INVESTMENT COMPANY INSTITUTE®

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

Susan M. Olson
GENERAL COUNSEL

202-326-5813
susan.olson@ici.org

May 22, 2023

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

Re: Reopening of Comment Period for Proposed Cybersecurity Risk Management Rule for Investment Companies and Investment Advisers
File No. S7-04-22

Dear Ms. Countryman:

The Investment Company Institute[1] appreciates the opportunity to provide its comments in response to the U.S. Securities and Exchange Commission reopening the comment period on the rule it proposed last year that would require registered investment companies and investment advisers to adopt and implement written cybersecurity risk programs.[2] The Commission is reopening the comment period "to allow interested person additional time to analyze the issues and prepare their comments in light of other regulatory developments in cybersecurity."[3] These other regulatory developments include the Commission's proposed cybersecurity risk

[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 $29.1 trillion in the United States, serving more than 100 million investors.

[2] *See Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies; Reopening of Comment Period,* SEC Release Nos. 33-11167; 34-97144; IA-6263; IC-34855 (March 15, 2023) (the "Release") (or the "2022 Release").

[3] Release at p. 1.

management rule for broker-dealers, transfer agents, and other covered entities[4] and revisions to Regulation S-P. [5]

Last year, the Institute filed detailed comments on the 2022 Release.[6] We were disappointed to see none of our recommended revisions nor similar recommendations from other public commenters reflected in the 2023 Release. In fact, with two exceptions, the 2023 Release is identical to the 2022 Release. We hoped that, in drafting a cybersecurity risk management program for various covered entities, the SEC would have addressed the concerns of commenters on the 2022 Release in the 2023 Release. In the open meeting at which the Commission considered this proposal, Commissioner Uyeda commented on the lack of consideration given to commenters' concerns with the 2022 Release when it drafted the 2023 proposal:

> If today's proposal provides a sense of déjà vu, perhaps it is because many of the requirements are substantially similar to the February 2022 proposal from the Division of Investment Management. I am perplexed as to why this proposal does not appear to react to the public comments received on the 2022 proposal.[7]

Because none of our concerns nor the similar concerns of others with the 2022 Release were addressed in the 2023 Release, we are filing this letter in response to the current republication to both repeat and supplement our comments on the 2022 Release. In particular, this letter: (1) again recommends that the Commission incorporate any cybersecurity risk management regulations into Regulation S-P rather than imposing these requirements through variety of discrete rules under the various securities acts (the Investment Company Act of 1940, the Investment Advisers Act of 1940, and the Securities Exchange Act of 1934); and (2) reaffirms our strong opposition to the Commission's proposed disclosure requirements – both public disclosure and confidential disclosure to the Commission – in the event of a significant cybersecurity events. While these two issues are the focus of this letter, because the 2023 Release for broker-dealers, transfer agents, and other covered entities includes none of our recommendations on the 2022 Release, we also incorporate and reiterate all recommendations from our 2022 Letter even if they are not explicitly restated in this letter.

---

[4] *See Cybersecurity Risk Management for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents,* SEC Release No. 34-97143; File No. S7-06-232 (March 15, 2023)(the "2023 Release").

[5] *See Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information,* Release Nos. 34-57427 and IA-2712, 73 FED. REG. 13692 (Mar. 13, 2008).

[6] *See* Letter from Susan M. Olson to Vanessa Countryman, Secretary, dated April 11, 2022 (the "Institute's 2022 Letter").

[7] *See Statement on the Proposed Cybersecurity Risk Management Rule for Market Entities,* Commissioner Mark T. Uyeda (March 15, 2023), available at https://www.sec.gov/news/statement/uyeda-statement-enhanced-cybersecurity-031523.

Executive Summary

Consistent with our comments on the 2022 Release, as well as our comments on the 2023 Release and the proposed revisions to Regulation S-P, we recommend that the Commission incorporate any cybersecurity risk management program requirements into Regulation S-P rather than adopting them as multiple stand-alone rules. We additionally recommend that the Commission rethink the provisions in the 2022 and 2023 Releases relating to the disclosures that must be made and the notices that must be filed with the SEC by any registrant that is the victim of a significant cybersecurity incident.

1. Broadening the Scope of Regulation S-P to Include Cybersecurity Requirements

The Institute opposes the Commission adopting the cybersecurity risk management program requirements as separate rules under the Investment Company Act, the Investment Advisers Act, and the Securities Exchange Act. Instead, as we noted in our previous comment letter, we strongly recommend that Regulation S-P be revised to include these provisions. This approach has several advantages over the SEC's proposed disparate approach. First, it acknowledges the interconnectedness of data safeguards, cybersecurity, and breach notices – which are all within the scope of Regulation S-P. Second, it will result in a more uniform and coherent framework (in a single regulation) and avoid a disjointed and disparate regulatory approach whereby there are similar, yet connected, rules in different places.[8] Third, it will be consistent with the related regulations of the Interagency Guidelines of the federal banking regulators. Because the SEC is currently considering significant amendments to Regulation S-P, this would seem an appropriate time to incorporate any requirements relating to cybersecurity risk management programs into that regulation.

[8] William Birdthistle, Director of the Division of Investment Management, recently commented on the connection between electronic records and the need to notify individuals when those records are compromised:

> For asset managers, . . advancement in digital communications, information storage tools, and other technologies have simplified the ability of firms to obtain, share, and maintain individuals' personal information. While this technological progress may offer certain benefits, this evolution also has changed – or perhaps even exacerbated – risks of unauthorized access to or use of personal information. The proposed amendments to Regulation S-P would respond to these threats by requiring registered investment advisers to adopt written policies and procedures for incident response programs that address unauthorized access to or use of customer information, and would require timely notification to individuals affected by an information security incident.

See Remarks at the ICI Investment Management Conference, William Birdthistle (March 20, 2023), available at https://www.sec.gov/news/speech/birdthistle-remarks-ici-investment-management-conference-032023.

1.1. Regulation S-P is the Appropriate Vehicle to Address Cybersecurity

Regulation S-P was originally adopted by the SEC in 2000 to implement Section 501 of the GLB Act enacted in 1999. Section 501 of the GLB Act provides as follows:

> SEC. 501. [15 U.S.C. 6801] **PROTECTION OF NONPUBLIC PERSONAL INFORMATION.**
> (a) PRIVACY OBLIGATION POLICY.—It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.
> (b) FINANCIAL INSTITUTIONS SAFEGUARDS.—In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards—
>
> (1) to insure the security and confidentiality of customer records and information;
> (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
> (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

Under the GLB Act, federal regulators of financial institutions, including the SEC,[9] were directed by Congress to work together, through joint rulemaking initiatives, to implement the Act to ensure the consistent protection of individual's NPPI without regard to what type of institution held such NPPI. In response to this directive, the SEC adopted Regulation S-P to require the safeguarding of NPPI. The federal banking regulators adopted Interagency Guidelines Establishing Standards for Safeguarding Customer Information to implement the GLB Act.[10]

Like Regulation S-P, when the Interagency Guidelines were adopted in 2001, their focus was on safeguarding NPPI.[11] Since then, however, unlike Regulation S-P, they have been amended to address other issues relating to data security, including cybersecurity protections and breach notices. In particular, in 2005, the Interagency Guidelines were revised to add Appendix A to require institutions to have cybersecurity response programs for unauthorized access to customer

[9] These regulators included, among others, the Board of Governors of the Federal Reserve System (the Federal Reserve), the Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (FDIC), and the Office of Thrift Supervision (OTS). *See* Section 505 of the GLB Act.

[10] 12 CFR Part 364, Appendix B(III) of the Interagency Guidelines Establishing Standards for Safeguarding Customer Information.

[11] *See* 66 FED. REG. 8816 (February 1, 2001).

information.[12] The cybersecurity risk management programs proposed by the Commission for investment companies and investment advisers last year and this year for broker-dealers and transfer agents are patterned after the Interagency Guidelines.

1.2 The Commission Should Address Data Security Issues Holistically

We believe the Interagency Guidelines' holistic approach to governing banking institutions' data safeguards, cybersecurity, and breach notices is preferable and superior to the multiple, separate rules approach the Commission has proposed to impose similar regulatory requirements. Under the SEC's construct, covered entities will have an obligation to safeguard information under Regulation S-P and, if that information is breached, Regulation S-P would require the covered entity to notify the individual of a compromise of the individual's NPPI. But, the rules governing how these covered entities are to maintain and protect the NPPI from a cyber intrusion will not be in Regulation S-P. Instead, to find those requirements, one must first identify the type of entity maintaining the NPPI. If it is an investment company, proposed Rule 38-2 under the Investment Company Act of 1940 would contain the new requirements. If it is an investment adviser, proposed Rules 204-6 and 206(4)-9 would govern the adviser's cyber information. If it is a broker-dealer or a transfer agent, proposed Rule 242.10 under the Securities Exchange Act would be the operative provision.[13]

The Commission's multiple-rule approach to addressing these issues was commented on during the Commission's March 15, 2023 open meeting at which the Commission proposed the current Release as well as amendments to Regulation S-P and republished last year's cybersecurity risk management program for investment companies and investment advisers. Commissioner Peirce observed:

> . . . let me make one comment that applies to all the rules before us today. The proposed expansion of Regulation SP is one of three cybersecurity and systems-protection proposals we are considering today. Regulation SP overlaps and intersects with each of the others, as well as with other existing and proposed regulations – *e.g.*, the cybersecurity rule for investment advisers, investment companies, and business development companies, and the recently proposed investment adviser outsourcing rule. The release does not try to hide these facts, and actually goes into considerable detail about the redundancies, but then it simply declares them appropriate given the different purposes, that they are 'largely consistent,' and probably not

[12] In 2021, the Guidelines were amended to require financial institutions to notify federal banking regulators of any "notification incident," which is defined similarly to how the SEC proposes to define a "significant cybersecurity incident." *See Computer-Security Incident Notification Requirement for Banking Organizations and Their Bank Service Providers,* 86 Fed. Reg. 66424 (November 23, 2021).

[13] If an investment company or investment adviser violates the proposed cybersecurity rule, they would be engaging in fraudulent activity. Identical violations by a broker-dealer or transfer agent under Rule 242.10 would not be considered fraud. There is no explanation for the difference.

> 'unreasonably costly.' Admittedly, rationalizing these overlapping requirements would be hard. To paraphrase John Kennedy when addressing another difficult challenge, the Commission should choose to harmonize and synthesize these rules not because it is easy, but because it is hard, because the goal will serve to organize and measure the best of our energies and skills, because the challenge is one that we are willing to accept, one we are unwilling to postpone.[14]

At the meeting, Commissioner Mark T. Uyeda, too, identified concerns with conflicts and confusion resulting from multiple regulations:

> In addition, today we are considering two other proposals that overlap with this proposal [*i.e.*, the proposed cybersecurity management program rule for broker-dealers and other market entities]: amendments to Regulation SCI and Regulation S-P. Regulation S-P would require policies and procedures to address certain types of cybersecurity risks. . . . [It] would similarly require notifications sent to customers and others about cybersecurity incidents.
>
> Make no mistake about it: cybersecurity is an incredibly important topic and the potential for harm to market participants and investors is significant, and to the markets and economy as a whole. It is crucial that there is a clear regulatory framework to address cybersecurity. The Commission's 'spaghetti on the wall' approach with these overlapping and potentially inconsistent regulatory regimes can create confusion and conflicts, and could even weaken cybersecurity protections. While the proposals acknowledge the possibility of potential overlap, they fail to address those concerns and simply ask commenters to specifically identify areas of duplication and costs. A preferable approach would have been to propose a set of coordinated rules and to consider those costs and benefits both individually and as a package.[15]

We concur with the views of Commissioners Peirce and Uyeda and recommend that, consistent with the tested approach taken by the federal banking regulators in the well-established

---

[14] *See Statement on Regulation SP: Privacy of Consumer Financial Information and Safeguarding Customer Information*, Commissioner Hester M. Peirce (March 15, 2022), available at https://www.sec.gov/news/statement/peirce-statement-regulation-sp-031523.

[15] *See Statement on the Proposed Cybersecurity Risk Management Rule for Market Entities*, Commissioner Mark T. Uyeda (March 15, 2023). Because the SEC has elected to propose separate rules to address these issues, in addition to filing this comment letter, the Institute is filing comment letters on the proposed amendments to Regulation S-P and on the SEC's republication of the proposed cybersecurity rule for investment companies and investment advisers. As with this letter, in each of those letters, ICI will include commentary expressing concern with the Commission's proposed disjointed and fragmented approach to address the safeguarding of individual's NPPI, the proper disposal of NPPI, breach notices, and cybersecurity risk management programs. Those letters, too, will recommend that the Commission harmonize all these requirements into Regulation S-P.

Interagency Guidelines, the Commission address these issues holistically in one regulation – Regulation S-P.

1.3 The Advantages of the Interagency Guidelines' Holistic Approach

As stated above, we very much prefer the holistic approach of the Interagency Guidelines to the SEC's proposed approach of adopting a variety of rules under the various securities laws to impose substantially similar requirements. Aside from the logic of combining related provisions in one regulation, another advantage of the holistic approach is that the requirements will apply uniformly. As proposed by the Commission, while all covered institutions will be subject to the same regulatory requirements applicable to safeguarding customer information, providing breach notices, and disposing of NPPI, the SEC has proposed disparate rules for different SEC registrants as it implements new cybersecurity requirements. For example, if a fund were to violate the proposed cybersecurity program rule (Rule 38a-2), it would be deemed to be engaging in fraud. The same would not be true of a broker-dealer or transfer agent that violates their proposed cybersecurity program rule (Rule 242.10). This disparity in treatment is puzzling, unnecessary and serves no public purpose. It can be avoided by incorporating any provisions addressing covered entities' cybersecurity risk management programs into Regulation S-P, where they could be applied consistently to all covered entities.

1.4 The Advantages of Addressing Data Security Holistically

We appreciate that the Commission is seeking to address complicated issues through the Regulation S-P and cybersecurity risk management program proposals, and we commend it for addressing these issues. We strongly recommend, however, that the SEC rethink its disparate approach to protecting individuals' information and instead, like the Interagency Guidelines, protect such information holistically and more uniformly in Regulation S-P. Such an approach would ensure that:

(i) SEC covered entities' responsibilities would not be dependent upon how the covered entity is registered with the SEC;
(ii) All provisions relating to protection of customer information – whether in paper or electronic form – including its disposal and breach notices would be easily found in one regulation. This would obviate the need for covered entities to review a variety of rules under the Investment Company Act, the Investment Advisers Act, and the Securities Exchange Act to determine the applicable law; and
(iii) A violation of the Regulation would be sanctioned the same for all covered entities based on the facts and circumstances of the violation and not as fraudulent conduct if the violator is an investment company or investment adviser and as non-fraudulent conduct if the violator is a broker-dealer or transfer agent.

Also, a holistic approach should facilitate both registrants' compliance with these requirements and the Commission's efforts to consistently enforce these requirements. Customers and investors also would be better served by a more coherent and less confusing regime.

Our recommendation is consistent with our April 2022 comments on the SEC's proposed cybersecurity risk management program rule. That letter recommended that the Commission address cybersecurity risks in Regulation S-P and noted that, among other advantages of this approach, it would subject all registrants to a uniform set of cybersecurity regulations. We were disappointed to find that, while the Commission proposed amendments to Regulation S-P at the same time as it published the Release, the proposed amendments to Regulation S-P did not reflect any recommendations in our 2022 Letter relating to cybersecurity management programs.

2. Disclosure of Cybersecurity Risks and Incidents

The Commission's proposed cybersecurity risk management rules would require registrants to publicly disclose cybersecurity risks and to disclose to the Commission significant cybersecurity incidents. For the reasons discussed below, the Institute continues to strongly oppose public disclosure of a covered entity's cybersecurity risks. While we support covered entities alerting the Commission of significant cybersecurity incidents, we strongly oppose the method proposed for this disclosure. Each of these recommendations was discussed in detail in the Institute's 2022 Letter. In this letter, we supplement those comments in light of the 2023 Release.

2.1 Disclosure of Cybersecurity Risks

According to the 2022 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."[16] As we noted in the Institute's 2022 Letter, 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. In the 2022 Release, the Commission, too, questioned the usefulness of such disclosure:

> 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.[17]

[16] Release at p. 66.

[17] Release at p. 104.

We continue to question the value of this information to an investor making an investment decision.[18] By contrast, bad actors will be very interested in reading this disclosure.[19]

2.2 The Public Disclosure Could be Harmful

As with the comments in the Institute's 2022 Letter, we noted in our comments on the 2023 Release that harm could flow from the amount of information covered entities would be required to disclose publicly about their significant cybersecurity incidents. Our 2022 letter described in detail our serious concerns with the proposed disclosure.

Regardless of the form this public disclosure takes – whether in a prospectus, Form ADV, proposed Form SCIR, through website disclosure, or otherwise – we continue to vigorously oppose requiring registrants to publicly disclose their significant cybersecurity incidents due to the harm that may result to the registrant. Such disclosure will be of the greatest interest and benefit to bad actors – indeed it will be a treasure trove of information for them.[20] As such, its potential harm will surely exceed any benefit the Commission believes this information will provide to the public.[21]

2.3 Reporting Significant Cyber Incidents to the Commission

The Institute continues to oppose the Commission requiring use of any form to report to the Commission any significant cybersecurity incidents. This is because any such form would contain highly sensitive information, and if the SEC collects such information

---

[18] 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 include: 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.

[19] As discussed below, we support the Commission maintaining the confidentiality of any information it receives relating to a funds 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.

[20] Likely the federal banking regulators are aware of the harm that would flow from putting similar information relating to banking institutions in the public domain, which is why such institutions are not required to publicly disclose this information. The Commission should have similar concerns with its publication.

[21] 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.

through required form filings (*e.g.*, Form ADV-C or Form SCIR) and warehouses such forms on its systems, this database will be an attractive target for bad actors. As noted in the Institute's 2022 and 2023 Letters, there are alternative methods of reporting that have the advantage of reducing certain risks, while meeting the needs of the Commission. Our comment letter on the 2023 proposal and the Regulation S-P amendments also detail our significant concerns with the Commission warehousing any of this information due to the SEC's ineffective information security, which has been consistently documented by auditors, including the SEC's Inspector General. Our comments also questioned requiring a registrant whose systems have experienced a significant cyber incident to use those very same 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 on the form.[22]

In lieu of this proposed reporting, we continue to recommend that the Commission require registrants to report significant cyber incidents "by email, telephone, or other similar methods"[23] that 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.[24] 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. Indeed, providing the SEC notice of significant cybersecurity incidents in this manner could result in a productive dialogue between the registrant and the Commission's staff. 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.

2.3.1 The Disclosure Would Serve No Public Purpose

On March 10, 2022, the Commission's Investor Advisory Committee held a meeting that included a "Panel Discussion Regarding Cybersecurity." One of the panelists leading the

---

[22] The Institute's comment letter on the SEC's *Cybersecurity Risk Management for Broker-Dealers et al.*, Release No. 34-97143 (March 15, 2023) discusses in detail the advantages to the SEC and to registrants of the SEC aligning its notice requirements with those of the Interagency Guidelines.

[23] We presume that such email could be sent via a secure 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 computer based (*e.g.*, voice over Internet Protocols (VOIP)), we presume the call would come from a secure phone number to avoid use of the firm's compromised systems(s).

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

Committee's discussion – from an investor advocacy perspective – was Athanasia Karananou, Director of Governance and Research, Principles for Responsible Investment. Ms. Karananou discussed her organization's research on investors' expectations relating to cybersecurity disclosures. Significantly, according to this research, when it comes to cybersecurity information, investors are most interested in being informed regarding cybersecurity governance – not disclosure of cybersecurity incidents. Accordingly, we recommend that, in lieu of requiring disclosure of a covered entity's cybersecurity risks and descriptions of its significant cybersecurity incidents, the Commission instead require covered entities to disclose on their websites or otherwise, their governance approach to addressing their cybersecurity risks.

In other words, the Commission's Investor Advisory Committee heard from an expert that investors do not appear to be interested in the cybersecurity information that the Commission would require to be disclosed. Neither the 2022 nor 2033 Releases cite any evidence to support this required disclosure.

2.3.2 The Disclosures Would be Very Meaningful to Bad Actors

While research shows that investors are not seeking disclosure of cybersecurity incidents, bad actors will, undoubtedly, be very interested in and benefit from the required disclosure to the detriment of the victims of these incidents.

We think the Commission has underestimated the sophistication of bad actors and their ability to render great harm from limited information. We are highly concerned that the proposed disclosure could facilitate more harm by bad actors. As noted by one cyber expert, "Anything in the public domain [about a cybersecurity incident] creates a growing body of knowledge about you as an organization, who your players are, the technologies you're using, even how to respond. All that allows someone to attack you better."[25] The Institute therefore strongly opposes any public disclosure of this information.

3. Concerns with Using EDGAR as the Filing Portal and Repository

As noted above, the Commission's 2023 cybersecurity proposal would require filings related to significant cybersecurity incidents. This information would be reported to the SEC via Form SCIR, which would be filed with the Commission through the EDGAR system. Our 2022 Letter detailed our serious concerns with using the Investment Adviser Registration Depository (IARD) to notify the Commission via proposed Form ADV-C of significant cybersecurity incidents of registered investment companies and investment advisers. Our concerns with using EDGAR for covered entities' filings are heightened. In our comment letter on the 2023 Release, we urged the Commission not to use EDGAR for these purposes. Our concerns relate to the ineffectiveness and the inadequacies of the Commission's information security controls, which are discussed in detail in our

[25] *See "A Data Breach is Bad But Disclosing Too Much Could be Worse,"* Adam Stone (October 16, 2022).

comment letter on the 2023 Release. We incorporate those comments herein rather than repeat them.

4. The SEC Should Avoid Duplicative Reporting of Cyber Incidents

Though mentioned in the Institute's letter on the 2023 Release, but not in our letter on the 2022 Release, we recommend that any cybersecurity rules the Commission adopts provide an express exemption from the rules' notice requirements if the covered entity has reported the significant cybersecurity incident to another federal agency. For example, SEC registrants have long been required by the Bank Secrecy Act (BSA) to file Suspicious activity Reports (SARs) with the Financial Crimes Enforcement Network (FinCEN) to report cyber-enabled crimes and cyber events. SARs filed on cyber events must include all relevant and available information regarding the suspicious transactions and the cyber event, including its type, magnitude, and methodology as well as signatures and facts on a network or system that indicate a cyber event.

Aside from these required reports, private sector entities experiencing cyber incidents are encouraged to report a cyber incident to the local field office of federal law enforcement agencies including the Federal Bureau of Investigation,[26] the National Cyber Investigative Joint Task Force, the U.S. Secret Service, the U.S. Immigration and Customs Enforcement/Homeland Security Investigations, the U.S. Postal Inspection Service, the Bureau of Alcohol, Tobacco, Firearms, and Explosives, and the National Cybercrime and Communications Integration Center. Unlike the SEC, each of these agencies is in the business of identifying, and bringing action against bad actors. As such, they are experienced in dealing with cybersecurity incidents, conducting cyber investigations, and bringing to justice the persons who perpetrate cyber crimes. This being the case, in the event a covered entity is working with a federal law enforcement agency on a cyber incident, it should not additionally be required to report the incident to the Commission. Nor should the SEC get involved in a registrant's engagement with a law enforcement agency investigating a cyber security incident.

In addition, the federal Cybersecurity and Infrastructure Security Agency (CISA) is currently in the process of gathering information and receiving input to assist it in implementing the Cyber Incident Reporting for Critical Infrastructure Act of 2002 (CIRCIA). CIRCIA's implementation will include provisions relating to the reporting of cyber incidents to CISA. According to CISA:

> Enactment of CIRCIA marks an important milestone in improving America's cybersecurity by, among other things, requiring CISA to develop and implement regulations requiring covered entities to report covered

[26] The Institute maintains relationships with the FBI and has undertaken initiatives to introduce our members to personnel in their local FBI field office so, in the event of a cyber incident, the member is not "cold calling" the FBI but, instead, connecting with an agent with whom they have a relationship.

> cyber incidents and ransom payments to CISA. These reports will allow CISA, in conjunction with other federal partners, to rapidly deploy resources and render assistance to victims suffering attacks, analyze incoming reporting across sectors to spot trends and understand how malicious cyber actors are perpetrating their attacks, and quickly share that information with network defenders to warn other potential victims.[27]

Reporting cyber incidents to CISA has several advantages over reporting to the SEC:

- CISA has "highly trained investigators who specialize in responding to cyber incidents for the express purpose of disrupting threat actors who caused the incident;"[28]

- CISA is able to provide "technical assistance to protect assets, mitigate vulnerabilities, and offer on-scene response personnel to aid in incident recovery;"[29]

- CISA works with its federal partners to "share information about indicators of compromise, tactics, techniques, procedures, and best practices to reduce the risk of a cyber incident propagating within and across sectors;"[30] and

- CISA's involvement with cyber incidents extends well beyond those in the financial service sector that would impact SEC registrants.

Once CISA adopts rules providing for the reporting to it of cyber incidents, we believe such reporting should trump and replace any reporting requirements the SEC adopts under the federal securities laws other than the registrant perhaps simply notifying the Commission of the fact that it is working with CISA on the incident. Otherwise, SEC registrants will be required to make duplicative reports and, unlike the reports to CISA, those filed with the SEC will have no residual benefits for registrants or investors as the SEC does not have CISA's mission, experience, or resources to "rapidly deploy resources and render assistance to victims suffering attacks, analyze incoming reporting across sectors to spot trends and understand how malicious cyber actors are perpetrating their attacks."[31]

---

[27] *See Department of Homeland Security Cyber Incident Reporting for Critical Infrastructure Act of 2022 Listening Sessions*, 87 Fed Reg. 55830 (September 12, 2022).

[28] *Ibid.*

[29] *Ibid.*

[30] *Ibid.*

[31] *Ibid.*

In summary, we recommend that any cybersecurity rules adopted by the Commission that require a registrant to notify the Commission of a significant cybersecurity incident should include an exclusion along the lines of the following:

> (3) (a) *Exclusion from the notification and reporting requirements.* The notification requirements of this rule shall not apply to any covered entity that has either:
> (i) Filed a Suspicious Activity Report (SAR) with the Financial Crimes Enforcement Network (FinCEN) under the Bank Secrecy Act to report the significant cybersecurity incident;
> (ii) Reported the incident to a federal agency charged with providing assistance to financial services firms that have been the subject of a cyber incident involving unauthorized access; or
> (iii) Reported the incident to the Cybersecurity and Infrastructure Security Agency pursuant to its rules for reporting cyber incidents.
>
> (b) In the event a covered institution is excluded from filing a notice under this exclusion, it shall by phone, email, or other similar method, inform the Commission of its reliance on this exclusion.

5. A Meaningful and Adequate Transition Period is Necessary Prior to Compliance Date

Finally, we would like to reiterate the need for an adequate compliance date once the rules are adopted. The Institute recommends the Commission establish a compliance date 24-36 months after the rules' adoption. We believe such a period is warranted based on the complexity of the policies, procedures, and processes covered entities will have to implement and test as part of their cybersecurity risk programs. Even for those covered entities that have mature programs in place, they will be required to ensure that such programs satisfy the rules' specific 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; and respond to, and recover from, cybersecurity incidents.

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; amending contracts with service providers; and engaging with boards and others on these issues. All of this will have to take place while covered entities are allocating considerable resources to implement the panoply of new rules recently adopted or soon-to-be adopted by the SEC. There are no exigent circumstances that would appear to require a more immediate compliance date. The recommended compliance period will support a more orderly and effective implementation of any new requirements. In the meantime, the

SEC still has sufficient inspection and enforcement authority to enable it to take action in the event a significant cybersecurity incident arises with an individual covered entity.

Most importantly, however, to the extent any cybersecurity rules adopted by the Commission require reporting of any significant cybersecurity incident, we urge the Commission to delay the effectiveness of that portion of such rules until such time as the Commission has demonstrated to auditors that it has effective data security and system security protections in place.

6. Conclusion

The Institute and its members appreciate the opportunity to both reiterate and supplement the comments in the Institute's 2022 Letter, including our concerns with the ability of the Commission to hold confidential the very sensitive information the Commission will receive through the proposed notice requirements. If you have any questions or require further information regarding our comments, please do not hesitate to contact either the undersigned (solson@ici.org), Tamara Salmon, Associate General Counsel, ICI (tamara@ici.org), or Peter Salmon, Senior Director, Technology & Cybersecurity, ICI (salmon@ici.org).

Sincerely,

/s/

Susan M. Olson
General Counsel

cc: Gary Gensler, Chair, Securities and Exchange Commission
Hester M. Peirce, Commissioner, Securities and Exchange Commission
Caroline A. Crenshaw, Commissioner, Securities and Exchange Commission
Mark T. Uyeda, Commissioner, Securities and Exchange Commission
Jaime Lizárraga, Commissioner, Securities and Exchange Commission