommend that, in its adopting release, the Commission confirm that, subject to oversight by the fund's board, a fund may delegate to its adviser or another third party the responsibility for the fund's cybersecurity risk program – including drafting the required policies and procedures and establishing, implementing, and maintaining the fund's program. Enabling a fund to delegate these responsibilities seems consistent with the Commission's intent as expressed in the Release.[28] It would also be entirely consistent with the flexibility provided to funds in implementing the Mutual Fund Compliance Programs Rule, Rule 38a-1.

4.1 Changes Necessary to Various Components of the Proposed Cybersecurity Policies and Procedures

The Institute supports requiring registrants to have written policies governing their cybersecurity risk management programs. We concur that such policies and procedures "would help address operational and other risks that could harm advisory clients and fund investors or lead to the unauthorized access to or use of adviser or fund information."[29] We also support requiring registrants' policies and procedures to include provisions governing: conducting a risk assessment; user security and access; information protection; cybersecurity threat and vulnerability management; and cybersecurity incident response and recovery.[30]

---

[27] As noted in the Release, the Commission believes "that existing adviser and fund rules require certain cybersecurity practices to be substantially in place; consequently, the largest compliance costs resulting from the proposed policies and procedures requirements are likely to be borne by registrants not currently involving industry best practices." Release at p. 182.

[28] According to the Release, the "proposed cybersecurity risk management rules also would provide flexibility for the adviser and the fund to determine the person or group of people who implement and oversee the effectiveness of its cybersecurity policy and procedures." Release at p. 16.

[29] *Id.*

[30] These requirements appear consistent with those mandated by the Federal Information Security Management Act of 2022 (FISMA) (44 U.S.C. § 3541 *et seq.*), which governs the information security programs of the SEC and other federal agencies.

We are pleased that the Commission recognizes that, "given the number and varying characteristics (*e.g.,* size, business, and sophistication) of advisers and funds, firms need the ability to tailor their cybersecurity policies and procedures based on their individual facts and circumstances."[31] While the Commission intended to provide funds and advisers "flexibility to address the general elements [of the rule] based on the particular cybersecurity risks posed by each adviser's or fund's operations and business practices," some provisions of the rule should be revised to more effectively provide the intended flexibility.[32] To address this and provide registrants the necessary flexibility,[33] we recommend revisions to the proposed requirements as discussed below.

4.1.1 Risk Assessment Should Inform Implementation

The Institute supports requiring registrants to periodically assess the cybersecurity risks associated with fund information and systems. Such assessments should provide the foundation funds and advisers use to structure their cybersecurity risk programs. We recommend that the Commission, either in the rule itself or the adopting release, expressly recognize that the required risk assessment should govern and inform how registrants implement and maintain the other required elements for their cybersecurity risk programs. For example, because a fund's risk assessment should inform how it oversees its service providers, the oversight of service providers that present significant risk to the fund's information or information systems should be far more rigorous than it is for those service providers that present little, if any, cybersecurity risk.

4.1.2 User Security and Access Requirements Need to be More Flexible

The Institute has concerns with the provision in Section 38a-2(a)(2)(ii) that would govern the policies and procedures a fund or adviser would have to adopt to govern "user security and access." As proposed, the rule would require registrants to implement "authentication measures that require users to present a combination of two or more credentials for access verification."

We have two concerns with this provision in its current form. First, the phrase "two or more credentials" is problematic. It is not "credentials" that should govern access; it is "factors." By way of example, any person who has another's logon credentials – such as a username and password – may be able to access a system because the system uses these credentials to verify that the username and password are linked –

---

[31] Release at p. 17.

[32] *Id.*

[33] This flexibility will ensure that the Commission's requirements align with those of the Interagency Guidelines and avoid disruption of registrants' existing processes to address cybersecurity risks.

not to verify the identity of the person using these credentials. To verify that the person using these credentials has authority to access the system or information on the system, and to add an additional layer of security, *two-factor authentication* is necessary. With two-factor authentication, access to a system is only permitted if, after a person has signed onto a system using their username and password, such person verifies their identity by providing another crucial element of identification that only the authorized owner should have or know. Typically, this additional crucial element would be something the authorized owner knows (*e.g.,* a personal identification number (PIN)), something they have (*e.g.,* a token), or something intrinsic to them (*e.g.,* biometric information). This additional means of verifying a person's identity better protects systems from unauthorized access by a person using a stolen username and password (*i.e.,* two credentials).

Our second concern with requiring "two or more credentials" is that this is a static requirement based on today's technology. It is likely that, in the future, registrants will be able to secure their systems without the need to use multiple credentials (or multiple factors). Because, like many of the SEC's rules, this one can be expected to be in existence for decades to come, the user security and access requirements must be flexible enough to accommodate whatever technological security solutions the future holds.

To address these concerns, the Commission needs to revise proposed Rule 38a-2(a)(2)(ii) to read as follows:

> (ii) Adopting controls reasonably designed to authenticate authorized users and permit only authorized users to access fund information systems and fund information residing therein.

This revision, which is consistent with the provisions in the Interagency Guidelines that govern authentication controls, will enable registrants to evolve their user access and controls to stay current with evolving technologies.[34]

---

[34] We believe it is important for each of the elements in Rule 38a-2(a) to be flexible enough to enable registrants to evolve their policies, procedures, and practices to accommodate evolving technologies or best practices to address or mitigate cybersecurity threats and vulnerabilities. The user security and access element of the proposed rule would, in part, require registrants to establish procedures "for the timely distribution, replacement, and revocation or passwords or methods of authentication." This provision appears to provide registrants the flexibility they will need revise their password protocols as long-standing securities practices are found to be deficient. For example, securities experts used to advise rotating passwords frequently to avoid their compromise. Today, cybersecurity experts agree that, "Unless there is reason to believe a password has been compromised or shared, requiring regular password changes may actually do more harm than good in some cases." *See "Time to rethink mandatory password changes,"* FTC Blog (March 2, 2016), which is available at https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes.

4.1.3 Information Protection Requirements Are Sufficiently Flexible

Proposed Rule 38a-2(a)(3) would govern "information protection." It has two subsections: Subsection (i), which would govern internal access to information and information systems; and Subsection (ii), which would govern external access to a registrant's information or systems by service providers. Subsection (i) requires a registrant, in protecting its information, to take into account five factors: the sensitivity level and importance of the information to the registrant's business; whether any information is personal information; where and how information is accessed, stored, and transmitted; access controls and malware protection; and the potential impact on the registrant or its shareholders from a cybersecurity incident. We are pleased that, rather than taking a one-size-fits-all approach to information protection, the Commission has included these factors in this proposal because they will provide registrants the flexibility necessary to protect their information and systems differently based on a consideration of these factors. We support this provision.

4.1.3.1 Concerns with Monitoring Information in Transmission: Subsection 38a-2(a)(3)(i)

With respect to proposed Subsection 38a-2(a)(3)(i), the only provision in this subsection we recommend be revised is the provision in Paragraph (C), which would require a registrant to monitor "fund information in transmission." We understand that it is impossible to monitor data "in transmission." Accordingly, the phrase "including the monitoring of fund information in transmission" needs to be deleted from this provision.

4.1.3.2 Concerns with Breadth of Service Provider Oversight: Subsection 38a-2(a)(3)(ii)

Proposed Subsection 38a-2(3)(ii) would require registrants' policies and procedures to include provisions requiring the oversight of service providers that receive, maintain, or process a registrant's information or that have access to a registrant's information or information systems. We do not oppose the Commission requiring registrants to oversee those service providers that have access to a registrant's information or information systems. Indeed, in conducting due diligence of its service providers that will have access to their information or systems, registrants have long routinely included cybersecurity considerations.

While we support the Commission requiring registrants to have written policies and procedures that will govern their oversight of those service providers with access to fund information and fund systems, we recommend several revisions to the rule to:

- Align its requirements with the Commission's regulatory jurisdiction;

- Exclude certain service providers; and
- Require service providers covered by the rule to provide notice to a registrant whenever the service provider experiences a significant cybersecurity incident.

Each of these recommendations is discussed separately below.

4.1.3.3 Aligning the Rule with the Commission's Jurisdiction

Subsection 38a-2(a)(3)(ii) would require every registrant to require each of its service providers that has access to a registrant's information or information systems to execute a written contract in which the service provider agrees "to implement and maintain appropriate measures, including the practices described in paragraph (a)(1), (a)(2), (a)(3)(i), (a)(4), and (a)(5)" of Rule 38a-2. Through this requirement, the Commission appears to be attempting to wield its regulatory jurisdiction over persons that Congress has not authorized it to regulate. Exacerbating our concerns with this approach to regulation is the fact that it is a registrant that would be subject to enforcement sanctions *for a service provider's violation of the requirements of the rule.*
To our knowledge, the only contracts that Congress has authorized the Commission to regulate appear to be those between a fund and its adviser and underwriter, which are governed by Section 15 of the ICA. While the ICA imposes many restrictions on the activities of investment companies, the only provision addressing an investment company's *contracts* with any person, including any service provider, are those is Section 15.

Under the *expressio unius est exclusion alterius* maxim of statutory construction, the fact that Congress limited the Commission's regulatory jurisdiction over an investment company's contracts to those contracts between a fund and its adviser and underwriter would appear to indicate that the Commission lacks authority to regulate other contracts funds enter into with their service providers. And, because Section 38 of the ICA only authorizes the Commission to make and issue those rules "necessary or appropriate *to the exercise of the powers conferred upon the Commission,*" the Commission would not appear to have authority to regulate contracts beyond those with a fund's adviser or underwriter.

If Congress intended to grant the Commission the authority to regulate the terms of any contract involving a fund, such a provision would have been included in the ICA. Because it is not, the Commission's attempt to do so appears outside of its authority under Section 38 of the ICA and, therefore, wholly inappropriate. For these reasons we strongly oppose the Commission dictating the terms of a fund's contracts with any service providers other than with the fund's adviser or underwriter.

While we oppose the Commission imposing requirements on registrants' contracts with their service providers, we concur with the Commission's goal of ensure that registrants, "when considering whether to hire or retain service providers, [assess] whether they are capable of appropriately protecting important information and systems." This goal, however, can be accomplished in a far less burdensome and onerous way and in a way that is consistent with the Commission's regulatory authority. In particular, the Commission should revise the rule to require registrants, when retaining any service provider with access to the registrant's information or information systems, to ensure that such service provider implements and maintains appropriate measures that are designed to protect the registrant's information and information systems. Importantly, this approach would avoid disruption of how funds and advisers engage with service providers in the due diligence and oversight processes and ensure, consistent with current practices, that registrants document the cybersecurity considerations of their oversight process in their written policies and procedures.

Revising the provision in this way: avoids the Commission exerting its jurisdiction over persons it is not authorized to regulate; avoids the Commission dictating the contents of registrants' contracts with a significant range and variety of service providers; maintains the current ability registrants have to ensure their service providers are properly protecting their information and information systems; and preserves the ability of the Commission to sanction registrants that fail to appropriately oversee their service providers' protection of information or information systems in the event of a significant cybersecurity incident.

Accordingly, while we support the proposed rule requiring registrants to oversee their vendors with a view towards ensuring the protection of fund information and fund information systems, we strongly oppose the Commission's attempting to do so by attempting to indirectly regulate, through contractual provisions, persons that it lacks legal authority to regulate directly.

4.1.3.4 Excluding Certain Service Providers

As proposed, the provisions of Rule 38a-2(a)(3)(ii) relating to service providers would apply to all service providers with access to a registrant's information or information systems. The Commission has asked for comment on whether it should "require advisers and funds to assess the compliance of all service providers that receive, maintain, or process adviser or fund information" or that have access to fund information.[35] It has also sought comment on the challenges funds and advisers have, or may have, in obtaining information about their service providers' cybersecurity practices. We are pleased that the Commission has sought comment

[35] Release at p. 37.

on these issues as we believe consideration of them is a critical to ensuring that the rule is appropriately tailored to accomplish its intent and funds and advisers are able to maintain their operations without disruption once the rule is adopted.

As discussed in more detail below, we believe there are certain service providers that should not be considered "service providers" for purposes of the rule. These service providers fall into two categories: (1) those that have access to some fund information or fund systems but that, if compromised, would neither impact the ability of the fund or adviser to maintain critical operations nor jeopardize the confidentiality or security of fund information or information systems (*i.e.,* result in a "significant cybersecurity incident"); and (2) those whose cybersecurity practices are already subject to government oversight.

4.1.3.5 Service Providers Presenting Limited Risk

With respect to the first category of service providers, a fund should not be required to expend resources overseeing the cybersecurity practices of those service providers that, if breached, will neither impact the ability of the fund or adviser to maintain critical operations nor jeopardize the confidentiality or security of fund information or fund systems. Instead, consistent with the fund's or adviser's required risk assessment, the oversight required by the rule should be risk-based and focused on those service providers that present the greatest cybersecurity risks. Those service providers that present minimal risk to a fund or adviser should not be within scope of the rule's oversight requirements and funds should not have to expend precious resources overseeing them as required by the rule. Importantly, even if such service providers are excluded from the rule's scope (as they should be), they will remain subject to a fund's or adviser's due diligence and oversight as required by the Mutual Fund Compliance Program rule, Rules 38a-1 under the ICA. The only responsibility funds and advisers will be relieved of under our recommendation is compliance with the oversight requirements of Rule 38a-2(a)(3)(ii). To the extent the Commission finds a fund's or adviser's oversight of excluded service providers is deficient, the Commission would be able to sanction such deficiency under Rule 38a-1.

4.1.3.6 Service Providers Already Subject to Government Oversight

With respect to the second category of service providers, those whose information security practices are already subject to government oversight, excluding these service providers from the rules' scope will alleviate the challenges (and substantial costs) a registrant will have in trying to assess and oversee their practices as required by the rule. These challenges are not new; they have long existed. But they will be substantially exacerbated and complicated by a rule requiring funds and advisers to both assess such service providers' cybersecurity controls and require them to execute a contract with the fund or adviser in which they agree to establish,

implement, and maintain the information security policies and procedures required by Rule 38a-2.

Service providers subject to government oversight would include, for example, those financial institutions subject to the Interagency Guidelines. As noted above, these Guidelines were adopted in February 2001 by the Department of the Treasury, the Federal Reserve System, and other federal regulators of financial institutions. They were adopted to implement Section 501(b) of the Gramm-Leach-Bliley Act. Consistent with Section 501(b), they impose upon national and federal banks, among others, duties similar to those proposed in Rule 38a-2 – *i.e.,* a duty to: identify and evaluate the risks to their information; develop a plan to mitigate those risks; implement the plan; test the plan; update the plan when necessary; and require their service providers with access to an institution's information to take appropriate steps to protect the security and confidentiality of such information. Financial institutions' compliance with these requirements are subject to inspection by federal banking agencies and, if an institution is found to be deficient in their compliance, it may be subject to a regulatory action.

Pursuant to Section 17(f) of the ICA, registered investment companies are required to custody their assets with a bank, a member of a national securities exchange regulated by the Commission, or a registered company subject to rules and regulations of the Commission. Among these categories of custodians, only banks are not subject to the Commission's jurisdiction. Instead, they are subject to the jurisdiction of the federal banking regulators and such regulators' Interagency Guidelines. The information security protections provided by these Guidelines should obviate the need for SEC registrants to have to oversee the information security practices of any bank serving as a fund custodian.

Another type of service provider whose information security practices are subject to government oversight includes large multi-national companies that provide cloud-based services, such as Microsoft or Amazon Web Services (AWS). These companies have always been unwilling to enter into agreements authorizing any private or government entity (including the SEC) to prescribe how they operate their businesses or the cybersecurity controls they have in place. Nor do they provide any person detailed information about their controls. And yet, the federal government and its agencies are dependent upon the services provided by these companies. To address these companies' recalcitrancy about sharing the details of their information security programs, the federal government developed a rigorous process, the Federal Risk and Authorization Management Program (FedRAMP) process discussed below, to assess these companies' security practices and authorize their use by the federal government.

According to the General Services Administration of the U.S. Government (GSA), FedRAMP was established in 2011 "to provide a cost-effective, risk-based approach

for the adoption and use of cloud services by the federal government."[36] In order for federal agencies, including the SEC, to use a cloud service provider (*e.g.,* Microsoft or AWS), the service provider must be authorized by FedRAMP. "Getting FedRAMP authorization is serious business. The level of security required is mandated by law. There are 14 applicable laws and regulations, along with 19 standards and guidance documents. It is one of the most rigorous software-as-a-service certifications in the world."[37] Once a cloud service provider is authorized by FedRAMP to provide cloud services to U.S. government entities, it is listed in the FedRAMP Marketplace, which is a public data base of authorized cloud service providers.

Unless the SEC addresses the challenges presented by companies such as Microsoft and AWS, the proposed rule will make it especially difficult, perhaps impossible, for funds and advisers to fulfill their new regulatory responsibilities under the rule with respect to those service providers that have been vetted under the federal government's FedRAMP and are authorized to provide cloud services to it. Failing to permit SEC registrants to leverage the government's rigorous process for reviewing these companies' information security practices will present a terrible conundrum for those funds and advisers reliant upon them.

To avoid disrupting or impeding the relationships funds and advisers have with service providers whose cybersecurity practices are already subject to government oversight, the Commission must narrow the service providers within scope of the rule to exclude them. Failure to do so will result in severe disruptions to registrants' operations and impede their ability to continue to utilize necessary service providers to operate their businesses. In particular, the following service providers, at a minimum, should be outside the scope of the rule:

- **SEC Registrants** – Persons subject to the Commission's jurisdiction should have an independent obligation to establish, implement, and maintain a cybersecurity or information security risk program. It is inappropriate for the Commission to require one SEC registrant to verify that another registrant has a program in place that is compliant with the SEC's requirements. At a minimum, the Commission should exclude a fund's service providers under Rule 38a-1 (*i.e.,* a fund's adviser, transfer agent, principal underwriter, and administrator) as all such persons have an independent obligation under Rule 38a-1 to ensure they have compliance policies and procedures in place to ensure compliance with the federal securities laws, including their fiduciary duty to protect nonpublic information. We recommend, however, that *all* SEC registrants be excluded from the term "service provider" as used in Rule 38a-2.

---

[36] *See* https://www.fedramp.gov/program-basics/.

[37] *Id.*

- **Financial Institutions** – Financial institutions are subject to regulation under the Interagency Guidelines. As such, they are required to have information security programs that are substantively identical to those the Commission proposes under Rule 38a-2. Because federal banking regulators oversee institutions' implementation of the Guidelines' requirements, SEC registrants should not have an independent obligation to do so.

- **Regulated Industry Utilities** – Industry utilities such as the Depository Trust Clearing Corporation and its subsidiary, the National Securities Clearing Corporation (NSCC), should not be considered "service providers" for purposes of the rule. These utilities are regulated by the SEC and users of their services should not be required to oversee their cybersecurity risk programs.

- **Members of the NSCC** – In 2019, the SEC approved a change to the NSCC's rules to require all NSCC members and limited members to "have implemented a cybersecurity program designed from a recognized security framework so that such Member's SMART network and/or other connectivity is adequately protected against cybersecurity risks."[38] To evidence the member's compliance, as of January 12, 2021, the Control Office of each NSCC member has been required to digitally sign and submit to the NSCC a "Confirmation Form" at least once every two years. This being the case, it is redundant and unnecessary for SEC registrants to oversee the cybersecurity risk program of any NSCC Member that is compliant with this requirement.

- **Authorized FedRAMP Vendors** – Due to the rigorous nature of the FedRAMP process as discussed above, it is unnecessary for the SEC to require registrants to assess the cybersecurity practices of FedRAMP authorized cloud service providers. Therefore, service providers listed in the FedRAMP Marketplace should be excluded from the oversight required by the proposed rule.

To ensure that these services providers are outside the scope of the rule, Subsection (f) of the rule, Definitions, should be revised to define "service provider" and specify which service providers are outside of the definition's scope.[39]

---

[38] *See DTCC Important Notice Regarding Cybersecurity Confirmation* (July 20, 2020). *See, also, Self-Regulatory Organizations: National Securities Clearing Corporation; Order Approving a Proposed Rule Change to Require Confirmation of Cybersecurity Program,* SEC Release No. 34-87696 (December 9, 2019).

[39] *See* Section 4.7.3 of this letter, below, for the revision we recommend to Subsection (f).

4.1.3.7 Service Providers Should Provide Notice of Significant Cybersecurity Incidents

Rule 38a-2(a)(3)(ii) does not require service providers with access to a registrant's information or system to provide notice to a fund or adviser if the service provider experiences a significant cybersecurity incident that may impact the fund's information or information systems. Consistent with the requirements imposed on federal banking institutions (*e.g.,* through the Interagency Guidelines),[40] we believe those service providers within the rule's scope should have a duty to provide notice of significant cybersecurity incidents to a fund or adviser so it can take any steps necessary to protect its information and systems. We recommend that the Commission revise Rule 38a-2 to include such a requirement.[41]

4.1.3.8 Recommended Revisions to Rule 38a-2(a)(3) to Limit Scope of Service Provide Oversight Requirements

Based upon the above discussed concerns and consistent with the requirements imposed on federal banking institutions, in addition to adding a definition of "service provider" to Rule 38a-2(f), as set forth below under Section 4.7.3, we recommend that the Commission revise Rule 38a-2(a)(3) in relevant part to read as follows:

> (a)(3)(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 section,~~ that are designed to protect fund information and fund information systems. Such contract shall require the service provider to notify the fund by phone or email as soon as possible, but no later than 48 hours, after the service provider has a reasonable basis to conclude that a significant cybersecurity incident has occurred or is occurring that impacts the fund's information or information systems.

[40] *See, e.g.,* Rule 225.303 of 12 CFR Part 255, which governs Bank Service Provider Notification.

[41] Language to accomplish this is included in the amendment we propose in Section 4.7.3, below.

4.2 Clarifying Cybersecurity Threat and Vulnerability Management Provisions

Rule 38a-2(a)(4) would require funds' policies and procedures to include measures to detect, mitigate, and remediate "*any* cybersecurity threats and vulnerabilities" relating to fund information systems or the information they hold. [Emphasis added.] While the Institute supports including this provision in the rule, we recommend deleting "any" because the terms "cybersecurity threat" and "cybersecurity vulnerability" are comprehensively defined in subsection (f) of the rule. As a result, it is unnecessary to include "any" in this provision and we are concerned that its inclusion risks being read to mean a registrant's policies and procedures must address cybersecurity threats and vulnerabilities beyond those covered by these definitions.

4.3 Support for Cybersecurity Incident Response and Recovery Provisions

We support the Commission requiring registrants to detect, respond to, and recover from a cybersecurity incident and we believe the proposed elements a registrant's policies and procedures must include are appropriate. We have no additional comments on this provision.

4.4 Need to Clarify the Required Annual Review Process

Proposed Rule 38a-2(b) would require a fund to conduct an annual review of the design and effectiveness of its cybersecurity policies and procedures. We support including this requirement in the rule. We recommend, however, that with respect to a fund's review of its service providers (as required by Rule 38a-2(a)(3)(ii)), the Commission clarify that funds are not required to review each of their service providers' activities each year. Instead, in its policies and procedures under Rule 38a-2, a fund should be able to specify the frequency with which it will review its service providers' activities. This will provide funds the flexibility to determine an appropriate schedule for conducting oversight based on factors such as the significance of the service provider to the fund and the risks it presents. So, for example, funds may decide to review their critical vendors' activities annually and less-critical vendors' activities less frequently (*e.g.,* every other year or every third year). This approach to service provider oversight is consistent with the long-standing way in which funds and their advisers oversee their service providers under Rule 38a-1.[42]

[42] It is also consistent with the risk-based approach the SEC's Examinations staff uses to determine which registrants to examine and how often.

4.5 Board's Role in Overseeing the Program; Rules Need to be Flexible in Preparation of the Annual Written Report

Proposed Rule 38a-2(c) would require fund boards to approve a fund's cybersecurity policies and procedures.[43] This section of the rule also would require a fund to provide the board an annual written report regarding the fund's assessment of its cybersecurity policies and procedures. This report must include, at a minimum, a description of the fund's review conducted pursuant to Rule 38a-2(b) and any control tests performed. It must also: explain the results of the review, assessment, and tests; document any cybersecurity incidents that occurred since the date of the last report; and discuss any material changes to the fund's policies and procedures since the last report. The Institute supports the Commission including as part of a fund's cybersecurity risk management program board oversight,[44] including receipt of an annual written report containing the elements required by the rule.

The Commission seeks comment on whether the Commission should designate the persons who should be required to complete the annual review and prepare the annual written report. In our view, funds are in the best position to determine how to accomplish these tasks and the Commission should not mandate how they do so. Such a mandate would likely be quite burdensome to funds that are already struggling to allocate existing staff to implement the variety of new regulatory responsibilities being imposed on them.[45]

The Commission also seeks comment on whether funds should be required to have their cybersecurity policies and procedures audited by an independent third-party to assess their design and implementation. Due to the substantial costs this would impose upon funds and the lack of demonstrated need for or value of such audits, we strongly oppose requiring funds to incur this expense. We note that the Interagency Guidelines do not

---

[43] Consistent the requirement in Rule 38a-1 that fund's board approve a funds compliance policies and procedures, we appreciate the Commission clarifying that a fund's board "may satisfy its obligation to approve a fund's cybersecurity policies and procedures by reviewing summaries of those policies and procedures." Release at fn. 52.

[44] With respect to the board's approval of a fund's cybersecurity policies and procedures, we note that fund boards are not required to include cybersecurity experts and they should not be expected to pass on the sufficiency or adequacy of such policies and procedures. Instead, in keeping with the board's oversight role, the board's review should ensure that the fund's policies and procedures include all the elements required by Rule 38a-2.

[45] These regulatory responsibilities currently include, among others, implementing: the Liquidity Risk Management Program Rule, the Derivatives Rule, the Fund-of-Funds Rule, and the Valuation Rule. The Commission has also proposed rules, which remain pending, relating to money market fund reform, shortening the securities transaction settlement cycle (*i.e.,* T+1), private funds, beneficial ownership, proxy voting advice, security-based swaps, reporting of securities loans, regulation of alternative trading systems, short sales disclosure and reporting, and disclosure reform, among others.

require an independent third-party assessment of financial institutions' required cybersecurity policies and procedures.

4.6 Clarifying Prospective Application of Recordkeeping Requirements

Proposed Rule 38a-2(e) would require funds to maintain records relating to: their policies and procedures; annual written reports; annual review of the policies and procedures; any reports provided to the Commission; any cybersecurity incident (including document of the fund's response to and recovery from such incidents); and the risk assessment required by Rule 38a-2(a)(1). We recommend that, in lieu of requiring copies of reports provided to the Commission, the rule instead require a fund to maintain documentation of its communications with the Commission regarding those significant cybersecurity incidents it reported to the Commission.[46] The Commission also should clarify in the adopting release that the rules' recordkeeping requirements are prospective in application.

4.7 Recommended Revisions to the Rules' Definitions

The Commission has proposed to define the following terms in Rule 38a-2(f): cybersecurity incident, cybersecurity risk, cybersecurity threat, cybersecurity vulnerability, fund, fund information, fund information systems, personal information, and significant fund cybersecurity incident. We support adoption of the proposed definitions because they will appropriately complement and delineate the duties imposed on registrants' cybersecurity risk programs to ensure that funds take the steps necessary to analyze and protect their information and information systems from foreseeable cyber threats and vulnerabilities.

While we support adoption of these definitions, we recommend minor revisions to the definitions of "cybersecurity threat" and "significant fund cybersecurity incident" to better align them with the intent of the proposal. As discussed previously and as set forth below, we also recommend that the Commission add a definition of "service provider" to the rule to clarify that certain entities are outside the scope of the provisions in Rule 38a-2(a)(3)(ii) that require oversight of service providers.

4.7.1 "Cybersecurity Threat" Needs to be Revised to be Consistent with other Definition

As mentioned above, the proposal includes definitions of "cybersecurity incident," "cybersecurity risk," "cybersecurity threat," and "cybersecurity vulnerability." The definitions for "cybersecurity risk" and "cybersecurity vulnerability" clarify that they only include those risks and vulnerabilities that may result in a "cybersecurity incident." The same is not true for the definition of "cybersecurity threat." This term

[46] This recommendation corresponds to our recommendation in Section 7 of this letter that, in lieu of requiring registrants to use Form ADV-C to notify the Commission of significant cybersecurity events, such notice be provided by telephone, email, or similar means.

is defined to include "any potential occurrence" that could adversely affect the confidentiality, integrity, or availability of a fund's information or information systems. As such, this definition is incredibly broad and would reach conduct that may, but is unlikely, to impact fund information and fund systems. Consistent with the definitions of "cybersecurity risk" and "cybersecurity vulnerability," the Commission must narrow the definition of "cybersecurity threat" to only include those potential occurrences that may result in a "cybersecurity incident."

4.7.2 Definition of "Significant Fund Cybersecurity Incident" Should Not Include Degradation of Systems

The Commission has proposed to define the term "significant fund cybersecurity incident" to mean an incident or group of incidents that significantly: (1) disrupts or degrades a fund's ability to maintain critical operations; or (2) leads to the unauthorized access or use of fund information where such unauthorized access or use of such information results in substantial harm to the fund or to an investor whose information was accessed. The Institute commends the Commission for proposing a definition that is targeted at those cybersecurity incidents that imperil a fund's operations or puts in jeopardy the information it maintains.

We concur that the proposed definition will ensure that the Commission receives notice of those incidents of greatest concern to registrants, regulators, and potentially the financial markets, while filtering out the noise of cyber incidents that do not significantly impair fund operations, fund information, or fund systems. We recommend, however, that the Commission delete the phrase "or degrades" from the proposed definition. The purpose of reporting significant cybersecurity incidents to the Commission is to alert it to disruptions in critical operations or substantial harm to a fund or its investors. The fact that a registrant's systems may have been degraded due to a cybersecurity incident should not necessitate reporting to the Commission.[47] Unless and until the degradation results in the fund's inability to maintain critical operations or secure its data, it should not rise to the level of a "significant cybersecurity incident" that necessitates reporting to the Commission.

[47] For example, degradation of a registrant's systems may mean a slower response time for systems to respond to a command. This slower response time would not necessarily impair the registrant's ability to maintain business operations or impact the security of its information. As such, it should not warrant a report to the Commission. Should, however, such degradation become a "significant cybersecurity incident" that impact a member's ability to maintain business operations or its ability to secure its information, under our recommendation, the rule would still require notification to the Commission.

4.7.3 Definition of "Service Provider" Should be Added to the Rules

As discussed above, the Commission should exclude from the proposed Rule 38a-2(a)(3)(ii), which require registrants to oversee their service providers with access to fund information or fund systems, two categories of service providers – *i.e.,* SEC registrants and those service providers whose cyber hygiene is already subject to government oversight. Consistent with this recommendation, the Commission should add a definition of "service provider" to Rule 38a-2(f) along the lines of the following:

> *Service provider* means a third-party that receives, maintains, or processes fund information or that otherwise is permitted to access fund information systems and any fund information residing therein if a breach of such service provider's systems or data would disrupt the fund's or adviser's ability to maintain critical operations or compromise the security of fund information. The term does not include any: (i) SEC registrant; (ii) financial institution subject to the Financial Institutions Safeguards adopted under Section 501(b) of the Gramm-Leach-Bliley Act; (iii) industry utility regulated by the Commission such as the Depository Trust Clearing Corporation (DTCC) or its subsidiary the National Securities Clearing Corporation (NSCC); (iv) NSCC Member that has a current Cybersecurity Confirmation on file with the NSCC; and (v) any service provider listed in the FedRAMP Marketplace.

5. The Proposal's Revisions to Fund Registration Statements (Forms N-1A et al.)

The Commission has proposed to amend funds' registration forms to require a description of any significant fund cybersecurity incident that has occurred in its last two fiscal years.[48] This disclosure is intended to "provide investors a short history of cybersecurity incidents affecting the fund while not overburdening the fund with a longer disclosure period."[49] The Release seeks comment on whether such disclosure should be required and whether it would be helpful for shareholders and potential shareholders.[50]

---

[48] With respect to the proposed amendments to Form N-2, the registrant form for closed-end funds, we note that many such funds do not annually update their registration statements in reliance on SEC Rule 8b-16. As such, they may not be subject to the proposed prospectus disclosure requirements.

[49] Release at p. 66.

[50] On March 10, 2022, the Commission's Investor Advisory Committee held a meeting (the "IAC Meeting") that included a "Panel Discussion Regarding Cybersecurity." One of the presenters, Joshua Mitts, Associate Professor of Law at Columbia Law School, expressed the benefits of public disclosure of breaches, but his focus was solely on how such disclosure would avoid asymmetrical trading whereby insiders with knowledge

The Institute strongly opposes the Commission amending funds' registration forms to require a description of any significant fund cybersecurity incident. In support of this recommendation and as discussed in more detail below, we note that the proposed disclosure: is unnecessary for an investor considering an investment decision; would not serve any public purpose and, in fact, would be a road map for bad actors; and we are not aware of any other financial institution, commercial business, or government agency that is currently required to provide public disclosure of their significant cybersecurity incidents.[51]

5.1 The Proposed Disclosure is Unnecessary

According to the Release, disclosure of significant cybersecurity incidents "would improve the ability of shareholders and prospective shareholders to evaluate and understand relevant cybersecurity risks and incidents that a fund faces and their potential effect on the fund's operations."[52] In our view, adding this disclosure to a fund's prospectus is unnecessary to inform investors in light of other disclosure currently in fund prospectuses and will be of limited value, if any, to investors making an investment decision. Funds are already required to disclose their principal risks. As noted in the Release, "if a fund determines that a cybersecurity risk is a principal risk of investing in the fund, the fund should reflect this information in its prospectus."[53] Moreover, funds are "already required to update their prospectuses so that they do not contain an untrue statement of a material fact (or omit a material fact necessary to make the disclosure not misleading)."[54] To the extent cybersecurity events become a principal risk of investing in the fund, a fund would be required to update its prospectus to add this disclosure.

---

of a breach are able to benefit by trading prior to the public being informed of the breach. When asked about hackers who had knowledge of the breach being able to trade in advance of the public becoming aware of the breach, he said there would be no way to determine whether they are engaging in such conduct – the focus on his research was on corporate insiders. He never addressed the costs and harm to a firm that will result from bad actors being able to exploit public disclosure of the details of a registrant's cybersecurity incidents. In our view, these costs far outweigh any benefit resulting from preventing asymmetrical trading. *Cf.* comments of presenter Athanasia Karananou discussed in fn. 56, supra.

[51] We note, however, that subsequent to publishing the Release, the Commission proposed rules that, among other things, would require public companies to disclose material cybersecurity incidents. *See Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure,* SEC Release Nos. 33-11038, 34-94382, and IC-34529 (March 9, 2022). Comments on the proposal must be submitted by May 9, 2022.

[52] Release at p. 66.

[53] *Id.*

[54] Release at p. 67.

Prospectuses are not the only way investors would learn about significant cybersecurity incidents. As the Release notes, funds should already be disclosing significant cybersecurity events in their shareholder reports to the extent such incidents were a factor that materially affected the fund's performance over the past fiscal year.[55]

In other words, in the absence of adding the proposed disclosure to registration statements, once a significant cybersecurity incident becomes a principal risk of investing in the fund or materially affects fund performance, this disclosure is already required. As such, revising fund registration forms to add it as a separate disclosure element is unnecessary.

Further, this information will be of limited, if any, value or use to an investor making an investment decision.[56] We cannot see how the investor's investment decision will be aided by the disclosure the Commission is proposing; nor do we believe that an investor who has made a decision to invest in a particular fund will reconsider their decision based on the proposed disclosure. According to the Release:

> The markets for advisory services and funds present clients and investors with a complex, multi-dimensional, choice problem. In choosing an adviser or fund, clients and investors may consider investment strategy, ratings or commentaries, return histories, fee structures, risk exposures, reputations, etc. While we are not aware of any studies that examine the role perceptions of cybersecurity play in this choice problem, the extant academic literature suggests that *investors focus on salient, attention-grabbing information, such as past performance and commissions when making choices*.[57]

We concur with the lack of value this information will be to an investor making an investment decision.[58] By contrast, bad actors will be very interested in reading this

---

[55] *Id.*

[56] During the March 10, 2022 IAC meeting, one of the panelists, Athanasia Karananou, Director of Governance and Research, Principles for Responsible Investment, discussed her group's research on investors' expectations relating to cybersecurity disclosures. Importantly, according to their research, when it comes to cybersecurity, investors are interested in being informed regarding cybersecurity *governance*. There was no mention in her presentation of investors being interested in disclosure of cybersecurity incidents.

[57] Release at p. 104. [Emphasis added.]

[58] According to Institute research, when making an investment decision, almost 9 in 10 households indicated that fund fees and expenses were a very important consideration. Other information that shareholders are most interested in making their decisions includes: historical performance (94%); performance compared to an index (89%); and ratings from a rating service (76%). *See, What US Households Consider When They Select Mutual Funds, 2020,* ICI Research Perspective (Vol. 27, No.4, April 2021) at p.8.

disclosure.[59] Consistent with the Commission's interest in limiting the length of prospectuses and ensuring they focus on "key information that is particularly important for retail investors to assess and monitor their fund investments,"[60] we recommend that it avoid adding redundant and unnecessary disclosure to fund prospectuses and we vigorously oppose requiring disclosure of funds' significant cybersecurity incident.[61]

5.2 The Prospectus Disclosure Could be Harmful

The disclosure the Commission has proposed to add to mutual fund prospectuses regarding their significant cybersecurity events for the last two fiscal years would consist of: the entities affected by the incident; when the incidents were discovered and whether they are ongoing; whether any data was stolen, altered, or accessed or used for an unauthorized purpose; the effect of the incident on the fund's operations; and whether the fund or a service provider has remediated or is currently remediating the incident.

We are at a loss to understand what public purpose this disclosure would serve. In our view, the specificity that would be required to be included in this disclosure will be a very valuable road map for bad actors that have attempted to breach the fund's systems or may be planning to do so. For those bad actors who have already breached a fund's systems or information, the required disclosure will be a report card of sorts letting them know how successful their efforts were. The Release expressly acknowledges the harm that can result from this disclosure:

---

[59] As discussed below, we support the Commission maintaining the confidentiality of any information it receives relating to a fund's or adviser's "significant cybersecurity incidents" to avoid public disclosure of the very sensitive information included in the notice. We are concerned that, while the information in such notices would be confidential, the disclosure the Commission proposes to be included in fund registrant statements and adviser brochures would, in fact, result in public disclosure of such sensitive information.

[60] *See Tailored Shareholder Reports, Treatment of Annual Prospectus Updates for Existing Investors, and Improved Fee and Risk Disclosure for Mutual Funds and Exchange-Traded Funds; Fee Information in Investment Company Advertisements*, SEC Release Nos. 33-10814; 34-89478; IC-33963 (August 5, 2020).

[61] The proposal would also require funds to tag this information in a structured, machine-readable data language (*i.e.,* XBRL). Should the Commission revise fund registration statements, notwithstanding our opposition to such revisions, we oppose requiring funds to tag the proposed disclosure. According to the Release, such XBRL tagging will make "the disclosures more readily available and easily accessible for aggregation, comparison, filtering, and other analysis." [Release at p. 68.] We oppose such tagging because it will increase funds and shareholder costs. We note that tagging is currently only required for Items 2, 3, and 4 under Form N-1A and that is to enable fee comparisons among various funds. To the extent that a fund includes cybersecurity risk as a principal risk, this information would already be tagged. For all other cybersecurity disclosures, we cannot imagine investors needing this information to be tagged so they can compare disclosures among funds. This is because, as noted above, the disclosure would have limited value to an investor making an investment decision. In light of the fact that tagging is unnecessary, will increase fund and shareholder costs, and such costs are likely to exceed the benefits of tagging, we oppose it.

> Mandating disclosure about cybersecurity incidents entails a tradeoff. While disclosure can inform clients and investors, *disclosure can also inform cyber attackers that they have been detected.* Also, disclosing too much (*e.g.,* the types of systems that were affected, how they were compromised) *could be used by cybercriminals to better target their attacks,* imposing costs on registrants. For example, announcing a cybersecurity incident naming a specific piece of malware and the degree of compromise can imply a trove of details about the victim's computer systems, the security measures employed (or not employed), and *potentially suggest promising attack vectors for future attacks by other would-be hackers*.[62]

While we oppose public disclosure of this information for the reasons discussed above, we do not oppose the SEC being notified of significant cybersecurity incidents. We note that, in other contexts, the Commission has shown greater appreciation for the benefits of non-public reporting to the Commission only. For instance, if an open-end fund exceeds the 15 percent limit on illiquid securities or falls below its highly liquid investment minimum (HLIM) or a fund breaches its outer bound limit on fund leverage, it reports only to the Commission.[63] In adopting these requirements, the Commission found that it was neither necessary nor appropriate in the public interest or for the protection of investors to make this information publicly available.[64] And, in 2018, when the Commission changed course and decided to make *all* liquidity classification information on Form N-PORT non-public, it noted that public disclosure of this information could suffer from a lack of context and "inappropriately focus investors on one investing risk over others."[65]

---

[62] Release at pp. 106-107. [Emphasis added.]

[63] *See, generally,* Rule 30b1-10 under the ICA and Form N-LIQUID (now Form N-RN).

[64] *Investment Company Liquidity Risk Management Programs,* SEC Release Nos.33-10233 and IC-32315 (October 13, 2016) at p. 299. *See, also, Use of Derivatives by Registered Investment Companies and Business Development Companies,* SEC Release No. IC-34084 (November 2, 2020).

[65] *See Investment Company Liquidity Disclosure,* SEC Release No. IC-33142 (June 28, 2018) at p. 9. The Commission has similarly determined in several instances that certain disclosures not be public. *See, e.g.,* Instruction E to Form N-PORT (noting that several pieces of information on Form N-PORT will not be publicly disclosed, including: derivatives exposure; results from certain Value-at-Risk tests; country of risk and economic disclosure; delta for options; miscellaneous securities information; or explanatory notes related to any of these topics.

Because the proposed prospectus disclosure could be more harmful than beneficial, we vigorously oppose revising fund registration forms to include disclosure of significant cybersecurity incidents.[66]

5.3 Funds Alone Would be Subject to Public Disclosure of Cyber Events

We are not aware of any other financial institution, commercial entity, or government entity that is currently required by law to provide detailed disclosure to the public at large regarding the cyber events they have experienced or are experiencing.[67] While limited information about certain cyber events may wind up in the public domain,[68] the details regarding such events are not broadly shared or disclosed. These details remain confidential and outside the public domain deliberately. It is to avoid copycat breaches or intrusions. The omission of details is codified in state breach laws. Under such laws, persons impacted by a breach must receive notice of the breach, but the information provided about the nature, scope, and success of the breach is limited; it is not as extensive as what the Commission is proposing.[69] In our view, information regarding cyber events should *only* be shared only on a "needs-to-know" basis (*e.g.,* with the Commission) to avoid enlightening bad actors about the success of their breaches or encouraging copycat bad actors.[70]

---

[66] If the Commission disagrees and requires funds to disclose significant cybersecurity incidents, notwithstanding the considerable risks associated with such disclosure, we strongly urge that it remove the proposed detailed requirements about such incidents and permit funds to describe them more generally using their own discretion. Funds are in the best position to determine what information should be disclosed and how it should be disclosed to reduce the potential harm from such disclosure to the fund and its shareholders. In addition, given the limited importance of such information to investors, we also strongly urge the Commission to move such disclosure from the prospectus to the Statement of Additional Information.

[67] *See, however,* fn. 51, infra.

[68] *See, e.g.,* fn. 78, supra.

[69] We note that, in the absence of requirements under the federal securities laws to provide customers notice of a breach that may have impacted them, the Commission has sanctioned broker-dealers when, in the Commission's view, such notices violated the anti-fraud provisions of federal law. *See SEC Announces Three Actions Charging Deficient Cybersecurity Procedures,* SEC Press Release 2012-169 (August 21, 2021).

[70] Along these lines, members of the Institute have long been concerned with the fact that the Commission would have no duty to notify registrants when the Commission's systems are compromised and the persons compromising such systems have access to the vast amount of confidential information the Commission has received from registrants through examinations, investigations, or reporting requirements. In the absence of a duty, even though registrants would have a need to know about a breach of the Commission's systems, the SEC does not provide such information, which leaves registrants unaware of the need to take remedial steps to protect their systems and information.

For all of the above reasons, we strongly oppose the amendments proposed to registration forms.

6. Concomitant Concerns with the Proposal's Provisions Governing Investment Advisers' Cybersecurity Risk Management Programs

The Commission has proposed to adopt Rule 206(4)-9 "as a means reasonably designed to prevent fraud."[71] The rule would make it unlawful for an adviser to provide investment advice unless it "adopts and implements written policies and procedures that are reasonably designed to address the adviser's cybersecurity risks." The policies and procedures advisers must adopt and implement are identical to those funds must adopt under proposed Rule 38a-2. Advisers would also be required to: report to the Commission on Form ADV-C any significant cybersecurity incident; revise their brochures to include disclosure of (i) the adviser's cybersecurity risks that could materially affect its advisory services and (ii) certain cybersecurity incidents that have occurred within the last two fiscal years; and maintain records documenting their compliance with these requirements.

For the same reasons the Institute supports the adoption of Rule 38a-2, we support the Commission adopting rules to require investment advisers to adopt, implement, and maintain a cybersecurity risk program. We recommend, however, that the provisions within proposed Rule 206(4)-9 be revised as discussed under Section 6.1. We also strongly recommend that the Commission *not* adopt this rule under Section 204 of the Advisers Act. Instead, we recommend the Commission adopt a cybersecurity risk program rule for advisers under Section 211 of the Advisers Act.

Section 206 of the Advisers Act prohibits advisers from employing any device, scheme, or artifice to defraud any client or prospective client and from engaging in any transaction, practice, or course of business that operates as a fraud or deceit upon any client or prospective client. In other words, it prohibits *an adviser* from engaging in any fraudulent or deceitful conduct.[72] While Section 206 of the Advisers Act only authorizes the Commission to adopt rules defining fraudulent, deceitful, and manipulative conduct, Section 211 of the Act provides the Commission the authority "from time to time to make, issue, amend, and rescind such rules and regulations and such orders as are necessary or appropriate to the exercise of the functions and powers conferred upon the Commission" in the Advisers Act. We believe that Section 211 provides the Commission a more solid foundation from

---

[71] Release at fn. 21.

[72] Subsection 206(4) authorizes the Commission to adopt rules and regulations and "prescribe means reasonably designed to prevent, such acts, practices, and courses of business as are fraudulent, deceptive, or manipulative."

which to promulgate rules requiring advisers to have policies and procedures governing their conduct.

Consistent with Subsection 206(4), any rules the Commission adopts under Section 206 should address conduct *of advisers* that is fraudulent, deceptive, or manipulative. This section should not be used to prescribe salutary practices. Indeed, Subsection 206(4) does not appear to provide the Commission the authority to adopt rules that govern the day-to-day business operations of an adviser nor to impose new regulatory requirements on them. Adopting rules governing an adviser's cybersecurity risk program under Section 206 would mean that, any time an adviser's program is found to be deficient, the adviser could be cited for engaging in fraudulent, deceptive, or manipulative conduct.[73] And yet, but for the structure of the Commission's proposed rule, such deficiencies could not be deemed fraudulent, deceptive, or manipulative as those terms are commonly understood or as they have been construed by courts and the SEC under the federal securities laws. We are curious as to why, in the Commission's view, an adviser with a deficient cybersecurity risk program should be deemed to be engaging in fraudulent, deceptive, or manipulative conduct.

We also question why the Commission would choose to further victimize an adviser that is victimized by a cybersecurity incident by citing the adviser for fraudulent conduct under Rule 206(4)-9 following such incident based on a deficiency in their cybersecurity risk program. This seems unduly punitive in addition to being unnecessary. If the Commission were to require advisers to have cybersecurity policies and procedures under Section 211 of the Advisers Act, the Commission would be able to sanction an adviser if its policies and procedures were found to be deficient. The only thing the Commission would be unable to do under Section 211 versus Section 206 is to charge an adviser with fraud and publicly tout such enforcement proceeding as one in which the Commission sanctioned an adviser for fraudulent conduct. For these reasons, we strongly oppose the Commission adopting the proposed rules under Section 204 of the Advisers Act.[74]

6.1 Advisers' Cybersecurity Policies and Procedures Should by Substantially Similar to Funds' Policies and Procedures

As noted above, the requirements of proposed Rule 206(4)-9 are substantively identical to those of proposed Rule 38a-2. We concur with the Commission imposing

[73] Moreover, by the text of proposed Rule 206(4)-9, it would be unlawful for an adviser to continue to render investment advice for compensation while its cybersecurity risk program is deficient.

[74] We note that this recommendation is consistent with Commissioner Hester M. Peirce's *Statement on Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies* (Feb. 9. 2022), which we fully concur with and support.

identical requirements on both funds and their advisers with regards to their cybersecurity risk program's policies and procedures. Accordingly, we recommend the Commission make the same revisions to Rule 206(4)-9 that we recommend be made to Rule 38a-2 in Section 4.1 of this letter.

7. Support for Reporting Significant Cybersecurity Incidents but Not as Proposed on Form ADV-C

The Commission has proposed that registrants notify it no more than 48 hours after having a reasonable basis to conclude that a "significant cyber incident" has occurred at the adviser or at a fund the adviser advises.[75] Notification would occur by the adviser filing Form ADV-C with the IARD system.[76] Among other things, the Form ADV-C would require a registrant to disclose details of the incident and how it is being remediated. It would have to be filed initially within 48 hours of the incident and, until the incident is resolved, registrants would have to update the form whenever any information previously reported on it becomes materially inaccurate.[77] According to the Release, the reporting of significant cybersecurity incidents would help the Commission protect investors in connection with cybersecurity incidents, enable it to better understand such incidents, and help it assess potential systemic risks affecting financial markets more broadly.

The Institute appreciates the importance of the SEC being made aware of significant cybersecurity incidents impacting registrants and, for this reason, we support the

---

[75] The Release notes that an adviser must make the report "within 48 hours after having a reasonable basis to conclude that an incident has occurred or is occurring, and not after definitively concluding that an incident has occurred or is occurring. The 48-hour period would give an adviser time to confirm its preliminary analysis and prepare the report while providing the Commission timely notice about the incident." Release at pp. 50-51. Also, the Commission believes "that an adviser would generally gather relevant information and perform an initial analysis to assess whether to reasonably conclude that a cybersecurity incident has occurred or is occurring and follow its own internal communication and escalation protocols concerning such an incident before providing notification of any significant incident to the Commission." Release at fn. 65.

[76] For those internally managed funds that have no investment adviser, we recommend the Commission revise its proposal to permit the board of such fund board to designate an officer or officers who are responsible for providing notice to the Commission of significant cybersecurity incidents. This is the approach the Commission took in December 2020 when it adopted its rule governing Good Faith Determination of Fair Value. *See* Release No. IC-34128 (December 3, 2020).

[77] According to the Release, "While advisers and funds have other incentives to investigate and remediate significant cybersecurity incidents, [the Commission] believes these ongoing reporting obligations would further encourage advisers and funds to take the steps necessary to do so completely." Release at p. 51. We disagree with this statement and believes it belies the priority funds and their advisers place on cybersecurity. As noted previously, "a mutual fund's brand and success as a business are highly dependent upon investor confidence and cybersecurity attacks or incidents could easily and quickly erode or destroy such confidence." It is for this reason that funds and advisers have long taken seriously their cybersecurity risks.

Commission requiring registrants to provide the SEC notice of such incidents. We strongly oppose, however, adoption of Form ADV-C as the notification medium.

7.1 Concerns with Using Form ADV-C to Report Significant Cyber Incidents

We are pleased that the Commission seeks input on whether there are ways, other than by filing Form ADV-C, it should use for the reporting of significant cybersecurity incidents. While the Institute supports requiring registrants to notify the Commission of significant cyber incidents, we strongly oppose requiring the use of Form ADV-C or any paper or electronic form as the reporting medium.

We are concerned with the Commission requiring use of a form that contains highly sensitive information due to the potentially dire consequences to a registrant if the information on the form were compromised. While we support the Commission treating all information it receives about significant cybersecurity incidents confidential, we are concerned that if the SEC collects such information through required form filings and warehouses such forms on its systems, this database will be an attractive target for bad actors. We believe there are alternative methods that would be equally effective as Form ADV-C reporting but have the advantage of reducing certain risks, while meeting the needs of the Commission

Both the SolarWinds breach and the compromise of the SEC's EDGAR system, which was announced in September 2017 by SEC Chair Clayton,[78] evidence that even the SEC's systems are not immune from compromise. Also, as recently as October 2021, the SEC's Inspector General has found that "opportunities remain to improve the overall management of the SEC's IT investments, including by strengthening the agency's cybersecurity posture and continuing to mature its information security program."[79] Should there be current or future compromises of the Commission's systems or information, such compromises could result in unauthorized access to or exfiltration of information reported on Form ADV-C. A breach of this nature could result in substantial harm to the adviser or fund that was the subject of a significant cyber incident.

---

[78] Although Chair Clayton publicly announced the EDGAR breach in 2017, according to a civil compliant the SEC filed against the hackers, they were able to penetrate the EDGAR computer network on or about May 3, 2016 and they had unauthorized access to EDGAR files until at least October 2016 – *i.e.,* for over a year before the incident was publicly reported. Nine defendants and four relief defendants were the subject of the SEC's civil action. Four of the defendants were located in the Ukraine, four were in the Russian Federation, two were in Los Angeles, California, and the remaining defendants were in Hong Kong, Belize, and the Republic of Korea. *See U.S. Securities and Exchange Commission v. Oleksandr Ieremenko, et al.,* District of New Jersey, Civil Action No. 19-cv-505 (January 15, 2019).

[79] *See* SEC Inspector General Report at p. 7.

In addition, however, it seems counterintuitive to require a registrant whose systems have experienced a significant cyber incident to use its systems to make a report to the Commission about the incident. In a worst-case scenario, the bad actors who compromised the registrant's system may still be in those systems and, therefore, have access to the report. This would enable them to learn what the victim knows about the compromise and how it is being remediated, which could result in the bad actors altering how they are attacking the registrant's systems or the systems they are attacking. It may even enable the bad actors to destroy or alter the information reported of the form.

The SEC has proposed to have Form ADV-C filed with the IARD. We are pleased that the Commission seeks comment on whether the "IARD is the appropriate system for investment adviser to file Form ADV-C with the Commission."[80] We oppose the use of the IARD system as the repository for these filings. We note that, according to the IARD's website, "FINRA is the developer and operator of the IARD."[81] As such, it is not a proprietary system of the SEC and it is a system that persons other than the SEC have access to. This further exacerbates our concerns with the possible compromise or unauthorized access of such reports. To the extent the Commission requires the reporting of information, the information should be reported to the SEC directly and not through another entity. It also bears noting that the IARD system is not available 24-hours a day, seven days a week, and 365 days a year. As a result, when registrants need to make a report, it is possible that the system is unavailable due to a planned or unplanned outage.[82]

To avoid the potentially significant harm to registrants that may result from filing Form ADV-C with the SEC through the IARD or otherwise and to better ensure the confidentiality of the sensitive information in such reports, we strongly recommend that the Commission eliminate requiring registrants to use paper or electronic forms to report their significant cybersecurity incidents.

Instead, we recommend that the Commission require registrants to report significant cyber incidents "by email, telephone, or other similar methods"[83] that are

---

[80] Release at p. 59. The Release also seeks comment on whether the EDGAR system should be used for the filings. For the same reasons we oppose the use of the IARD as a filing repository, we oppose using EDGAR, which has previously been breached by hackers. .

[81] *See* https://www.iard.com/.

[82] *See* https://www.iard.com/availability for the IARD's planned outages. It seems possible that, in addition to these planned outages, compromises of the IARD could result in unplanned outages that might impact registrants' ability to use it to make required filings.

[83] We presume that such email could be sent via a secure personal email account to avoid use of the compromised system(s) to make the report. Similarly, if the fund's or adviser's telephone systems are

secure and that avoid electronic filings. This mode of reporting would be consistent with that used by the Department of the Treasury, the Federal Reserve System, and other Federal financial institution regulators.[84] In addition to enhancing the security and confidentiality of registrants' reports, this way of reporting would be more effective than a textual filing and would enable the Commission to establish a communication channel with the registrant under attack. This communication channel could remain open until such time as the incident is resolved and the Commission could require it to be used whenever information previously reported to the Commission becomes materially inaccurate. Discussing the registrant's incident with a Commission staff member is likely to be far more meaningful to the Commission and less burdensome to the registrant than a textual paper or electronic filing. Indeed, the Release notes that the Commission

> . . . believes it is likely that an adviser could regularly engage in a productive dialogue with applicable Commission staff after the reporting of an incident and the filing of any amendments to Form ADV-C, and, as part of that dialogue, could provide the Commission staff with any additional information necessary, depending on the fact and circumstances of the incident and the progress resolving it.[85]

We concur that providing the SEC notice of significant cybersecurity incidents could result in a productive dialogue between the registrant and the Commission's staff but we do not believe the filing of the Form ADV-C should be the catalyst for such dialogue. Instead, it could begin more efficiently and effectively when the registrant contacts the Commission through a secure phone line, email, or similar means to report the incident.

To ensure that the registrant has a record of its communication(s) with the Commission about the incident, the Commission could require the registrant to make and keep a written record of all of its communications with the SEC about the incident, including those taking place by phone or email.

---

computer based (*e.g.,* voice over Internet Protocols (VOIP)), we presume the call may come from a secure personal phone number to avoid use of the firm's compromised systems(s).

[84] *See, e.g.,* Subpart N, Section 225.302 of the Federal Reserve System Regulation Y.

[85] Release at p. 51. The SEC's Office of Technology Controls Programs within the Division of Examinations would be well-suited to receive registrants' reports of significant cybersecurity incidents. This Office currently administers the SEC's CyberWatch program, which is the primary intake point for information filed under Regulation SCI regarding systems events.

7.1.1 Tailoring the Information Reported to the Commission Following a Significant Cybersecurity Incident

As noted above we do not support filing proposed Form ADV-C but agree the proposed form contains the information that the Commission would be interested in receiving from a registrant that has experienced a significant cybersecurity incident. We concur that most of the information the Commission seeks would be relevant to the Commission's interest in understanding the incident, its impact on the registrant and investors, and whether it may present systemic risks that might affect the markets more broadly.

The Commission has sought comment on whether it should eliminate any of the items it has proposed to include in Form ADV-C.[86] There are three items of information included on Form ADV-C that we do not believe should be a part of the notice a registrant must provide to the Commission. These three are: Items 12, 15, and 16 relating to remediation, disclosure, and cybersecurity insurance, respectively.

7.1.2 Concerns with Reporting Remediation Efforts Under Item 12

Item 12 on Form ADV-C would require the registrant to disclose any "actions taken or planned to respond to and recover from the *significant cybersecurity* incident." [Emphasis in the form.] We recommend this disclosure be eliminated from the form for two reasons. First, it would require a registrant to disclose proprietary system information that would be of limited, if any, use to the Commission. Moreover, this could result in such lengthy, detailed, technical information that it would not further the Commission's interest in understanding the incident, its impact on the registrant and investors, and whether it may present systemic risks that might affect the markets more broadly. The information about the incident most relevant to understanding it would be the type of incident and its scope, not how the registrant is resolving or remediating it. Second, if compromised, this information will provide a road map for bad actors that would enable them to refine their attack methods after better understanding how the fund's systems were compromised and the steps the fund has taken to remediate such compromise. In the hands of a bad actor, this information could have a severe adverse impact on a fund's operations. For these reasons, we strongly recommend that Item 12 be eliminated from the information that must be disclosed to the Commission about the incident.

[86] While, as discussed above, we strongly oppose the SEC using Form ADV-C or any paper or electronic filing to report significant cyber incidents, except as discussed in this section, we do not oppose the Commission receiving the information that Form ADV-C would require about a significant cybersecurity incident.

7.1.3 Details of Public Disclosure of Incidents Under Item 15 Needs to be Narrowed

Item 15 on Form ADV-C asks whether disclosure has been made about the incident "to the adviser's clients or and/or to investors" in any fund the adviser advises. If the registrant responds "Yes," it must disclose when the disclosure was made. If it responds "No," it must explain "why such disclosure has not been made." We recommend that this Item be revised to only require disclosure: (1) made to any funds the adviser advises that may be impacted by the incident; and (2) made under state breach disclosure laws to any person impacted by the incident.

The Form seems to presume that anytime a registrant has a significant cybersecurity incident there must be public reporting of it. We disagree. We believe that, aside from reporting the incident to the Commission, reporting it to others should only occur in two instances. The first is if the incident impacts mutual funds or private funds the adviser advises. If so, the adviser should inform the funds of the incident so the fund can determine how it may impact its operations and their shareholders and take appropriate prophylactic action to address or mitigate such impact. The second instance is if non-public personal information of shareholders has been subject to unauthorized access, compromise, or exfiltration. If so, the states' breach laws would govern whether and how such shareholders must be notified of the breach. We recommend the Commission defer to the states' laws regarding whether such notice must be provided and, if so, their contents and timing. In both instances, the persons receiving the information have been, or may be, impacted by the incident so the notice would alert them to the incident so they can take prophylactic actions to address the incident's impact. Aside from these two instances, we see no value in requiring disclosure of the incident.

We therefore recommend that Item 15 be revised to read as follows;[87]

> 15) Has disclosure about the *significant cybersecurity incident* been made:
>
> a) To any investment company registered under the Investment Company Act of 1940 or to a company that has elected to be a business development company pursuant to section 54 of that Act, or to a *private fund* that has been or may be impacted by the incident?
> ☐ Yes -- if yes, when and to whom was disclosure made?
> ☐ No

[87] While recommending revisions to Form ADV-C, as discussed above, we are not advocating use of the Form for notifying the Commission of the incident. Instead, we are recommending that, when a significant cybersecurity incident is reported to the Commission by phone, email, or similar means, the report include this revised information.

b) To any person who, pursuant to a state's breach law, you were required to provide notice of a breach of such person's non-public personal information.
   ☐ Yes
   ☐ No

7.1.4 Eliminating the Proposed Disclosure of Cybersecurity Insurance Proposed in Item 16

The final question on the Form asks whether the incident is "covered under a cybersecurity insurance policy" maintained by the adviser or a fund the adviser advises. According to the Release, this information "would assist the Commission in understanding the potential effect that incident could have on an adviser's clients. This information would also be helpful in evaluating the adviser's response to the incident given that cybersecurity insurance may require an adviser to take certain actions during and after a cybersecurity incident."[88]

Cybersecurity insurance is an incredibly complex topic. We disagree that informing the Commission regarding whether the adviser has such insurance would render any meaningful information to the Commission consistent with the purpose behind requiring the reporting of significant cybersecurity events.

Insurance is a risk-management strategy – it is a way for the insured to transfer risk to another person, typically an insurance company. Accordingly, in assessing its risks and developing risk strategies, insurance is but one factor an adviser may consider. Other factors might include: the nature of the risk, the impact of the risk, other risk-mitigation or avoidance strategies in place, the costs associated with the risk, and the costs associated with mitigating or transferring the risks. In other words, the decision regarding whether to purchase cyber insurance and, if so, for what and in what amount, is a business decision to be made by an adviser based on its risk profile and an assessment of its needs. Without accessing an adviser's risk insurance policy – which we would strongly object to – the Commission will be at a loss to understand what insurance the adviser has, the scope of such coverage (including any exclusions), and how it may impact the adviser's response to or remediation of a significant cybersecurity incident.

By way of example, let us assume Target (the retail chain) was an adviser that was required to file Form ADV-C with the Commission after it experienced a significant data breach in 2013. At the time of the breach, Target had $90 million in cybersecurity insurance. As such, in response to Item 16 on Form ADV-C, Target would have answered "Yes" that it had cybersecurity insurance and "Yes" it had reported its breach to its insurance carrier. We

[88] Release at p. 58.

question what value these two "yes" responses would have been to the Commission in understanding the potential effect that incident could have on Target's customers or how it would assist the Commission in evaluating Target's response to the incident.

While Target had $90 million in cyber insurance, according to a March 2015 article about the breach, as of that date, the breach had cost Target at least $252 million. According to this article:

> You'd think that a behemoth retail chain like Target would have an insurance policy befitting its size, and before the 2013 data breach, its Cyber Insurance limits probably seemed high enough. But the figures for 2014's cleanup costs are in, and it looks like Target's policy only covered a fraction of its data breach expenses.
>
> Here is a rundown of Target's expenses, courtesy of a report by Advisen:
>
> - 2013: **$61 million** total; insurance covered **$44 million**.
> - 2014: **$191 million** total; insurance covered **$46 million**.
> - Total data breach expenses so far: **$252 million**.
> - Total covered by insurance so far: **$90 million**.
> - Total Target paid out of pocket: **$162 million**.
>
> * * *
>
> What's driving these costs? You may have heard that several banks are suing Target over the cost of replacing customer credit cards, but that's just the start of Target's money hemorrhage. Other costs stem from:
>
> - Investigating the breach.
> - Repairing security weaknesses.
> - Complying with breach notification requirements.
> - Offering credit-monitoring services for breached customers.
> - Hiring a legal defense team to respond to lawsuits.
> - Curbing reputational damage through PR measures and advertising.
>
> Target's Cyber Insurance can help cover these costs, but the policy's limits aren't high enough to bear the majority of the costs.[89]

We use this example to demonstrate that the complexity of issues relating to cybersecurity insurance should not be underestimated. Nor, as demonstrated by Target's experience, should the fact that an adviser has cybersecurity insurance be indicative of the potential

---

[89] *See Target's Cyber Liability Insurance Covered 36% of its Data Breach Costs. How Much Does Yours Cover?* Insureon Blog (March 24, 2015), which is available at: http://www.insureon.com/blog/post/2015/03/24/how-much-does-your-cyber-liability-insurance-cover.aspx.

effect the incident could have an adviser's clients, the adviser's response to the incident, its cybersecurity hygiene, or its ability to cover the costs associated with a significant cybersecurity incident, which is the Commission's purpose in collecting this information. Because of the lack of meaningful value that responses to Item 16 would provide to the Commission, we recommend this it be deleted from the reporting requirements.

8. Clarifying Prospective Application of Advisers' Recordkeeping Requirements

Consistent with proposed Rule 38a-2(e), the Commission has proposed to revise Rule 204-2, which governs an adviser's recordkeeping requirements, to require advisers to keep records of: their cybersecurity policies and procedures, the annual written report documenting the adviser's review of its policies and procedures; a copy of any notices filed with the SEC; documentation of any cybersecurity incidents; and records documenting the adviser's risk assessment. We support the Commission revising Rule 204-2 as proposed but, as with our comments on Rule 38a-1(e), we recommend that, in lieu of requiring records of any notices filed with the SEC (*i.e.,* Form ADV-C), the rule instead require advisers to maintain documentation of any communications they have with SEC staff regarding their significant cybersecurity incidents. We also recommend, as discussed in Section 4.6 of this letter, that the Commission clarify in the adopting release that these new recordkeeping requirements are prospective in application.

9. The Risks to an Adviser Resulting from the Proposed Brochure Rule Disclosure Would Outweigh Any Benefits to Investors

The Commission has proposed to revise the "Brochure Rule," Rule 204-3, to require disclosure of an adviser's cybersecurity risks and incidents. These disclosures would be included in an adviser's brochure by adding a new Item 20 to Part 2 of the Form ADV. Item 20.A. of Form ADV would require an adviser to "describe the *cybersecurity risks* that could materially affect the advisory services" the adviser offers. [Emphasis in original.] An adviser would also have to describe how it assesses, prioritizes, and addresses cybersecurity risks created by the nature and scope" of the adviser's business.

With respect to disclosure of "incidents," an adviser would have to provide a description of any cybersecurity incident that has occurred within the last two fiscal years that significantly disrupted or degraded the adviser's ability to maintain critical operations, or has led to the unauthorized access or use of adviser information, that resulted in harm to the adviser or its clients. This disclosure must include information substantially similar to that the Commission has proposed to require in investment company registration statements discussed above in Section 5 of this letter.

For all of the reasons discussed under Section 5 of this letter, the Institute strongly opposes the Commission requiring this disclosure. These reasons include that: this disclosure: is unnecessary; would serve no public purpose; and would be a valuable road map to bad actors. Additionally, as noted in Section 5, we are not aware of any other financial institution, commercial entity, or government entity that is required by law to provide detailed disclosure to the public at large regarding cybersecurity events they have experienced or are experiencing. Also, as noted in Section 5, to the extent an advisory client may be impacted by a breach of the adviser's information or information systems, state breach laws would require the adviser to provide such clients notice of the breach. We recommend the Commission not revise Form ADV to require disclosure of this information.

10. Lengthy Transition Period is Necessary Prior to Compliance Date

The Release is silent as to an anticipated compliance date after the Commission adopts rules mandating adoption, implementation, and maintenance of cybersecurity risk programs. The Institute recommends the Commission establish a compliance date 24 -36 months after the rules' adoption. We believe a lengthy period is warranted based on the complexity of the policies, procedures, and processes registrants will have to implement as part of their cybersecurity risk programs. Even for those registrants that already have mature programs in place, they will be required to ensure that such programs satisfy the rules' requirements relating to how they: conduct their risk assessments; address user security and access; protect their information; oversee their service providers; assess their cybersecurity threats and information; respond to and recover from cybersecurity incidents; and get their board's approval of their policies and procedures governing each of these processes.

Time will also be needed to develop a process for: conducting the annual review; preparing an annual written report; determining when a significant cybersecurity incident triggers reporting to the SEC; developing a process to report such incidents to the SEC; revising recordkeeping requirements to capture newly required records; and amending contracts with service providers. As previously noted, registrants will be allocating resources to accomplish all this while also devoting considerable resources to implement the panoply of new rules recently adopted or soon-to-be adopted by the SEC. We also note that there are no exigent circumstances that would appear to require a more immediate compliance date. Should such a circumstance arise with an individual registrant, the SEC's enforcement powers would provide it ample authority to take appropriate action to address the Commission's concerns with the registrant's ability to protect their systems or information.

11. Implementation Guidance Will be Necessary Due to Rules' Complexity

Should the Commission pursue adoption of final rules requiring funds and advisers to establish, implement, and maintain cybersecurity risk programs along the lines outlined in the Release, registrants have already expressed the need for guidance from the Commission in interpreting the new requirements to ensure that registrants implement them as the Commission intends. Accordingly, once rules are adopted, we strongly encourage the Commission to work closely with registrants – as it has done in connection with previous rulemakings – to understand challenges the new rules will present to registrants and consider issuing guidance as necessary to facilitate their compliance efforts.

12. Conclusion

The Institute and its members appreciate the opportunity to comment on the Commission's proposed cybersecurity risk program rules. If you have any questions or require further information regarding our comments, please do not hesitate to contact either the undersigned [redacted], Tamara Salmon, Associate General Counsel, ICI [redacted], or Peter Salmon, Senior Director, Technology & Cybersecurity, ICI [redacted].

Sincerely,

/s/

Susan M. Olson
General Counsel

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