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 23, 2023

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

Re: Cybersecurity Risk Management for Broker-Dealers et al.;
File No. S7-06-23

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 various SEC covered entities, including broker-dealers and transfer agents, 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 covered entity's cybersecurity risks. The proposal would also impose disclosure, reporting, and recordkeeping requirements on persons subject to the new rules.

We are pleased that the Commission has proposed provisions that would require covered entities to have formal programs designed to address cybersecurity risks. Currently, the only information security requirement applicable to SEC covered entities is in Section 248.30 of Regulation S-P, which "requires covered entities 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

[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 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)(Release). Of the entities covered by the proposal, the Institute's comments relate to its impact on transfer agents.

2002, we believe it is appropriate for the Commission to impose greater rigor on covered entities information security and we support the Commission's adoption of appropriate rules in this area. While we largely support the substance of the Commission's proposal, we oppose the Commission adopting new rules to impose these requirements. Instead, we strongly recommend, as the Commission revises Regulation S-P,[3] that the Commission incorporate any provisions relating to cybersecurity risk management programs into the Regulation. This is appropriate because Regulation S-P governs safeguarding of customers' non-public personal information (NPPI), and, as proposed to be amended by the Commission, it would also require covered institutions to provide breach notices to persons affected by a breach of the institution's NPPI.

Last year, the Institute filed detailed comments on the proposed cybersecurity risk management program rules for investment companies and investment advisers.[4] When the Commission proposed a cybersecurity rule for covered entities this year, we were disappointed to see none of our recommended revisions, nor similar recommendations from other public commenters, reflected in this proposal. We hoped that, in drafting a cybersecurity risk management program for other SEC covered entities, the SEC would have addressed the concerns of commenters on the 2022 Release in the current proposal. In the open meeting in which the Commission considered this proposal, Commissioner Uyeda commented on the lack of consideration given to commenters' concerns in drafting this 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.[5]

Because our concerns with the 2022 Release have not been addressed in the proposed rule for broker-dealers, transfer agents, and other covered entities, and because, with the exception of provisions in the proposal relating to disclosure of cyber incidents and the reporting of such incidents to the Commission, the current proposal is identical to the 2022 Release, much of this letter repeats the comments we provided on that proposal.[6]

---

[3] *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).

[4] *See* SEC Release Nos. 33-11028, 34-94197, IA-5956, and IC-34497 (February 9, 2022) (the "2022 Release").

[5] *See Statement on the Proposed Cybersecurity Risk Management Rule for Market Entities,* Commissioner Mark T. Uyeda (March 15, 2023).

[6] Our comment letter on the SEC's reopening of the comment period on the 2022 Release repeats the comments in this letter relating to the Release's disclosure of cyber events and the reporting of cyber events to the Commission. *See Reopening of Comment Period for Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies,* SEC Release Nos. 33-11167, 34-97144, IA-6263, and IC-34855 (March 15, 2023).

**Executive Summary**

While the Institute largely supports the substance of the Commission's proposal, we recommend that the Commission incorporate any cybersecurity risk management program requirements into Regulation S-P rather than adopting them as stand-alone rules. As regards details of the Commission's proposal, we recommend various revisions to it. These revisions are intended to ensure that the adopted rules provide covered entities the flexibility necessary to implement their cybersecurity risk management programs in a way that (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 covered entities' cybersecurity policies and procedures;
- 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 a covered entity and those whose cybersecurity practices are already subject to government oversight;
- Urges that the definitions for "cybersecurity threat" and "significant cybersecurity incident" be revised to target those threats and incidents impacting a covered entity's ability to maintain critical operations or protect information;
- Opposes the proposed public disclosure of cybersecurity incidents;
- Opposes the adoption of Form SCIR or any electronic or paper form to notify the Commission of significant cybersecurity incidents;
- Opposes using EDGAR as the portal for filing information with the Commission about significant cybersecurity incidents;
- Recommends the Commission avoid multiple reporting to federal agencies of the same significant cybersecurity incident;
- 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 covered entities once the rules are adopted.

## 1. The Scope of Regulation S-P Should Include Cybersecurity Requirements

The Institute opposes the Commission adopting the proposed cybersecurity risk management program requirements as separate rules under the Securities Exchange Act of 1934. Instead, we strongly recommend that Regulation S-P be revised to include these provisions within its scope. As discussed in more detail below, this approach to adopting cybersecurity regulations is appropriate due to the interconnectedness of data safeguards, cybersecurity, and breach notices – which are all within the scope of Regulation S-P – and it will result in harmonizing the disjointed and disparate manner in which the Commission has, to date, proposed to address these issues. [7]

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

Regulation S-P was 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

[7] William Birdthistle, Director of the SEC's 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).

> (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,[8] were directed by Congress to work together, through joint rulemaking initiatives, to implement the Act to ensure the consistent protection of an 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.[9]

Like Regulation S-P, when the Interagency Guidelines were originally adopted in 2001, their focus was on safeguarding NPPI.[10] Since then, however, they have been amended at various times to address other issues relating to data security, including cybersecurity and breach notices. In 2005, the Interagency Guidelines were revised to add an Appendix A to require institutions to have cybersecurity response programs for unauthorized access to customer information.[11] The cybersecurity risk management programs the Commission proposed last year for investment companies and investment advisers and for broker-dealers and transfer agents this year are, in part, patterned after those required by 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, the SEC has proposed to regulate that information under a new rule, Rule 38-2 under the Investment Company Act of 1940. If it is an investment adviser, proposed Rules 204-6 and 206(4)-9 would govern the

---

[8] 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.

[9] 12 CFR Part 364, Appendix B(III) of the Interagency Guidelines Establishing Standards for Safeguarding Customer Information.

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

[11] In 2021, the Interagency 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 Requirements for Banking Organizations and Their Bank Service Providers,* 86 Fed. Reg. 66424 (November 23, 2021).

adviser's cyber information. If it is a broker-dealer or a transfer agent, proposed Rule 242.10 under the Securities Exchange Act of 1934 would be the operative provision.[12]

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 issued 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 '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.[13]

Commissioner Mark T. Uyeda 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.

---

[12] 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.

[13] *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.

> 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.[14]

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

### 1.3 Advantages of the Interagency Guidelines' Holistic Approach

We believe the holistic approach of the Interagency Guidelines is preferable 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) governing their cybersecurity programs. This disparity in treatment is puzzling as it is both 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.

---

[14] *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. 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.

### 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 commend the Commission for its interest in 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 of 1934 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.

## 2. 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[15] – remain intent on penetrating systems of financial

[15] As we learned from the recent Consumer Financial Protection Board (CFPB) and SolarWinds breaches, cyber compromises are not limited to the private sector. The CFPB in April disclosed a breach by an employee of data of over 250,000 consumers. *See* Politico, April 19, 2023, "CFPB says Employee Breach Data of over 250,000 Consumers in 'Major Incident'" available at https://www.politico.com/news/2023/04/19/cfpb-employee-consumer-data-breach-00092919. The 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 2022). 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

institutions to access data or infiltrate their systems. 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."[16] 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.[17]

Mr. Zelvin also stated that, with respect to cybersecurity, the financial services sector is "doing extraordinary work. It's highly impressive."[18]

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

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).

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

[17] *Id.* at pp. 12-13.

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

> 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.[19]

Participants in the Roundtable also strongly recommended that, in taking any steps to address cybersecurity concerns, all federal regulators of financial institutions work collaboratively and talk to each other on these issues [20] to avoid conflicting regulations and requirements.

While these comments and recommendations were made in 2014, they remain valid today. For this reason, as the Commission considers adopting its proposed rules, we highlight and echo these recommendations. We urge the Commission to recognize the experiences and observations of experts, the work and experiences of their colleagues in the federal government that regulate the financial services sector, including the Interagency Guidelines, and the vigorous and distinctive efforts of our industry – in the absence of regulatory requirements – to maintain effective information security programs. Much is at stake. It is critical that the Commission utilize the expertise of stakeholders and experts in this space, including the federal Cybersecurity and Infrastructure Security Agency (CISA). The Commission must ensure that any rules it adopts in this area align with existing federal regulations related to cybersecurity, including those imposed on financial institutions or those adopted by CISA regarding cybersecurity reporting. Further, as reflected in expert advice, it is essential that the Commission avoid imposing overly prescriptive requirements that would disrupt covered entities' long-standing information security programs or fail to provide needed flexibility to respond to new and changing threats. It should also avoid imposing regulatory reporting requirements that increase the vulnerability of covered institutions to breaches or the actions of bad actors.

---

[19] *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.

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

## 3. Revising Elements of Proposed Rule 242.10 to Provide Flexibility and Consistency

There is much about the Commission's proposal that we support. We support the SEC

- Requiring covered entities to adopt, implement, and maintain cybersecurity risk management programs;
- Adopting rules to define the structural elements of those programs consistent with the NIST framework;
- Providing covered entities the flexibility necessary to tailor their programs based on the covered entity's business operations, including its complexity and attendant cybersecurity risks;
- Requiring the regular review of such programs;
- Ensuring that the SEC receives notice of certain significant cyber events impacting a covered entity; and
- Requiring covered entities to maintain records relating to their programs.

As is always the case, the devil is in the details. As noted previously, however, Regulation S-P should be the vehicle for imposing these requirements rather than imposing them through a variety of rules under the Investment Company Act of 1940, the Investment Advisers Act, and the Securities Exchange Act of 1934.

We recommend that the Commission revise some of the proposed provisions that would govern covered entities' cybersecurity risk programs to provide greater flexibility in the design and implementation of these programs. This approach will ensure that covered entities' existing cybersecurity risk programs, including any that are now governed by the Interagency Guidelines, are not disrupted or otherwise adversely impacted by adoption of the SEC's new rules.

### 3.1 The Institute Supports the Proposed Rules With Revisions

The Institute supports requiring covered entities to have written policies governing their cybersecurity risk management programs because such policies and procedures would help address operational and other risks that could result in harm or lead to the unauthorized access to or use of a covered entity's information. We also support requiring covered entities' 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.[21] Notwithstanding this support, we recommend various revisions to the proposed rules.

### 3.1.1 Risk Assessments Should Inform Implementation

The Institute supports requiring covered entities to periodically assess the cybersecurity risks associated with their information and systems. Such assessments should provide the foundation for covered entities 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 covered entities implement and maintain the other required elements of their cybersecurity risk programs. For example, because a covered entity's risk assessment should inform how it oversees its service providers, the oversight of service providers that present significant risk to the covered entity's information or information systems should be far more rigorous than it is for those service providers that present little, if any, cybersecurity risk.

### 3.1.2 User Security and Access Requirements Must be More Flexible

The Institute has concerns with the provision in Rule 242.10(b)(1)(ii) that would govern the policies and procedures a covered entity must have to adopt to govern "user security and access." As proposed, the rule would require covered entities 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 technical, yet important, provision. 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 ‑ *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).

[21] 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.

Our second concern with requiring "two or more credentials" is that this is a static requirement based on today's technology. We do not support imbedding a rigid requirement that will be overcome by technological advances. It is likely that, in the future, covered entities 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, we urge the Commission to revise proposed Rule 242.10(b)(1)(ii)(B) as follows:

> (B) Controls reasonably designed to authenticate authorized users and permit only authorized users to access the covered entity's information systems and information residing therein.

This revision is consistent with the provisions in the Interagency Guidelines that govern authentication controls and will enable covered entities to adapt their user access and controls to evolving technologies.[22]

### 3.1.3 The Information Protection Requirements Are Sufficiently Flexible

Proposed Rule 242.10(b)(1)(iii) would govern "information protection." It has two subsections: Subsection (A), which would govern internal access to information and information systems; and Subsection (B), which would govern external access to a covered entity's information or systems by service providers. Subsection (A) would require a covered entity, in protecting its information, to take into account five factors: the sensitivity level and importance of the information to the covered entity'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 covered entity or its clients 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 covered entities the flexibility necessary to protect their information and systems differently based on a consideration of these factors. We support this provision.

---

[22] We believe it is important for each of the elements in Rule 242.10 to be flexible enough to enable covered entities 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 covered entities to establish procedures "for the timely distribution, replacement, and revocation or passwords or methods of authentication." This provision appears to provide covered entities 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.

### 3.1.4 Concerns with Monitoring Information in Transmission

With respect to proposed Rule 242.10(b)(1)(iii)(A)(3), we recommend revising the provision that would require a covered entity to monitor "information in transmission." We understand that it is impossible to monitor data "in transmission." Accordingly, the phrase "including the monitoring of information in transmission" must be deleted from this provision.

## 3.2 Concerns with Breadth of Service Provider Oversight

Proposed Rule 242.10(b)(1)(iii)(B) would require a covered entity's policies and procedures to include provisions requiring the oversight of service providers that receive, maintain, or process the covered entity's information or that have access to its information or information systems. We do not oppose the Commission requiring covered entities to oversee those service providers that have access to their information or information systems. Indeed, we understand that covered entities have long routinely included cybersecurity considerations in conducting due diligence of their service providers that will have access to the covered institution's information or systems.

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

- Align any requirements with the Commission's regulatory jurisdiction;
- Exclude certain service providers; and
- Require service providers within the rule's scope to provide notice to a covered entity whenever the service provider experiences a significant cybersecurity incident.

Each of these recommendations is discussed separately below.

### 3.2.1 Aligning the Rule with the Commission's Jurisdiction

Rule 242.10(b)(1)(iii)(B) would require every covered entity to require each of its service providers that has access to a covered entity'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 paragraphs (b)(1)(i), (b)(1)(ii), (b)(1)(iii), (b)(1)(iv), and (b)(1)(v)" of the rule. Through this requirement, the Commission appears to be expanding its regulatory jurisdiction over persons that Congress has not authorized it to regulate.

If Congress intended to grant the Commission the authority to regulate the terms of any contract involving a covered entity, such provisions would have been included in the Securities Exchange Act of 1934. The Commission's attempt to do so appears outside of its authority under the Exchange Act. For these reasons we strongly oppose the Commission dictating the terms of a covered entity's contracts with any service provider.

In lieu of requiring these contractual provisions, we recommend that the Commission revise the rule to require covered entities, when retaining any service provider with access to the covered

entity's information or information systems, to ensure that such service provider implements and maintains appropriate measures that are designed to protect the covered entity's information and information systems. Importantly, this approach would avoid inappropriate and unnecessary disruption of how covered entities engage with a variety of service providers in the due diligence and oversight processes and ensure, consistent with current practices, that covered entities document the cybersecurity considerations of their oversight process in their written policies and procedures.

Such an approach would avoid disrupting covered entities' contracts with a significant range and variety of service providers. This is because covered entities would retain their ability to properly engage and oversee their specific service providers to ensure such service providers are properly protecting their information and information systems. This approach would also preserve the ability of the Commission to sanction covered entities 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 requiring covered entities to oversee their service providers with a view towards ensuring the protection of the entity's information and systems, we strongly oppose the Commission's approach to indirectly regulate, through contractual provisions, persons that it lacks legal authority to regulate directly.[23]

### 3.2.2 Excluding Certain Service Providers

As proposed, the provisions of Rule 242.10(b)(1)(iii)(b) relating to service providers would apply to all service providers with access to a covered entity's information or information systems. 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 with access to some information or systems of the covered entity but who, if compromised, would neither impact the ability of the covered entity to maintain critical operations nor jeopardize the confidentiality or security of such information or systems (*i.e.*, would not result in a "significant cybersecurity incident"); and (2) those whose cybersecurity practices are already subject to government oversight.

### 3.2.3 Service Providers Presenting Limited Risk

With respect to the first category of service providers, a covered entity 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 covered entity to maintain critical operations nor jeopardize the confidentiality or security of its information or systems. Instead, consistent with the covered entity'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 the covered entity should not be within scope of

[23] See also, ICI Letter to Vanessa Countryman, Secretary, July 28, 2022 (revising the proposed written contract provision in the 2022 Release for information handling service providers).

the rule's oversight requirements to avoid covered entities unnecessarily expending precious resources.

### 3.2.4 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 covered entity 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 covered entities to both assess such service providers' cybersecurity controls and require them to execute a contract with the covered entity in which they agree to establish, implement, and maintain the information security policies and procedures.

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 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 242.10 – *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.[24]

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, like the private sector, the federal government and its agencies are dependent upon the services provided by these companies. To address these companies' reluctance to share 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

[24] Unlike the SEC, such regulatory action would not seek to penalize or publicly sanction the banking institution for such violation. Instead, the federal banking regulators' focus would be on shoring up the institution's cyber defenses in the interest of the institution's safety and soundness and protection of the institution's customers.

use of cloud services by the federal government."[25] 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, which has been described as no easy feat.

> 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.[26]

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. Such service provider authorization should obviate the need for the SEC to include these service providers within the scope of its proposal.

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 covered entities 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 covered entities to leverage the government's rigorous process for reviewing these companies' information security practices will present an impossible dilemma for covered institutions.

We recommend that, to avoid disrupting or impeding the relationships covered entities have with service providers whose cybersecurity practices are already subject to government oversight, the Commission should exclude them from the rule. Failure to do so will result in severe disruptions to covered entities' 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 Covered entities** – 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 covered entity to verify that another covered entity has a program in place that is compliant with the SEC's requirements.

- **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 242.10. Because federal banking regulators oversee institutions' implementation of the

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

[26] *Ibid.*

Guidelines' requirements, SEC covered entities 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."[27] 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 covered entities 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 covered entities 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, Rule 242.10(a), Definitions, should be revised to add a definition of "service provider" and specify which service providers are outside of the definition's scope.[28]

### 3.2.5 Service Providers Should Provide Covered Entities Notice of Significant Cybersecurity Incidents

Rule 242.10 does not require service providers with access to a covered entity's information or system to provide notice to a covered entity if the service provider experiences a significant cybersecurity incident that may impact the covered entity's information or information systems. Consistent with the requirements imposed on federal banking institutions (*e.g.,* through the

---

[27] *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).

[28] *See* Section 3.2.10.3 of this letter, below, for our recommendations regarding a definition of "service provider."

Interagency Guidelines),[29] we believe those service providers within the rule's scope should have a duty to provide notice of significant cybersecurity incidents to a covered entity so it can take any steps necessary to protect its information and systems. We recommend that the Commission revise Rule 242.10 to include such a requirement.[30]

### 3.2.6 Recommended Revisions 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 242.10(a), as set forth below under Section 3.2.10.3, we recommend that the Commission revise Rule 242.10(b)(1)(iii)(B) in relevant part to read as follows:

> (B) Require oversight of service providers that receive, maintain, or process a covered entity's information, or are otherwise permitted access to the covered entity's information systems and any information residing on those systems, pursuant to a written contract between the covered entity and the service provider, through which the service providers are required to implement and maintain appropriate measures~~, including the practices described in paragraphs (b)(1)(i), (b)(1)(ii), (b)(1)(iii), (b)(1)(iv), and (b)(1)(v) of this section,~~ that are designed to protect the covered entity's information systems and information residing on those systems. Such contract shall require the service provider to notify its customers by phone or email or other similar means 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 customer's information or information systems.

### 3.2.7 Clarifying Cybersecurity Threat and Vulnerability Management Provisions

Rule 242.10(b)(1)(iv) would require a covered entity's policies and procedures to include measures to detect, mitigate, and remediate "*any* cybersecurity threats and vulnerabilities" relating to its information systems or the information they hold. [Emphasis added.] We recommend deleting "any" because the terms "cybersecurity threat" and "cybersecurity vulnerability" are comprehensively defined in subsection (a) of the rule. As a result, it is unnecessary to include "any" in this provision. Further, we are concerned that its inclusion risks being read to mean a covered entity's policies and procedures must address cybersecurity threats and vulnerabilities beyond those covered by these definitions.

### 3.2.8 Support for Cybersecurity Incident Response and Recovery Provisions

---

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

[30] *See* Section 3.2.6 of this letter. We note, however, that, if the revisions the Commission has proposed to Regulation S-P are adopted, service providers would have a duty under Section 248.30 to provide the notice we recommend.

We support the provision in Rule 242.10(b)(10(iv) that would require covered entities to detect, respond to, and recover from a cybersecurity incident. We believe the proposed elements of a covered entity's policies and procedures are appropriate.

### 3.2.9 Need to Clarify the Required Annual Review Process

Proposed Rule 242.10(b)(2) would require a covered entity to conduct an annual review of the design and effectiveness of its cybersecurity policies and procedures. We support including this requirement.

### 3.2.10 Recommended Revisions to the Rules' Definitions

The Commission has proposed to define the following terms in Rule 242.10(a): covered entity, cybersecurity incident, cybersecurity risk, cybersecurity threat, cybersecurity vulnerability, information, information systems, market entity, personal information, and significant cybersecurity incident. We support adoption of the proposed definitions. The definitions appropriately complement and delineate the duties required of covered entities' cybersecurity risk programs to ensure that such entities take the steps necessary to analyze and protect their information and information systems from reasonably foreseeable cyber threats and vulnerabilities.

We recommend minor revisions to the definitions of "cybersecurity threat" and "significant 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 242.10(b)(1)(iii)(B) that require oversight of service providers.

#### 3.2.10.1 Revise "Cybersecurity Threat" to be Consistent with other Definitions

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 could result in or from a "cybersecurity incident." By contrast, the definition of "cybersecurity threat" would include "any potential occurrence" that could adversely affect the confidentiality, integrity, or availability of a market entity's information or information systems. This definition is too broad, reaching conduct that may, but is unlikely, to impact the market entity's information or systems. Consistent with the definitions of "cybersecurity risk" and "cybersecurity vulnerability," we recommend narrowing the definition of "cybersecurity threat" to only include those potential occurrences that may result in a "cybersecurity incident."

#### 3.2.10.2 Definition of "Significant Cybersecurity Incident" Should Not Include Degradation of Systems

The Commission has proposed to define the term "significant cybersecurity incident" to mean an incident or group of incidents that significantly: (1) disrupts or degrades a market entity's ability to maintain critical operations; or (2) leads to the unauthorized access or use of the market entity's information where such unauthorized access or use of such information results in substantial harm to the market entity or to a customer, counterparty, member, registrant, or use of the market entity, or any person that interacts with the market entity. The Institute commends the Commission for proposing a definition that is targeted at those cybersecurity incidents that imperil a market entity'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 covered entities, regulators, and potentially the financial markets, while filtering out the noise of cyber incidents that do not significantly impair the market entity's operations, information, or 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 the market entity or person it engages with. The fact that a market entity's systems may have been degraded due to a cybersecurity incident should not necessitate reporting to the Commission.[31] Unless and until the degradation results in the market entity'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.

### 3.2.10.3 Definition of "Service Provider" Should be Added to the Rules

As discussed above, we recommend that the Commission exclude from Rule 242.10(b)(1)(iii)(B), which requires covered entities to oversee their service providers that have access to a covered entity's information or 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 242.10(a) along the lines of the following:

> *Service provider* means a third-party that receives, maintains, or processes a covered entity's information or that otherwise is permitted to access the covered entity's information systems and any information residing therein if a breach of such service provider's systems or information would disrupt the covered entity's ability to maintain critical operations or compromise the security of the covered entity's information. The term does not include any: (i) person regulated by the Commission; (ii)

[31] For example, degradation of a covered entity's systems may mean a slower response time for systems to respond to a command. This slower response time would not necessarily impair the covered entity'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 impacts 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.

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) service provider listed in the FedRAMP Marketplace.

## 4. Disclosure of Cybersecurity Risks and Incidents

The Commission has proposed to require covered entities to publicly disclose cybersecurity risks and to disclose to the Commission significant cybersecurity incidents. For the reasons discussed below, the Institute strongly opposes public disclosure of a covered entity's cybersecurity risks. And, while we support covered entities alerting the Commission of significant cybersecurity incidents, we strongly oppose the method proposed for this disclosure.

### 4.1 Disclosure of Cybersecurity Risks

Rule 242.10(d)(1)(i) would require a covered entity to "provide a summary description of the cybersecurity risk that could materially affect the covered entity's business and operations and how the covered entity assesses, prioritizes, and addresses those cybersecurity risks." This disclosure would be provided through Parts I and II of a new form, Form SCIR, which would be filed with the SEC's EDGAR system. In addition to making these disclosures through the EDGAR system, covered entities would also be required to post Part II of Form SCIR "on an easily accessible portion of the [covered entity's] business Internet website that can be viewed by the public without the need of entering a password or making any type of payment or providing any other consideration."

As discussed in more detail below, we oppose this disclosure because it would not serve any public purpose and, in fact, it would be a road map for bad actors. 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.[32] 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 even better." [33]

#### 4.1.1 The Disclosure Would Serve No Public Purpose

[32] We note, however, that the Commission has 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 were due by May 9, 2022.

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

According to the Release, the "objective of these disclosures is to provide greater transparency to customers, counterparties, registrants, or members of the Covered Entity, or to users of its services, about the Covered Entity's exposure to material harm as a result of a cybersecurity incident, which, in turn, could cause harm to customers, counterparties, members, registrants, or users. . .."[34] We disagree that such transparency will be meaningful or of value to customers or counterparties.[35] Nor do investors appear to be interested in this information.

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 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 their governance approach to addressing their cybersecurity risks.

### 4.1.2 The Disclosures Would be Very Meaningful to Bad Actors

Bad actors will be very interested in reading the proposed disclosure. According to the Release,

> . . . the intent of the disclosure on Part II of proposed Form SCIR is to avoid overly detailed disclosures that could increase cybersecurity risks for the Covered Entity and other persons. Revealing too much information could assist future attackers as well as lead to loss of customers, reputational harm, litigation, or regulatory scrutiny, which would be a cost associated with public disclosure. Therefore, under proposed Rule 10, the Covered Entity would be required to provide *only a summary description of its cybersecurity risk and significant cybersecurity incidents.* [Emphasis added.]

According to Part II of Form SCIR, the "summary description" of each significant cybersecurity incident that would be disclosed on the form must include each of the following:

- The person or persons affected;
- The date the incident was discovered and whether it is ongoing;

---

[34] Release at p. 161

[35] As regards requiring this disclosure to provide greater transparency to the covered entity's business partners, we disagree that this disclosure is necessary. This is because it is common practice for any business partner of a covered entity, when conducting due diligence of the covered entity to assess the entity's cyber hygiene and explore any cyber incidents.

- Whether any data was stolen, altered, or accessed or used for any other authorized purpose;
- The effect of the incident on the covered entity's operations; and
- Whether the covered entity, or service provider, has remediated or is currently remediating the incident.

This is not a "summary description." Instead, it will be a treasure trove of information for current and future bad actors that will enable them "to attack you better." It will provide bad actors the information to understand the modus operandi and success of an intrusion into a covered entity's systems. We also are very concerned that this disclosure will apply to ongoing intrusions of those systems. For those bad actors that have already breached these systems or information, the required disclosure will be a report card of sorts letting them know how successful their efforts were.

We see substantial harm from such disclosure. The specificity that would be included in this disclosure will be a very valuable road map for bad actors that have attempted to breach the covered entity's systems or may be planning to do so. We disagree with the Commission's view that,

> The requirement that the disclosure contain summary descriptions only is designed to produce meaningful disclosures but not disclosures that would reveal information (e.g., proprietary or confidential methods of addressing cybersecurity risks or known cybersecurity vulnerabilities) that could be used by threat actors to cause harm to the Covered Entity or its customers, counterparties, members, users, or other persons.[36]

We think the Commission underestimates the sophistication of bad actors and their ability to render great harm from limited information. The Commission risks facilitating the ability of bad actors to exploit these disclosures by requiring persons filing Form SCIR to use "SCIR-specific XML" language when making the disclosures. Requiring disclosure of these significant cybersecurity incidents in an XML format will better enable bad actors to analyze and exploit the disclosures to the detriment of covered entities and their customers. For all these reasons, the Institute strongly opposes the disclosures that would be required by Rule 242.10(d)(2).

### 4.2 Disclosing Significant Cybersecurity Incidents to the Commission

In addition to requiring public disclosure of cybersecurity incidents, proposed Rule 242.10(c) would require covered entities to provide the Commission "immediate notice" – *i.e.*, no later than 48 hours – upon having a reasonable basis to conclude that a "significant cyber incident" has occurred or is occurring. Notification would occur by filing Parts I and II of Form SCIR with the Commission electronically through the Commission's EDGAR system. Part II of Form SCIR would have to be filed initially within 48 hours of the incident and, until the incident is

[36] Release at p 161.

resolved, covered entities would have to update the form whenever any information previously reported on it becomes materially inaccurate. According to the Release, the "Commission staff could use the reports to focus on the Covered Entity's operating status and to facilitate their outreach to, and discussions with, personnel of the Covered Entity who are addressing the significant cybersecurity incident."[37]

The Institute appreciates the importance of the SEC being made aware of significant cybersecurity incidents impacting covered entities and, for this reason, we support the Commission requiring covered entities to provide the SEC some notice of such incidents. We strongly oppose, however, how the SEC proposes to be notified of these incidents and we strongly oppose the SEC using Form SCIR – or any form – for this purpose as well as it using EDGAR as the portal for and repository of this information.

### 4.2.1 The Reporting Protocols of the Interagency Guidelines

As noted previously, in November 2021, the Interagency Guidelines were amended by the federal banking regulators to require federal banking institutions to notify their primary regulator in the event of a "notification incident."[38] While the SEC's current proposal largely tracks the requirements of the Interagency Guidelines, when it comes to the required reporting to a regulator of a cybersecurity event, the SEC's proposal significantly deviates from that of the Interagency Guidelines with respect to (1) how the report is made and (2) the information that must be included in it. We strongly recommend that the Commission better align its reporting requirements with those of the Guidelines.

#### 4.2.1.1 The Interagency Guidelines Reporting Protocols

The SEC has proposed that covered institutions report to the SEC via Form SCIR that, as discussed in more detail below, would include very detailed information about the incident. A covered institution would have to continually update the information on the form to ensure its accuracy. These forms would be filed via EDGAR, and EDGAR would maintain a database of this very sensitive and confidential information. By contrast, reports made to banking regulators under the Interagency Guidelines do not involve any forms. Instead, they are to be made by "email, telephone, or other similar methods" approved by the regulators. These methods of communication were chosen to balance "the need for banking organizations to have some flexibility, *including if a communication channel is impacted by the incident,* with the agencies' need to ensure that they actually receive the notification." [Emphasis added.][39] We strongly urge

---

[37] Release at p. 137.

[38] *See* fn. 11, supra. The Guidelines define "notification incident" as "a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade a banking institution's" ability to carry out banking operations, business lines, or operations.

[39] *See* 86 Fed. Reg.66433. As discussed in this letter, the Institute opposes the SEC's proposed notification requirements because, along with other reasons, they would require covered institutions to report to the SEC through systems compromised by the significant cybersecurity incident.

the Commission to align its reporting protocols to those of the Interagency Guidelines to avoid requiring covered institutions to file reports through systems that risk being compromised. Requiring reporting by phone, email, or other similar methods is far more likely to result in a dialogue between the SEC and the covered institution concerning the incident than a form filing.

#### 4.2.1.2 Information Reported under the Interagency Guidelines

The other way in which the SEC's proposed reporting significantly deviates from that of the Interagency Guidelines relates to what information is reported. As noted in the release adopting the Interagency Guidelines' reporting requirements, "*No specific information is required in the notification other than that a notification incident has occurred."*[40] This seems appropriate because such reporting is intended to commence a dialogue between the regulator and the institution. During the resulting discussion, the regulator can ask the questions necessary to understand the incident, its impact, and how the institution is responding. This discussion seems far more informative and meaningful – for both the regulator and the institution – than the information that would be required by a static form, such as Form SCIR. If the SEC's interest is to understand them, and not merely a form filing exercise, it should adopt the federal banking regulators' approach to reporting so it can actively engage with a covered institution as soon as an incident is reported.

#### 4.2.1.3 The Goals and Objectives of Reporting Incidents to Regulators

The federal banking regulators are interested in receiving reports of cyber incidents so they can understand the incident, how it may be impacting the financial institution, and, importantly, assist the institution in dealing with it:

> Timely notification is important as it would allow the agencies to (1) have early awareness of emerging threats to banking organizations and the broader financial system, (2) better assess the threat a notification incident poses to a banking organization and take appropriate action to address the threat, (3) facilitate and approve requests from banking organizations for assistance through the U.S. Treasury Office of Cybersecurity and Critical Infrastructure Protection (OCCIP), (4) provide information and guidance to banking organizations, and (5) conduct horizontal analyses to provide targeted guidance an adjust supervisory programs.[41]

---

[40] *Id.*

[41] 86 Fed. Reg. 66425. Footnote 6 within this text explains that OCCIP coordinates with U.S. Government agencies to provide agreed-upon assistance to banking and other financial services sector organizations on computer-incident response and recover efforts. These activities may include providing remote or in-person technical support to an organization experiencing a significant cyber event to protect assets, mitigate vulnerabilities, recover and restore services, identify other entities at risk, and assess potential risk to the broader community.

With these as their goals and objectives for receiving notice of cyber events, the federal banking regulators have deliberately designed their notification requirements to ensure that there is a dialogue between a banking institution and the institution's primary regulator. Moreover, however, as noted above, the federal banking regulators are requiring this report, in part, *in order for them to assist the banking institution in resolving the incident,* including by connecting the institution to the OCCIP.

By contrast, however, the SEC's goal in requiring the filing for Form SCIR to report an incident is so "Commission staff could use the reports to focus on the Covered Entity's operating status and to facilitate their outreach to, and discussions with, personnel of the Covered Entity who are addressing the significant cybersecurity incident."[42] We believe, consistent with the Interagency Guidelines, that when a federal agency requires reporting of a cyber event, such reporting should trigger the agency engaging with the institution reporting the incident, in part, to provide assistance and resources to the institution as it resolves the incident. There does not appear to be any discussion in the SEC's Release regarding the proposed notice triggering the SEC actively assisting the covered institution in mitigating and addressing the incident. This is unfortunate and a missed opportunity.

In conjunction with its interest in receiving notice of these incidents, the Commission should commit to actively working with covered institutions to assist them. For example, the federal Cybersecurity and Infrastructure Agency (CISA) will soon be drafting rules to implement the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). In addition to these rules governing the reporting of cyber incidents to the Federal government, such reporting will allow CISA to rapidly deploy resources and assistance to victims of these incidents. The Commission should consider acting as a conduit between covered institutions and CISA to assist covered institutions that are the victim of an incident to resolve such incident.

#### 4.2.1.4 Align the SEC's Reporting Requirements to those of the Interagency Guidelines

In summary, the Institute supports the SEC receiving timely notice of any significant cybersecurity incident a covered institution experiences. Such notice, however, should be meaningful and informative to both the covered institution and the SEC with an overall goal of working to resolve the incident and helping to protect the affected persons. To ensure this will be the case, the SEC should align its reporting with those of the federal banking regulators such that it is designed to commence a timely engagement between the SEC and the covered institution regarding the incident. The SEC should also, like its banking counterparts, stand ready to "provide information and guidance" to the covered institution regarding the incident and make the institution aware of any federal resources that may be beneficial to it as it addresses and responds to the incident.

### 4.3 Concerns with Using Form SCIR to Report Significant Cyber Incidents

[42] Release at p. 137.

The SEC has proposed to require covered institutions to report significant cybersecurity incidents on Form SCIR. We are pleased that the Commission seeks input on whether there are ways, other than by filing Form SCIR, that could be used to report significant cybersecurity incidents. As discussed above, we strongly recommend that the Commission rethink using a form to report these incidents and, instead, align its reporting requirements with those of the Interagency Guidelines.

We are concerned with the SEC requiring covered institutions to report highly sensitive information through any form, including Form SCIR, due to the risk of the form being compromised with potentially dire consequences to a covered entity. We support the Commission treating this information as confidential. Nevertheless, we are extremely concerned that, by collecting such information through required form filings the SEC, will create a warehouse of such forms on its systems, including its EDGAR system, which will be an attractive and identified target for bad actors. Conforming the Commission's method of reporting significant cyber events to the approach of the federal banking regulators as discussed above would address our concerns. It is a tested and well understood approach too. Such reporting would meet the interests of the SEC in receiving this information in a timely manner while reducing the considerable risks associated with Form SCIR.

In addition, it seems counterintuitive to require a covered entity 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 covered entity'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 covered entity'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 or use its filing to install malware, thereby infecting the SEC's systems.

By aligning its reporting requirements with those of Interagency Guidelines, the Commission would avoid: (1) Commission staff having to conduct EDGAR searches to determine which covered entities are experiencing significant cybersecurity incidents; and (2) enable the Commission staff to have a timely and productive discussion with the covered entity about the incident. This dialogue would begin as soon as the covered entity contacts the Commission through a secure phone line, email, or similar means to report the incident. Requiring reporting by phone or email would require the Commission staff receiving these notices to be knowledgeable about the types of significant cybersecurity incidents that occur, including the hackers' modus operandi and the incident's impact on the covered entity's systems and data. In our view, however, if the Commission is going to be collecting information about covered entity's cybersecurity incidents, its staff must be knowledgeable to understand the information the Commission receives about these incidents in order to identify "patterns and trends across Covered Entities, including widespread cybersecurity incidents affecting multiple Covered Entities at the same time" and "evaluate the effectiveness of various approaches to respond to and recover from a significant cybersecurity incident."[43] And, like the federal banking

[43] Release at p. 138.

regulators, it should be sharing relevant information with the covered institution rather than having these conversations be one way.

We note that under the Interagency Guidelines, there are *no* recordkeeping requirements imposed on financial institutions. Any records relating to information communicated to a federal banking regulator are created and maintained by the regulator. We concur with this approach as it limits vulnerabilities associated with this information. If the Commission is concerned about the covered entity maintaining a record of any notice it provides to the Commission regarding these incidents, the Commission could require a limited written record of its communications with the SEC about the incident, including those taking place by phone or email.

### 4.3.1 Concerns with Using EDGAR as the Filing Portal and Repository

As discussed above, last year the Institute filed a letter with the Commission on its proposed cybersecurity risk management program rule for registered investment companies and investment advisers. Like the current proposal, that proposal would require registrants to immediately notify the Commission of significant cybersecurity incidents. The proposal would require incidents to be reported to the Commission by filing a new form, Form ADV-C, which would be filed with the Investment Adviser Registration Depository (IARD).

Like this letter, our comments on that proposal strongly opposed using Form ADV-C and the IARD to report such incidents. The Commission's current proposal would require filings related to significant cybersecurity incidents be filed using the EDGAR system. While we had serious concerns with using the IARD for similar reports by registered investment companies and investment advisers, our concerns with using EDGAR for covered entities' filings are heightened. We urge that the Commission not use EDGAR for these purposes.

### 4.3.2 The Breach of the SEC's Systems, Including EDGAR

In September 2017, SEC Chairman Clayton issued a public statement on cybersecurity.[44] This statement was the first public disclosure of a 2016 breach of the SEC's EDGAR system, the system that the Commission is proposing be the repository for crucially sensitive information about a covered entity's significant cybersecurity incidents. As disclosed in the statement:

> In August 2017, the Commission learned that an incident previously detected in 2016 may have provided the basis for illicit gain through trading. Specifically, a software vulnerability in the test filing component of the Commission's EDGAR system, which was patched promptly after discovery, was exploited and resulted in access to nonpublic information. It is believed the intrusion did not result in unauthorized access to personally identifiable information, jeopardize the operations of the Commission, or

[44] The Chairman's statement is available at: https://www.sec.gov/news/press-release/2017-170.

> result in systemic risk. An internal investigation was commenced immediately at the direction of the Chairman.

Reading the pleadings filed against the hackers in January 2019,[45] the public learned that the hackers had been able to penetrate the SEC's EDGAR computer network in May 2016 and such unauthorized access continued until at least October 2016. In addition, while the Commission did not alert the public to this hack until September 2017 – almost 18 months after it occurred – FORTUNE magazine reported as early as March 2017 that EDGAR users has been receiving SEC emails the scammers were spoofing.[46] These emails were early indicators of the breach of the EDGAR system.

Just in April, the Consumer Financial Protection Board disclosed an employee breach of the data of more than 250,000 consumers. In 2020 Solar Winds, a software company whose Orion network management system was used by a variety of private and public organizations ‑ including the SEC ‑ to manage their IT resources was breached. This breach enabled the hackers to access data, networks, and systems of these organizations.

These hacks evidence that even the SEC's systems cannot be immune from attacks; hence our concerns with using EDGAR and our recommendation to follow the established approach of the federal banking regulators to reporting of significant cyber events.

## 5. The Commission's Challenges Regarding Information Security

The Commission has experienced challenges regarding its information security. In 2008, the Institute filed a comment letter on the proposal to revise Regulation S-P to require registrants to have more rigorous cybersecurity programs and provide customers breach notices in the event their NPPI was accessed without authorization. In that proposal, the Commission asked whether the Commission should provide breach notices whenever its information or systems were compromised. We responded affirmatively and recommended that the Commission provide such notices.

---

[45] *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).

[46] The Fortune article noted, in part, that the cyber scammers were "sending spoofed emails, purporting to be from the SEC, and aiming them at lawyers, compliance managers, and other company officials who file documents with the SEC. . . . Those who clicked on instructions in the Word document granted the attackers access to internal corporate networks . . .." According to the article, the security firm FireEye discovered these spoofed emails in February 2016 when it intercepted suspicious emails targeted at companies in sectors ranging from transportation to banking to retail. At the time, FireEye believed the scammers were likely an Eastern European criminal syndicate that was looking to make money by trading on inside information. *See "Fake SEC Emails Target Execs for Inside Information,"* Fortune (March 7, 2017), which is available at: http://fortune.com/2017/03/07/sec-phishing/.

In 2007, the Government Accountability Office (GAO)[47] and the SEC's Office of Inspector General ("OIG")[48] cited significant deficiencies in the Commission's information security and security of laptops. The GAO report stated that the SEC had not consistently implemented certain key information security controls, and it identified continuing and new information security weaknesses. GAO observed that the SEC had not mitigated weaknesses in various areas.[49]

While those reports are from more than 15 years ago, the information security concerns documented by the GAO and OIG continue to the present. According to the SEC's OIG most recent *Semiannual Report to Congress (10.01.21 to 03.21.22),* the OIG engaged Kearney and Company to conduct an independent evaluation of the SEC's information security programs and practices. This evaluation was conducted to assess the Commission's implementation of the Federal Information Security Modernization Act of 2014 (FISMA). FISMA "requires all federal agencies to develop, document, and implement an agency-wide information security program to protect its information and information systems . . .."

According to Kearney, the SEC's "information security program did not meet the FY 2021 IG FISMA Reporting metrics definition of 'effective,' which requires the simple majority of domains to be rated as 'Level 4: Managed and Measurable.'" Because the final report contains information about the Commission's systems, only a redacted version of the report is publicly available. As a result, while the Commission's information security program is described as ineffective, there is limited information about the specifics of these inadequacies. Appendix III to the Kearney report consists of a chart of the FISMA ratings of the SEC in nine areas: Risk Management; Supply Chain Risk Management; Configuration Management; Identify and Access Management; Data Protection and Privacy; Security Training; Information Security Continuous Monitoring; Incident Response; and Contingency Planning. Of the nine areas reviewed by Kearney, eight were rated overall as "Not Effective."[50]

---

[47] *See Financial Audit, Securities and Exchange Commission's Financial Statements for Fiscal Years 2007 and 2006* (GAO-08-167) (Nov. 2007) at pp.10-11. According to the GAO report, the GAO would be "issuing a separate report on issues [the GAO] identified regarding information security concerns at the SEC." To our knowledge, such a report was not published. By contrast we note that, according to the report of *The President's Identity Theft Task Force, Combating Identity Theft* (April 2007), "The SEC has not yet found any deficiencies during its examinations of [SEC registrants] that warranted formal enforce actions [under Regulation S-P] . . .." *See* Volume II of the report at p.13.

[48] *See Control Over Laptops,* SEC Office of Inspector General (Inspection Report No. 441, March 31, 2008). According to the Inspector General, the findings were of concern because of the SEC's enormous amount of non-public and sensitive market data, with most of it is stored on laptops. The Inspector General's report included five recommendations for the Commission to implement to enhance the security associated with laptops. We commend the Commission's staff for its expressed interest in implementing these recommendations but hope that the Commission will also adopt an information security program substantively similar to that proposed for registrants.

[49] *See* fn. 47, supra.

[50] The only area that did not receive a "Not Effective" rating was Incident Response. There are five maturity levels in the Cybersecurity Maturity Model Certification. The Commission's inability to be mature in Level 4 of this Certification should be of great concern to any persons whose information resides in the Commission's systems.

These most recent findings by Kearney are not an anomaly. Reviewing similar FISMA reports going back for nine years demonstrate persistent ineffective ratings of the Commission's information security program.[51] There also are other audits of the SEC's operations that identify concerns with the security of the SEC's information or systems:

- On September 30, 2020, during the pandemic when employees were more dependent on mobile devices, the SEC's OIG issued an audit report: *Opportunities Exist to Improve the SEC's Management of Mobile Devices.*[52] According to the findings of this audit, while the SEC's employees and contractors use mobile devices to perform their work and access SEC information, the SEC's Office of Information Technology (OIT) "did not establish and/or implement controls, including comprehensive processes and procedures, to effectively oversee the SEC's mobile devices and services." It concluded that:

  > Because OIT had not developed comprehensive policies and procedures specific to mobile device security or adequate processes to ensure compliance with recognized major controls affecting enterprise mobile device security, the SEC's processes did not adequately ensure compliance, assess risk, identify issues, or mitigate vulnerabilities specific to mobile device security.

  On November 7, 2019, the OIG issued an audit report: *The SEC Can More Strategically and Securely Plan, Manage, and Implement Cloud Computing Services.*[53] While portions of the Executive Summary of this report have been redacted, the report found that the SEC's: (1) system security plans for its cloud-based systems in operation as of March 20, 2019, were missing cloud-specific security controls and enhancements; and (2) security assessment reports for the system were incomplete. The report noted that these conditions occurred because the SEC's OIT

---

*See, An Introduction to Cybersecurity Maturity Model Certification (CMMS),* Katie C. Stewart and Andrew Hoover, Carnegie Mellon University Software Engineering Institute (March 30, 2020), which is available at: https://insights.sei.cmu.edu/blog/an-introduction-to-the-cybersecurity-maturity-model-certification-cmmc/. As noted in fn. 51, *infra*, the Commission has failed to receive a Maturity Level 4 effectiveness rating for almost ten years.

[51] *See* Fiscal Year 2020 Independent Evaluation of SEC's Implementation of the Federal Information Security Modernization Act of 2014, Report No. 563 (December 21, 2020); Fiscal Year 2019 Independent Evaluation of SEC's Implementation of the Federal Information Security Modernization Act of 2014, Report No. 558 (December 18, 2019); Fiscal Year 2018 Independent Evaluation of SEC's Implementation of the Federal Information Security Modernization Act of 2014, Report No. 552 (December 17, 2018); Audit of the SEC's Compliance with the Digital Accountability and Transparency Act for Fiscal Year 2017, Report No. 545 (November 7, 2017); Federal Information Security Management Act: Fiscal Year 2014 Evaluation, Report No. 529 (February 5, 2015); and Federal Information Security Management Act: Fiscal Year 2013 Evaluation, Report No. 522 (March 31, 2014).

[52] OIG Report No. 562 (September 30, 2020).

[53] OIG Report No. 556 (November 7, 2019).

> . . . had not developed policies and procedures specific to cloud system security, or adequate processes to ensure compliance with the Federal Risk and Authorization Management program baseline controls and enhancements for which the agency is responsible. As a result, the SEC's processes did not adequately ensure compliance risk, identity issues, or mitigate vulnerabilities specific to the agency's cloud-based systems.

- On November 25, 2013, the OIG published an audit: *SEC's Controls Over Sensitive/Nonpublic Information Collected and Exchanged with the Financial Stability Oversight Council and Office of Financial Research.*[54] Among other things, the audit found that the:

> SEC employees and contractors who access the SEC's e-mail system using Outlook Web Access are not restricted from saving and uploading sensitive or nonpublic information on non-SEC computers. Consequently, *sensitive or nonpublic information could potentially be disclosed to unauthorized persons*. [Emphasis added.]
>
> Also, the SEC has not appointed primary information owners to oversee information it receives and shares with the [Financial Stability Oversight Council], its member agencies, or [the Office of Financial Research]. In addition, a protocol for inventorying and ensuring documents are appropriately marked has not been fully developed. As a result, the SEC may be unable to efficiently identify information owners and ensure documents are tracked and marked as appropriate.

- On March 31, 2011, the OIG issued an audit report on *The SEC's Implementation of and Compliance with Homeland Security Presidential Directive 12 (HSPD-12).*[55] HSPD-12 was issued in 2004 to require federal agencies to have programs in place to ensure that the identifications issued by each agency to federal employees and contractors meet a common standard. According to its findings, "the OIC found deficiencies in nearly every aspect of the SEC's HSPD-12 program, as well as significant concerns about the SEC's authority to determine eligibility for access to classified information and the current process for granting temporary access to SEC facilities." The 2011 findings also cite four prior OIG reports documenting deficiencies in the SEC's compliance with HSPD-12. These four audits were in 2005, 2006, 2008, and 2011, showing ongoing deficiencies despite the audits.

---

[54] OIG Report 509 (March 25, 2013).

[55] OIG Report 481 (March 31, 2011).

- On September 29, 2010, the OIG issued an audit report on the *Assessment of the SEC Privacy Program*.[56] According to this report, "Overall, the assessments conducted identified significant concerns with the manner in which the SEC handles PII data." Also, "our review identified high level vulnerabilities affecting SEC computer systems" and that the SEC's Operations Center systems "are vulnerable to exploitation and infiltration." This report included the following findings among others:

    - OIT's categorization of network vulnerabilities does not accurately reflect the actual risk to the environment;
    - SEC laptops can connect to the SEC network via a local area network (LAN) port while simultaneously connected to an external wireless network, exposing the SEC network to potential compromise by a malicious attacker;
    - The existence of design flaws in the development of the HUB application could potentially result in a compromise of data;
        - PII at one regional office is contained on shared drives without access controls, allowing all of the office's employees unfettered access to documents and data that may be misused;
        - Employees at one regional office violated the SEC Rules of the Road by sending documents containing PII data to personal email accounts and by using portable media that was not encrypted;
        - Documents containing PII data were casually left on work tables, fax machines, and desks; and
        - File rooms, file cabinets, and offices containing very sensitive information were unsecured.

    The report concluded that "[t]hese findings indicate a significant risk to the SEC network and the security of the data/documents handled by the agency."

- Finally, a March 31, 2008 audit report, *Controls Over Laptops*,[57] concluded that "effective accountability of laptop computers simply did not exist." It noted that "a Commission-wide inventory of laptop computers has not been performed since 2003," and, as a result, "laptops are extremely susceptible to theft without detection."

This pattern of deficiencies over a decade must be fully remedied before the Commission contemplates requiring covered entities to provide the Commission especially sensitive information concerning their operations and vulnerabilities. The fact that the Commission's most recent FISMA audit continues to rank the Commission's FISMA compliance – including its data protection and privacy efforts – as "not effective" is of incredible concern to us and should be for the Commission, too, as it indicates that the Commission continues to fall short in

[56] OIG Report 485 (September 29, 2010).

[57] OIG Report 442 (March 31, 2008).

adequately protecting the information it receives. The information security issues documented in these reports place covered entities in a highly uncomfortable position.

Considering the importance of effective information security, it is troubling to think that an SEC registrant's NPPI may become vulnerable when it moves from the registrant's systems to those of the SEC, whose information security deficiencies have been consistently documented by auditors and inspectors. We urge that, in light of the Kearney and ongoing OIG findings regarding the SEC's deficiencies and ineffective information security, it reconsider requiring the filing of any written or electronic report with the SEC relating to a covered entity's significant cyber security incidents. We further urge that the Commission not create a repository containing this very sensitive and confidential information. This information in the wrong hands could be detrimental to the covered entity that was the subject of the incident, thereby exacerbating its impact. Customers, clients, and investors of the covered entity stand to be harmed by any breach of this information, which we urge the Commission to keep in mind too. If the SEC were to adopt the Interagency Guidelines' approach to reporting information about significant cybersecurity incidents, this would somewhat alleviate our concerns with that information being compromised. However, any records created by the SEC staff regarding these incidents could be at risk due to the SEC's deficiencies and ineffective information security as evaluated and reported by the OIG and others.

In summary, to avoid the potentially significant harm to covered entities that may result from filing Form SCIR with the SEC through the EDGAR system and to better ensure the confidentiality of the sensitive information in such reports, we urge that the Commission eliminate requiring covered entities to use paper or electronic forms to report their significant cybersecurity incidents. Furthermore, we strongly recommend that the Commission not continue to collect registrant's non-public or sensitive information until such time as the Commission demonstrates to auditors that it has effective data security and system security protections in place.

## 6. The Contents of Form SCIR

For the reasons discussed above, we strongly oppose the use of any form, including Form SCIR, to report significant cybersecurity incidents. If the SEC does not follow the Interagency Guidelines, there are three items of information included on Form SCIR that we recommend be revised or eliminated from the information reported to the Commission in connection with a significant cybersecurity incident. These three are: Items 8, 13, and 14 relating to remediation, disclosure, and cybersecurity insurance, respectively.

### 6.1 Concerns with Reporting Remediation Efforts Under Item 8

Item 8 of Form SCIR would require the covered entity to describe any "actions taken or planned to respond to and recover from the significant cybersecurity incident." We recommend this disclosure be eliminated for two reasons.

First, it would require a covered entity 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. Second, this information will provide a road map for bad actors that would enable them to refine their attack methods after better understanding how the covered entity's systems were compromised and the steps it has taken to remediate such compromise. In the hands of a bad actor, this information could have a severe adverse impact on the covered entity's operations. For these reasons, we strongly recommend that Item 8 be substantially revised to eliminate the detailed information. In lieu of reporting details of remediation, a covered institution should only be required to affirm that it is taking steps to respond to and recover from the incident.

### 6.2 Narrowing Public Disclosure of Incidents in Item 13

Item 13 on Form SCIR asks whether disclosure has been made about the incident on EDGAR, on the covered entity's business website, or, if applicable, to the covered entity's customers. If the covered entity responds "Yes," it must disclose when the disclosure was made. If it responds "No," it must explain "why the disclosures have not been made." We recommend that this Item be revised such that it only seeks information regarding disclosure made to the covered entity's customers if the incident involved NPPI the entity held on behalf of such customers and such notice was required by a federal or state breach notice requirement.

We therefore recommend that Item 13 be revised to: (i) only require disclosure of the event to the covered entity's customers when required by law and (ii) delete the required explanation of why such disclosure was not made.

### 6.3 Eliminating the Proposed Disclosure of Whether the Incident was Covered by an Insurance Policy in Item 14

The penultimate question on the Form asks whether the incident is "covered by an insurance policy of the covered entity." According to the Release, this information "could be relevant to Commission staff in assessing the potential magnitude of harm to the Covered Entity's customers, counterparties, members, registrants, or users and to the Covered Entity's financial condition."[58]

Cybersecurity insurance is an incredibly complex topic. We disagree that informing the Commission of the status of such insurance would render any meaningful information about the magnitude of harm of the incident or the covered entity's financial condition.[59] 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, which will vary considerably, is but one factor a covered entity may consider. Other

[58] Release at p. 152.

[59] Since Item 14 only asks whether the incident is "covered by an insurance policy," we are uncertain how, if the covered entity answers "Yes," the Commission would be able to assess from this response the magnitude of the harm from the incident or its impact on the covered entity's financial condition.

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 and with what terms and exclusions, is a business decision to be made by a covered entity based on its risk profile and an assessment of its needs. We disagree that the responses to Item 14 of Form SCIR will provide the Commission with any meaningful information or enable it to assess the potential magnitude of harm from a significant cybersecurity incident. Because of this, we recommend the Commission delete this Item from the reporting requirements.

### 6.4 Form SCIR's Execution Requirement

As proposed, Form SCIR would require the individual filing the form on behalf of the covered entity to certify that: (i) the Form was executed on behalf of, and the with authority of, the covered entity; (ii) the information reported on the Form is "current, true, and complete;" and (iii) "to the extent any information previously submitted is not amended, such information is current, true, and complete." According to the Release,

> The form of the certification is designed to ensure that the Covered Entity, through the individual executing the form, provides information that the Commission and Commission staff can rely on to evaluate the operating status of the Covered Entity, assess the impact of the significant cybersecurity incident may have on other participants in the U.S. securities markets, and formulate an appropriate response to the incident.

We recommend that the Commission eliminate this certification. Requiring a certification seems to emanate from concerns about the ability of the SEC to rely upon the information reported by a covered entity. We question this concern and fear that the value of this certification to the Commission will be to enable it to file an enforcement action against the person executing the form in the event the Commission determines there may be some inadvertent deficiency in the information reported or, when, in the Commission's view, such information was not timely updated. We do not believe these to be sound bases for requiring the certification and recommend it be deleted.

## 7. The SEC Should Avoid Duplicative Reporting of Cyber Incidents

The Institute recommends that Rule 242.10 be revised to address instances in which a covered entity has reported the significant cybersecurity incident to another federal agency with cybersecurity expertise. For example, transfer agents and other covered entities 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 the type, magnitude, and methodology of the cyber event 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,[60] 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 law enforcement. 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 agency – including a federal law enforcement agency – on a cyber incident, they should defer to the expertise of those agencies and the value they will add to helping a covered entity work to resolve the incident.

In addition, as discussed previously, CISA will soon be publishing rules to implement the Cyber Incident Reporting for Critical Infrastructure Act of 2002 (CIRCIA). CISA is currently in the process of gathering information and receiving input to assist it in drafting these rules. 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 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.[61]

When these rules are ultimately adopted, covered institutions should be encouraged to report their significant cybersecurity incidents to CISA. Reporting cyber incidents to CISA will have several advantages:

- CISA has "highly trained investigators who specialize in responding to cyber incidents for the express purpose of disrupting threat actors who caused the incident;"[62]

---

[60] 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 to an agent with whom they have a relationship.

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

[62] *Ibid.*

- CISA is able to provide "technical assistance to protect assets, mitigate vulnerabilities, and offer on-scene response personnel to aid in incident recovery;"[63]

- 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;[64] and

- CISA's involvement with cyber incidents extends well beyond those in the financials service sector that would impact SEC registrants.[65]

Once CISA adopts rules providing for the reporting of cyber incidents, we believe such reporting should trump and replace any detailed reporting requirements the SEC adopts under the federal securities laws. Otherwise, SEC registrants will be required to make duplicative reports and, unlike the reports to CISA, those filed with the SEC will not provide any benefit to the registrant as the SEC does not have CISA's mission, expertise, or ability 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."[66] If a covered institution is working with another federal agency that has experience with, and expertise in responding to, cyber intrusions, we do not oppose the SEC requiring the covered institution to alert it by phone or email to such engagement. We do, however, oppose the institution also having to duplicatively engage with the SEC regarding the incident or provide the SEC detailed information regarding the details of that engagement. Such diversion of resources will not be additive to efforts to resolve the incident.

In summary, we recommend that the notice provisions of Rule 242.10(c) be revised to add a new subsection (3) to provide as follows:

> (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 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 cybersecurity incident involving unauthorized access; or

---

[63] *Ibid.*

[64] *Ibid.*

[65] We presume CISA's efforts will complement the assistance the OCCIP provides to federal banking institutions when they experience cybersecurity incidents.

[66] *Ibid.*

(iii) Reported the incident to the Cybersecurity and Infrastructure Security Agency pursuant to its rules for reporting cybersecurity incidents.

(b) In the event a covered institution is excluded from filing a notice under this exclusion, it shall by phone or email or other similar method inform the Commission of its reliance on this exclusion.

## 8. Regulation by Enforcement Concerns

In recent dissents filed in connection with enforcement actions brought by the Commission, Commissioners Peirce and Uyeda have expressed concern with the Commission engaging in "regulation by enforcement" – *i.e.*, imposing new regulatory requirements on registrants when settling actions.[67] The Release appears to suggest such an approach.[68] For example, in discussing the risk assessment a covered institution would be required to conduct under the proposal, the Release states:

> In categorizing and prioritizing cybersecurity risks, the Covered Entity generally should consider consulting with, among others, personnel familiar with the Covered Entity's operations, its business partners, and third-party cybersecurity experts. In addition, a Covered Entity could consider an escalation protocol in its risk assessment plan to ensure that its senior officers, including appropriate legal and compliance personnel, receive necessary information regarding cybersecurity risks on a timely basis.[69]

We are very concerned with the Commission signaling in its releases that it is expecting registrants to take specific actions not required by the regulation. All regulatory requirements the Commission intends to impose on registrants should be expressly stated in the rule itself and, when inspecting for compliance with an SEC rule, a registrant should not receive a deficiency letter from the staff for not implementing requirements outside the rules' express requirements.

## 9. Meaningful and Adequate 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

---

[67] *See, e.g., Statement Regarding Huntleigh Advisors, Inc. and Datatex Investment Services, Inc.,* Commissioners Hester M. Peirce and Mark T. Uyeda (February 27, 2023), which is available at: https://www.sec.gov/news/statement/peirce-uyeda-statement-huntleigh-datatex-022723.

[68] We note, in reviewing the SEC's release proposing amendments to Regulation S-P, the SEC also signaled actions a registrant *should* take under the proposed amendments even though such actions are not required by the amendments.

[69] Release at p. 99.

Institute urges 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. The SEC also still has sufficient inspection and enforcement authority should a significant cybersecurity incident arise 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 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.

## 10. Implementation Guidance Will be Necessary Due to Rules' Complexity

Should the Commission pursue adoption of final rules requiring covered entities and market entities to establish, implement, and maintain cybersecurity risk programs along the lines outlined in the Release, these entities will need the Commission's guidance to properly understand the new requirements as the Commission intends. Once rules are adopted, we strongly encourage the Commission to work closely with covered entities and market entities ‑ as it has done with previous rulemakings ‑ to understand any post-adoption issues and implementation challenges that arise and consider issuing guidance as necessary to facilitate compliance and timely implementation efforts.

## 11. 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 (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