June 5, 2023

By Electronic Submission

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

Re: File No. S7-06-23; RIN 3235-AN
Cybersecurity Risk Management Rule 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

Dear Secretary Countryman,

The Securities Industry and Financial Markets Association ("SIFMA"), Bank Policy Institute ("BPI"), Institute of International Bankers ("IIB"), and American Bankers Association ("ABA"), (collectively, the "associations") appreciate the opportunity to respond to the Rule 10 Proposal issued by the Securities and Exchange Commission (the "Commission" or "SEC") on March 15, 2023 ("Rule 10 Proposal" or the "Proposal").[1] The associations recognize the importance of providing cybersecurity risk management rules for the entities covered by the Proposal ("Market Entities"), including broker-dealers and security-based swap dealers. A well-designed SEC rule could provide further clarity and guidance on strong cybersecurity practices, collaboration with government agencies, and proper cyber breach reporting. However, the associations recommend that the Commission significantly revise the notice of proposed rulemaking in line with essential cross-government harmonization, greater simplicity and flexibility, appropriate deference to the input of other government agencies, and thoughtful

[1] Cybersecurity Risk Management Rule 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, Release No. 34–97142, 88 Fed. Reg. 20212 (proposed Apr. 5, 2023) [hereinafter "Rule 10 Proposal"]. SIFMA notes that it requested an extension of the comment response deadline in order for it and other interested parties to have a full opportunity to comment effectively on this and many hundreds of pages of other SEC cybersecurity proposals that are simultaneously pending or were open or re-opened for comment at the same time as this Proposal. *See* SIFMA Letter to the SEC (Mar. 31, 2023), *available at* https://www.sec.gov/comments/s7-06-23/s70623-20162935-332874.pdf. The Commission failed to extend the comment deadline or otherwise respond to SIFMA's letter. The SEC's rushed proliferation of cybersecurity rulemakings is detrimental to sound policymaking in this crucial area and is not consistent with allowing regulated entities and other interested parties to fully evaluate the proposals and provide comprehensive feedback.

consideration of the burdens, impacts, and justifications for certain of the proposed requirements in the Proposal.

The Commission should reconsider significant aspects of its Rule 10 Proposal to allow the necessary flexibility for Market Entities to respond to unique circumstances that can arise during a cybersecurity incident. The Rule 10 Proposal should also account for the Commission's other proposals and existing cybersecurity requirements imposed by other financial regulators.

I. Executive Summary

The Commission should substantially reconsider the Rule 10 Proposal in light of several considerations, including the following:

- **The Commission should harmonize and reconcile the Rule 10 Proposal with other proposals and requirements**. The Commission must address and reconcile the considerable overlap and conflicts among the Regulation S-P Proposal, the Rule 10 Proposal, and other proposed and existing cybersecurity rules impacting the securities industry. While the Commission's narrative discusses the overlap in the proposals, it does not provide a clear guide to navigate the varying terms and processes of the different rules and proposals.

- **The Proposal's overly complex and granular requirements could impede the Commission's intended results of more effective cybersecurity risk management**. The proposed requirements should allow flexibility for Market Entities to tailor their policies and procedures according to their internal cybersecurity risk management framework. Further, notification and reporting requirements, redundant assessment, recordkeeping, and documentation requirements would over-burden Market Entities and interfere with substantive cybersecurity and incident response and are in sharp contrast to the requirements implemented by other financial regulators.

- **The proposed Form SCIR notification and public disclosure requirements may put security at risk and have financial stability implications**. The Commission should limit the data collected through Form SCIR to data that is directly relevant and necessary. Further, public disclosure of information relating to cybersecurity incidents or risks is unwarranted and may put Market Entities or the financial system at risk and could serve as a roadmap for a cybersecurity attack. For example, the requirement to rush public reporting of incidents, regardless of whether a company has successfully managed and recovered from an incident, could seriously mislead investors and the public about the degree of actual risk. Pressuring companies to prematurely declare incidents "significant" will induce investment decisions based on inaccurate or incomplete information and ultimately unwarranted market swings in public markets. EDGAR and other systems used to manage

incident information should be properly protected, and procedures for reporting EDGAR data breaches must be established.

- **Regulations should be designed to protect against cyberthreats, not to impose intrusive administrative burdens that also create undue enforcement and litigation risks**. The associations recommend that the Commission focus on regulations that aim to achieve greater cybersecurity rather than detailed and prescriptive administrative and recordkeeping requirements that may create undue enforcement and litigation risk, without advancing actual security. Rather than requiring onerous notification, reporting, assessment, and recordkeeping requirements, the Commission should reframe its proposals to support the efforts of firms to achieve better cybersecurity rather than divert resources (both technical and personnel) to excessive reporting intricacy and paperwork. The proposed SCIR process could distract and diminish resources better dedicated to responding and recovering from cybersecurity incidents. As CISA Director Jen Easterly recently noted, the government should not seek to "stab the wounded,"[2] especially considering that sophisticated cyber actors have the ability to victimize institutions (and government agencies) regardless of their cybersecurity measures in place.

II. The Proposal Does Not Align with Congressional, Executive, and Other Governmental Efforts to Harmonize and Enhance Our Nation's Cybersecurity Requirements; the Proposal Would Exceed the Commission's Proper Role in Addressing Cybersecurity.

A. The Commission Should Harmonize the Proposal with Existing and Upcoming Cybersecurity Regulations.

Over the past few years, our country and its industries have faced an increasingly challenging cyber threat environment that has drawn the attention of regulators and policymakers around the globe. This intense focus has led to a preponderance of new statutory and regulatory requirements and an increasing emphasis on cybersecurity for firms of all shapes and sizes. The associations welcome this change and reiterate their support for the Commission's continuing attention to cybersecurity risk management.

As Chair Gensler has noted, the SEC is an important member of Team Cyber, but not its captain.[3] Accordingly, rather than blaze its own trail as contemplated by this Proposal, the

[2] *See* Ben Kochman, *Biden Cyber Officials Pitch Partnership Amid Hacking Threat*, Law360 (Apr. 22, 2022), *available at* https://www.law360.com/corporate/articles/1482974/biden-cyber-officials-pitch-partnership-amid-hacking-threat.

[3] *See* Chair Gary Gensler note in his ("Working on Team Cyber") speech "Working On 'Team Cyber'" - Remarks Before the Joint Meeting of the Financial and Banking Information Infrastructure Committee (FBIIC) and the Financial Services Sector Coordinating Council (FSSCC), Speech, April 14, 2022, ("Other government entities,


associations recommend that the Commission should take a more holistic view, collaborate with other agencies and relevant self-regulatory organizations, and reconcile and harmonize what the SEC is proposing with existing and upcoming cybersecurity requirements. Additionally, while the Commission is focused on U.S. Market Entities, many Market Entities regulated by the Commission are global organizations. Accordingly, the Commission should consider global efforts to harmonize cyber incident reporting requirements. For example, the Financial Stability Board ("FSB"), of which the SEC is a member, recently published its final report on Recommendations to Achieve Greater Convergence in Cyber Incident Reporting.[4] The Report contains recommendations to promote convergence among cyber incident reporting frameworks, while recognizing that a one-size-fits-all approach is not feasible.

Harmonization of cybersecurity requirements is critical to advancing our Nation's important cyber efforts because consistency helps to ensure that scarce cyber professionals and limited resources can focus on protecting against threats rather than interpreting divergent standards. Congress and the Executive Branch have each promoted the importance of coordination, deconfliction, and harmonization. Under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA"), the Cybersecurity and Infrastructure Security Agency ("CISA") must consult with various entities, including Sector Risk Management Agencies ("SRMAs"), throughout its two-plus year cyber incident reporting rulemaking process.[5] CIRCIA also established the Cyber Incident Reporting Council ("CIRC") to "coordinate, deconflict, and harmonize federal incident reporting requirements."[6] The Administration, more recently, emphasized that the current environment requires a cybersecurity "regulatory framework[] . . . harmonized to reduce duplication."[7] According to the Administration, collaboration between regulators and industry will produce "operationally and commercially viable" regulatory requirements and "ensure the safe and resilient operation of critical infrastructure."[8]

The Commission's Rule 10 Proposal adds another regulation to the many regulations applicable to Market Entities, including those by CISA—the agency intended by Congress and the White House to lead the regulation of cyber incident reporting[9]—and fails to harmonize and reconcile where applicable.

---

such as the Federal Bureau of Investigation and CISA, captain Team Cyber—but the SEC has an important role to play as well."), *available at* https://www.sec.gov/news/speech/gensler-speech-joint-meeting-041422 [hereinafter Gensler "Working on Team Cyber" Speech].

[4] Financial Stability Board, Recommendations to Achieve Greater Convergence in Cyber Incident Reporting: Final Report (Apr. 13, 2023), https://www.fsb.org/wp-content/uploads/P130423-1.pdf.

[5] 6 U.S.C. § 681b(b)(1).

[6] 6 U.S.C. § 681f(a).

[7] White House, National Cybersecurity Strategy 8 (Mar. 2023).

[8] *Id.*

[9] The White House in its May 2021 Executive Order specifically identified CISA and the FBI, along with "other elements of the Intelligence Community," as being "responsible for investigating or remediating cyber incidents."

Association members already respond to, or are regulated by, numerous agencies (or their foreign counterparts) on matters related to cybersecurity. This is particularly true where members are entities registered with multiple federal regulators, such as broker-dealers that are also futures commission merchants or introducing brokers regulated by the Commodity Futures Trading Commission ("CFTC"), or where they are a part of corporate families that have other entities that are also federally regulated financial institutions. This includes cybersecurity regulation by CISA, the CFTC, and federal banking regulators such as the Office of the Comptroller of the Currency ("OCC") and the Federal Reserve Board. Moreover, numerous association members will likely be considered critical infrastructure sector entities subject to CIRCIA's requirements.[10] Despite this reality, the Rule 10 Proposal conflicts with these existing and upcoming requirements in multiple instances.

For example, the National Futures Association Interpretative Notice on Information Systems Security Programs, which are relevant to broker-dealers and security-based swap-dealers also regulated by the CFTC, establishes general requirements that provide its members the flexibility to design and implement policies and procedures based on their circumstances.[11] And unlike the immediate written electronic notice and 48-hour deadline to submit Part I of proposed Form SCIR, CIRCIA explicitly prohibits the CISA Director from requiring covered entities to report a cyber incident earlier than 72 hours.[12] Given Congress's, the Administration's, and the international FSB's direction, the Commission should recognize that overly prescriptive and inconsistent cyber requirements will be burdensome, confusing, and ultimately counterproductive and dangerous.[13]

The Commission is not an Intelligence Agency and does not have the expertise, resident in CISA and the FBI, to meaningfully assist on cybersecurity related matters. *See* Executive Order on Improving the Nation's Cybersecurity (May 12, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[10] Under CIRCIA, a "covered entity" means an entity in a critical infrastructure sector, as defined in PPD-21, that satisfies the definition established by CISA's rulemaking. 6 U.S.C § 681(5). PPD-21 identifies "Financial Services" as a critical infrastructure sector. CISA's definition of "covered entity" must be based on three factors: (1) "the consequences that disruption to or compromise of such an entity could cause to national security, economic security, or public health and safety"; (2) "the likelihood that such an entity may be targeted by a malicious cyber actor"; and (3) "the extent to which impact to such an entity will likely enable to disruption of the reliable operation of critical infrastructure." 6 U.S.C.§ 681b(c)(1).

[11] National Futures Association Interpretative Notice on Information Systems Security Programs, *available at* https://www.nfa.futures.org/rulebooksql/rules.aspx?RuleID=9070&Section=9.

[12] 6 U.S.C. § 681b(a)(1)(B) (providing that, although a covered entity shall report the covered cyber incident to CISA "not later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred" the Director "may not require reporting . . . any earlier than 72 hours after the covered entity reasonably believes that a covered cyber incident has occurred.").

[13] In dissent to the Proposal, Commissioner Uyeda commented:

> These prescriptive deadlines can potentially do more harm than good as these Commission regulatory filings would demand immediate attention from management all in the midst of

Additionally, the Commission should consider how the Proposal's requirements would overlap and potentially conflict with other SEC requirements, including those in the Public Companies Proposal that would, if finalized in present form, require current reporting about material cybersecurity incidents on Form 8-K within four business days after the registrant determines that it has experienced a material cybersecurity incident; and to amend Regulation S-K to require registrants to provide updated disclosure relating to previously disclosed cybersecurity incidents and to require disclosure, to the extent known to management, when a series of previously undisclosed, individually immaterial cybersecurity incidents has become material in the aggregate.[14]

For example, a public company that is also a Covered Entity, which includes some of the most highly regulated and systemically important global financial entities, would not have four business days as contemplated by the Public Companies Proposal to draft the appropriate disclosures in a Form 8-K filing, but would instead have its Form 8-K disclosures in effect supplanted and accelerated by the requirements in Form SCIR Part II. If the Commission believes public companies that are also Covered Entities require special treatment, it should explain its reasoning and how these accelerated and more prescriptive disclosures will not cause undue harm to the company and its shareholders.

We thus recommend that the Commission further harmonize its Proposal with existing cybersecurity requirements and cyber incident reporting requirements. Specifically, the Commission should adopt a flexible approach to cybersecurity policies and procedures that relies on existing frameworks like the National Institute of Standards and Technology ("NIST") Cybersecurity Framework. The Commission should also leverage the statutory and upcoming regulatory framework outlined in CIRCIA by providing a safe harbor from additional reporting requirements for critical infrastructure Market Entities and working with CISA and the Department of the Treasury to gather the information it seeks. To the extent CIRCIA is not applicable, the Commission should adopt the same approach as the banking agencies' Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers ("Interagency Notification Requirements"), which acknowledge the importance of providing

---

> responding to a breach and alerting other authorities, including law enforcement. And for what purpose? The SEC does not have a cyber response team that could immediately respond to seal the breach and provide technical assistance.

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

[14] Release Nos. 33-11038; 34-94382; IC-34529; File No. S7-09-22, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure.

financial institutions flexibility and confidentiality in reporting incidents "without unduly burdening banking organizations with detailed reporting requirements."[15]

Moreover, extending the Rule 10 Proposal to all transfer agents regardless of whether they are registered with the Commission would extend beyond the scope of the Commission's authority and could result in regulatory confusion. Transfer agents registered with an appropriate regulatory agency that is not the Commission could become subject to conflicting requirements from those regulators.

B. The Commission Should Not Seek to Displace the Sector Risk Management Agency for the Securities Industry or Agencies with Statutory Authority and Deep Cybersecurity Expertise.

While the Commission has a role to play in "Team Cyber" as the primary federal regulator for the securities businesses of the Market Entities and an interest in the cybersecurity of Market Entities,[16] it is not the SRMA for the financial services sector—that is the Department of the Treasury ("Treasury Department"). The SEC should therefore proceed with caution and refer to existing rules, guidance, regulators, and cybersecurity agencies. In Presidential Policy Directive – Critical Infrastructure Security and Resilience ("PPD-21"), President Obama identified Sector-Specific Agencies, now SRMAs, for each critical infrastructure sector.[17] Today, these SRMAs are statutorily tasked with certain incident response roles and responsibilities for their respective sectors, including "assessing [sector] risks" from "cybersecurity threats, vulnerabilities, and consequences" and "supporting incident management."[18] The Treasury Department is the SRMA for the financial services sector and securities industry—not the SEC. The Rule 10 Proposal, therefore, blurs the line between the SEC's role as a regulator of the Market Entities and Treasury Department's role as the financial services SRMA.

With respect to incident reporting and disclosure requirements, the Commission should defer to CISA and the Treasury Department. An objective of the Proposal's notification and reporting requirements is to "improve the Commission's ability to monitor and evaluate the effects of a significant cybersecurity incident . . . as well as assess the potential risks affecting financial

---

[15] Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers ("Interagency Notification Requirements"), 86 Fed. Reg. 66424, 66432 ("The final rule is designed to ensure that the appropriate agency receives timely notice of significant emergent incidents, while providing flexibility to the banking organization to determine the content of the notification. Such a limited notification requirement will alert the agencies to such incidents without unduly burdening banking organizations with detailed reporting requirements, especially when certain information may not yet be known to the banking organizations.").

[16] *See* Gensler "Working on Team Cyber" Speech.

[17] Presidential Policy Directive -- Critical Infrastructure Security and Resilience (Feb. 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[18] *Id.*; 6 U.S.C. § 665d(c)(5).

markets broadly."[19] However, the responsibility for achieving these objectives is already statutorily assigned to Treasury. Congress, through CIRCIA, further tasked CISA and the respective SRMAs with performing many of these functions to facilitate information sharing and prevent cascading effects. For example, CISA must "publish quarterly unclassified, public reports that describe aggregated, anonymized observations, findings, and recommendations" from covered cyber incident reports.[20] It is also required to provide covered cyber incident reports to "appropriate Sector Risk Management Agencies and other appropriate Federal agencies" within 24 hours.[21]

The Commission's efforts in the cybersecurity space are therefore duplicative, intrusive, and at times contradictory and counterproductive. This is compounded by the Proposal's granular reporting and disclosure requirements. For example, the Proposal would require Covered Entities to publicly disclose detailed information about incidents, such as "whether the covered entity . . . has remediated or is currently remediating the incident"[22] despite acknowledging that releasing too much information could further victimize the entity.[23] This requirement stands in stark contrast to not only investor protection and promoting fair, orderly, and efficient markets—two of the three parts of the Commission's three-part mission that cyber relates to[24]—but also to CIRCIA, which purposefully protects the identity of victims in its quarterly reports,[25] and the Interagency Notification Requirements, which explicitly applies the agencies' confidentiality rules to notifications and any information related to the incident.[26]

Reiterating our comments to the Public Company and Investment Advisers proposals, the Rule 10 Proposal will inevitably force Market Entities to address another layer of investigation by a division of an agency whose expertise and responsibility are not, and should not be, primarily focused on cybersecurity. The associations encourage the Commission to collaborate with and defer to other agencies with statutory authority and deep expertise in this area, so as not to risk requiring duplicative or counterproductive efforts from Market Entities. At a minimum, the Commission should reconcile and harmonize its Proposal with the work of these agencies. This will serve to minimize the impact of the requirements on already finite and burdened cybersecurity resources.

[19] Rule 10 Proposal at 20248.
[20] 6 U.S.C. § 681a(a)(8).
[21] 6 U.S.C. § 681(a)(10)-(b).
[22] Rule 10 Proposal at 20256, Part II.
[23] Rule 10 Proposal at 20321.
[24] *See* Gensler "Working on Team Cyber" speech.
[25] 6 U.S.C. § 681a(a)(8).
[26] Interagency Notification Requirements, 86 Fed. Reg. 66424, 66433.

III. Definitions

A. "Cybersecurity Incident" Should Be Defined More Narrowly. (Request for Comment 10)

The associations recommend the Commission remove "jeopardizes" from the definition of "Cybersecurity Incident" and limit the scope of incidents to those that cause *actual harm*. Removing "jeopardizes" would be in line with state data breach notification laws that generally define a reportable incident as one that "compromises" the security, confidentiality, and integrity of the information; the Interagency Notification Requirements, which defines a "computer-security incident" as an "occurrence that results in *actual harm* to the confidentiality, integrity, or availability" of an information system or its information;[27] and the latest FSB Cyber Lexicon definition of Cyber Incident.[28] Limiting incidents to those that impose an actual harm would avoid the reporting of harmless incidents at the expense of time and resources.

The Commission attempts to downplay just how expansive the definition of cybersecurity incident is by emphasizing the limiting role played by "*jeopardizes*." But the Proposal then provides examples that demonstrate how low the threshold may be. For example, availability would be jeopardized if an unauthorized occurrence "could result in" the inability to access or use an information system or information residing on the system.[29] There are a plethora of occurrences that could trigger this example, most of which would not result in significant, negative impact to the Market Entity. The extremely broad definitions of "information" and "information systems" further exacerbate our concerns with the use of "jeopardizes."

At a minimum, we recommend that the Commission define Cybersecurity Incident as an unauthorized occurrence that "*actually* jeopardizes" the confidentiality, integrity, and availability of an information system. This would align with CIRCIA which defines a "cyber incident" as an occurrence that actually jeopardizes, without lawful authority, the integrity, confidentiality, and availability of an information system or information residing on the system.[30] In addition to harmonization benefits, this qualifier would at least minimize our concerns with the expansive nature of "jeopardizes."

---

[27] 87 Fed. Reg. 13536. As we previously noted, this definition is "substantially similar" to the proposed definition of significant fund cybersecurity incident. *Id.* at n.60. The Proposed Interagency Notification Requirement actually included "potential harm," but the final rule "narrow[ed] the definition . . . by focusing on actual, rather than potential, harm." 86 Fed. Reg. 66429, 66426.

[28] FSB Cyber Lexicon - https://www.fsb.org/wp-content/uploads/P130423-3.pdf (defining "Cyber Incident" as "[a] cyber event that adversely affects the cyber security of an information system or the information the system processes, stores or transmits whether resulting from malicious activity or not.").

[29] Rule 10 Proposal at 20234.

[30] 6 U.S.C. § 681(6).

B. The Definition of "Significant Cybersecurity Incident" Should Require a Higher Threshold. (Request for Comment 17, 18, 19)

The associations encourage the Commission to align the definition of significant cyber incident as closely as possible with existing reporting requirements and frameworks. The current definition is too broad and would potentially cover incidents that do not impact the broader securities market. The proposed definition, specifically the second prong of the definition, would capture incidents that may only impact a single market entity, single customer, or single person that interacts with the market entity, which may not amount to substantial or demonstrable harm to the operations or stability of the U.S. securities market. The current definition does not support the Commission's purported justification for required reporting to assess the impact on the broader U.S. securities markets.[31]

Recognizing the concerns with over-reporting, agencies with statutory authority and deep expertise in cybersecurity have established higher thresholds for reportable incidents than found in this Proposal. For example, CIRCIA requires "demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the people of the United States."[32] Similarly, the Interagency Notification Requirements define a significant computer-security incident as one "that disrupts or degrades, or is reasonably likely to disrupt or degrade, the viability of the banking organization's operations . . . or impact the stability of the financial sector."[33]

The Commission should modify the definition to align with CIRCIA's approach, to require substantial or demonstrable harm to the operations or stability of the Market Entity or the U.S. securities markets as opposed to a single Market Entity or a customer, counterparty, member, registrant, or user of the Market Entity, or to any other person that interacts with the Market Entity. Doing so will allow market entities to focus their attention on incident response and remediation while also ensuring that the SEC can satisfy its objectives. As an alternative, the Commission could adopt the banking agency approach. Otherwise, the SEC risks being overwhelmed with notifications including false positives or insignificant incidents.

The Commission should also provide clarity on what qualifies as a "group of related cybersecurity incidents" as the inclusion of this phrase further broadens the scope of the definition. Recognizing that CIRCIA also incorporates this language, the SEC should coordinate with CISA to ensure a consistent approach. Through this coordination, we recommend that the Commission provide examples and/or temporal or qualitative criteria that provide Market Entities with sufficient clarity on what qualifies as a "group of related cybersecurity incidents."

[31] Rule 10 Proposal.
[32] 6 U.S.C. § 681(9).
[33] Interagency Notification Requirements, 86 Fed. Reg. 66424, 66425 (emphasis added).

IV. Proposed Requirements for Covered Entities

The Commission's proposed requirements for cybersecurity policies and procedures for Covered Entities are overly prescriptive and would require significant resources for implementation. We recommend that the Commission adopt a more flexible, principles-based approach that considers avoiding disproportionate burdens. Additionally, Covered Entities should be able to satisfy cybersecurity policy and procedures requirements by demonstrating compliance with existing cybersecurity frameworks, such as the NIST Cybersecurity Framework, or other Commission requirements, such as Regulation Systems Compliance and Integrity ("Regulation SCI" or "Reg SCI"). The periodic assessment requirements are unduly burdensome and would consume significant time and resources that could be allocated to more effective cybersecurity activities. We recommend that the Commission allow Covered Entities to conduct assessments in accordance with their circumstances and internal planning documents.

A. The Proposal's Cybersecurity Policies and Procedures Requirements, Particularly Regarding Service Providers, Are Unnecessarily Prescriptive. (Request for Comment 22, 23, 36)

The requirements for cybersecurity policies and procedures do not allow for necessary or appropriate flexibility across Covered Entities. At first glance, the Proposal appears to adopt a high-level and flexible approach by referencing policies and procedures that are "reasonably designed" or acknowledging the proposal is not a "one-size-fits-all approach."[34] It even purports to only set forth five minimum elements for the policies and procedures.

Upon closer review, however, the Proposal would impose unreasonably granular requirements on Covered Entities.[35] For example, Covered Entities would be required to identify all service providers that receive, maintain, or process information or are otherwise permitted to access information and then assess how they expose it to cybersecurity risks. This requirement, without qualification, is simply unmanageable and unnecessary—its principal purpose and effect would be to create legal peril, not sensible cyber governance.[36] The Proposal would also require

[34] Rule 10 Proposal at 20239.

[35] The Commission proposed a similar Cyber Risk Management rule in 2022. *See* File No. S7-09-22; RIN 3235-AM89: SEC Proposed Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, and received similar comments from many members of the public. *See,* e.g., letter from Melissa MacGregor, Managing Director & Associate General Counsel, SIFMA, May 9, 2022, at 22, *available at* https://www.sec.gov/comments/s7-09-22/s70922-20128347-291108.pdf. The associations share Commissioner Uyeda's perplexity at "why this proposal does not appear to react to the public comments received on the 2022 proposal." Commissioner Mark T. Uyeda, "Statement on the Proposed Cybersecurity Risk Management Rule for Market Entities," March 15, 2023, *available at* https://www.sec.gov/news/statement/uyeda-statement-enhanced-cybersecurity-031523.

[36] *See* Commissioner H. Peirce, *Statement on Proposed Cybersecurity Rule 10 and Form SCIR* (Mar. 15, 2023), https://www.sec.gov/news/statement/peirce-statement-enhanced-cybersecurity-031523 ("Instead, this proposal demonstrates that our priority is to create even more legal peril for a firm in this situation, legal peril that will distract employees of the firm from mitigating the immediate threat to the firm and its customers as they navigate the aggressive deadlines and open-ended information demands of the Commission.").

policies and procedures "designed to detect, mitigate, and remediate *any* cybersecurity threats and vulnerabilities."[37] This requirement is impractical as entities must assess and remediate vulnerabilities based on their risks. In fact, the Common Vulnerability Scoring System ("CVSS") standard "scores" vulnerabilities because it recognizes that entities must assess impact and prioritize remediation.

Moreover, the Proposal states: "A Covered Entity that implements these requirements of proposed Rule 10 with respect to its SCI systems and indirect SCI systems generally should satisfy the proposed requirements of Regulation SCI that the SCI entity's policies and procedures include a program to manage and oversee third-party providers that provide functionality, support or service, directly or indirectly, for SCI systems and indirect SCI systems."[38] This language implies that there should be consistency between Reg SCI's proposed third-party provider requirements and those proposed under Rule 10.[39] This would impose onerous and impractical requirements on Covered Entities to manage and oversee fourth-party and beyond service providers (i.e., those who indirectly provide functionality, support, or service) under Rule 10 even if Rule 10 itself does not cover the indirect provision of services. The associations recommend that the service provider requirements under Rule 10 remain limited to only those with a direct contractual agreement with the Covered Entity and, as noted in SIFMA's letter on Reg SCI, the "indirectly" should be removed from the Reg SCI provision for clarity and consistency.

The Proposal goes further by enlisting Covered Entities to indirectly regulate service providers. The associations' members recognize and understand their role with respect to the cybersecurity posture of their service providers. However, requiring Covered Entities to renegotiate contracts with service providers to implement and maintain specific practices, as described in the Proposal, is too overreaching. Many of these service providers are not regulated by the SEC and already have mature security programs subject to industry standard audits and certifications such as ISO 27001 or SOC 2. This may negatively impact a Covered Entity's ability to secure contracts with leading and well-established service providers. Service provider oversight should entail a principles-based approach.

The associations recommend that policies and procedures requirements be more principles-based to provide needed flexibility for Covered Entities to address changing threat landscapes and bespoke needs. NIST recently emphasized the value of the "flexible, simple, and easy-to-use-nature" of its Cybersecurity Framework.[40] The Commission's approach should similarly provide

[37] Rule 10 Proposal at 20344 (emphasis added).
[38] Rule 10 Proposal at 20271 (emphasis added).
[39] The associations also note that it is unclear how the use of "service providers" in the Rule 10 proposal differs from the phrase "third party provider" in Reg SCI. We recommend the Commission align these terms across the different rules.
[40] National Institute of Standards and Technology, *NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework* (Jan. 19, 2023),

Covered Entities with genuine flexibility to tailor their policies and procedures "to the nature and scope of the Covered Entity's business and address the Covered Entity's specific cybersecurity risks."[41]

B. The Proposal's Periodic Assessment Requirements Are Unduly Burdensome. (Request for Comment 27, 30, 39, 40)

The Proposal's periodic assessment requirements in Section 242.20(b)(2)(ii) would force Covered Entities to prepare burdensome and bureaucratic written reports. This goes beyond the requirements of the well-established cybersecurity frameworks, such as NIST, which the Commission so often references. In fact, the Commission has concluded, if at least implicitly, that adherence to NIST is inadequate with respect to implementing a cybersecurity and governance framework. Moreover, the Commission accords little to no recognition of the fact that many cyber incidents are effectively responded to, recovered from, and remediated by Covered Entities, and those incidents thus result in manageable or minor adverse impacts.

The proposed requirement to document any cybersecurity incident that occurred since the date of the last report will unnecessarily divert time and resources that would be better allocated to more effective cybersecurity activities. Because the definition of cybersecurity incident is extremely broad, Covered Entities would be required to document incidents that do not and likely will not result in any harm, let alone significant impact, to the Covered Entity.

The SEC should call on Covered Entities to consider their specific need for ongoing assessments. At a minimum, the Commission should not require anything beyond an annual assessment. And instead of imposing granular and prescriptive requirements on the associated written reports, the Proposal should require Covered Entities to conduct and document assessments in accordance with the entity's circumstances and internal planning documents.

C. The Commission Should Provide a Safe Harbor for Covered Entities that Maintain Compliance with Existing Frameworks or Standards. (Request for Comment 25)

The Proposal should deem a Covered Entity's policies and procedures reasonably designed if the Covered Entity maintains compliance with existing cybersecurity frameworks. There are numerous effective and well-established cybersecurity frameworks, standards, best practices, and

---

https://www.nist.gov/system/files/documents/2023/01/19/CSF_2.0_Concept_Paper_01-18-23.pdf, at 5 ("Overwhelmingly, respondents to the RFI made clear that the Framework's key attributes . . . have been beneficial for implementation . . . Reflecting this input, NIST aims to maintain the current level of detail and specificity in CSF 2.0.").

[41] Rule 10 Proposal at 20239.

resources.[42] In fact, the Commission repeatedly references the NIST Cybersecurity Framework throughout this section of the Proposal but does not sufficiently harmonize the Proposal's requirements with that framework. ISO/IEC 27001 is another international standard that provides guidance on "establishing, implementing, maintaining, and continually improving" an information security program[43] and SOC 2 is a framework designed to ensure service providers store and process client data in a secure manner.[44] Rather than developing a new, rigid framework, the Commission should identify existing frameworks and standards, such as the NIST Cybersecurity Framework, ISO/IEC 27001, SOC 2, and the Cyber Risk Institute Profile,[45] that would satisfy the policies and procedures requirements if implemented by a Covered Entity. The existing Regulation SCI recognizes as much, by providing that Regulation SCI policies and procedures "shall be deemed to be reasonably designed if they are consistent with current SCI industry standards, which shall be comprised of information technology practices that are widely available to information technology professionals in the financial sector and issued by an authoritative body that is a U.S. governmental entity or agency, association of U.S. governmental entities or agencies, or widely recognized organization."[46]

V. Notification and Reporting of Significant Cybersecurity Incidents

A. The Proposal's Significant Cybersecurity Incident Reporting Requirements Are Too Prescriptive, Not Aligned to the Commission's Objectives, and May Impede Restoration and Investigations. (Request for Comment 41, 46, 47, 53)

The immediate written electronic notice and proposed Part I of Form SCIR are unnecessarily prescriptive and may impede internal investigations of, and work to recover from, Significant Cybersecurity Incidents. The Proposal does not provide Covered Entities with sufficient time to investigate and respond to the incident before requiring a report. The Commission should therefore align the Proposal with CIRCIA, which provides 72 hours to report an incident at an initial, high level (rather than a premature, detailed report). Additionally, we recommend the Commission modify Part I to not require sensitive and irrelevant (to the SEC) data, such as cyber insurance information, and provide critical exemptions and safe harbors, such as a law enforcement/government agency notification exemption and FOIA protections.[47] The Commission should also provide Covered Entities with reasonable assurances as to its own data

[42] *NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework* (Jan. 19, 2023), https://www.nist.gov/system/files/documents/2023/01/19/CSF_2.0_Concept_Paper_01-18-23.pdf, at 5.
[43] https://ww w.iso.org/standard/27001.
[44] ISO, *What is ISO/IEC 27001?* (last visited May 26, 2023), https://www.iso.org/standard/27001.
[45] Cyber Risk Institute, *The Profile* (last visited May 26, 2023), https://cyberriskinstitute.org/the-profile/.
[46] 17 C.F.R. § 242.1001(a)(4).
[47] *See* SIFMA Comment Letter re "File No. S7-04-22 Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies," 13-14 (Apr. 11, 2022).

security practices and clarity around its plan to protect the EDGAR system, especially considering its original intended use[48] and history as a target for cyber threat actors.[49]

1. *The Immediate Written Electronic Notice Requirement Would Divert Resources Away from Critical Incident Response Efforts.*

The Proposal's requirement that Market Entities provide immediate written electronic notice would impact Covered Entities' ability to effectively respond to significant cybersecurity incidents. Although the required content is relatively minimal, the very act of providing notice will have outsized consequences on a Covered Entity's ability to respond. This is because the Commission intends on using the notice to start assessing the situation. In fact, the Commission envisions "engaging in discussions with the Covered Entity to understand better what steps it is taking to protect its customers, counterparties, members, registrants, or users."[50] In practice, this could further complicate a Covered Entity's incident response efforts as they simultaneously try to handle SEC inquiries.

The initial stages of an incident response require "all-hands-on-deck" to focus immediately and fully on understanding the incident and implementing mitigation and response measures. This is why the Interagency Notification Requirements only require informal, succinct notification by any means chosen by the financial institution within 36 hours after the entity has determined that a notification incident has occurred, and also why CIRCIA provides 72 hours for reporting covered cyber incidents at a high level of generality. The Commission should follow a similar approach and move back the timeframe for immediate written electronic notice to no sooner than 48 hours, and preferably within 72 hours, upon having a reasonable basis to conclude that the incident has occurred or is occurring, in order to allow sufficient time to make such a determination. The Commission should also allow the initial notice to be provided orally, over the telephone, or in writing as the Interagency Notification Requirements. Better aligning the initial notification with these existing reporting regimes would ensure the Commission receives timely notice of true emergent cyber incidents (for example, if email systems or internet access is not operational) while allowing firms to take appropriate steps to investigate, better understand, and mitigate the incident.

[48] In his statements at the open meeting, Commissioner Uyeda noted that EDGAR was initially designed to be public and not include confidential or proprietary information. https://www.youtube.com/watch?v=AWEwk_a3kfQ.
[49] *See* Press Release, SEC, SEC Brings Charges in EDGAR Hacking Case (Jan. 15, 2019), *available at* https://www.sec.gov/news/press-release/2019-1; Chairman J. Clayton, *Statement of Cybersecurity* (Sept. 20, 2017), https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20.
[50] Rule 10 Proposal at 20249.

2. *The Forty-Eight (48) Hour Deadline to Submit Part I of Proposed Form SCIR Is Insufficient Time to Investigate and Report on a Significant Cybersecurity Incident.*

The Commission purports to "provide the Covered Entity time to gather the information"[51] elicited by Part I of proposed Form SCIR, but a 48-hour reporting timeframe would not yield the disclosure the Commission seeks. It would instead require Covered Entities to divert time and resources away from effective incident response. It is also unlikely to elicit the information the Commission seeks and would likely require the Covered Entity to provide updated Part I's in the midst of an incident. This information, particularly about the nature and scope of a cybersecurity incident, is frequently not discernible within 48 hours. In these instances, the entity may still be trying to understand the parameters of the intrusion.

The proposed reporting timeline would unnecessarily burden Covered Entities at critical incident response times and take away resources from managing an incident and actively protecting investors.

The proposed rushed timeline also fails to recognize that completing such a form requires participation and review from multiple stakeholders. In stark contrast to the Interagency Notification Requirements, which does not impose any content requirements,[52] Part I of proposed Form SCIR requires 15 line items, including information about the remediation actions taken, whether and what type of personal information was compromised, and cyber insurance. With few exceptions, all responses to these questions would take time to analyze, draft, and review. The review process alone takes sufficient time given that many stakeholders—including risk and legal functions (and possibly outside counsel), operations functions, executive leadership, and third-party service providers—would need to be involved. As the Commission is aware given the recent Department of the Interior incident, collecting the requisite information from a third-party service provider takes time. The associations appreciate that a few line items allow the entity to check an "Unknown" box, but this does not mitigate the overarching concerns, especially in light of the Proposal's interim reporting requirements. Covered Entities need time to investigate and understand incidents before determining the nature and scope of an incident, let alone whether it is reportable, and to develop the expansive information sought by the Commission.

If the Commission proceeds with a new incident reporting framework, the scope of the requirement must be tailored to the SEC's objectives and the method of reporting must be flexible and efficient. As discussed in SIFMA's Investment Advisers comment,[53] we propose the adoption of a bifurcated notification/reporting regime. Under this system, Covered Entities would provide an initial, abbreviated notification that a significant cyber incident occurred followed by a more

[51] *Id.*

[52] Interagency Notification Requirements, 86 Fed. Reg. 66424, 66432 [defined earlier].

[53] *See* SIFMA Letter to the SEC (Apr. 11, 2022), *available at* https://www.sifma.org/wp-content/uploads/2022/04/SIFMA-and-AMG-Comment-Letter-on-SEC-Cybersecurity-Proposals.pdf.

detailed report (at least several weeks or 30 days later)—which should be a modified version of proposed Form SCIR Part I that would omit much of the Proposal's requirement for excessive and highly sensitive information that would not be relevant for action the SEC could take.

This bifurcated notification/reporting system, triggered upon the "determination" of a significant cybersecurity incident, would achieve the Commission's objectives without overwhelming entities or risking over-notification.

The initial notification should need to be submitted within 72 hours (or 48 hours at the earliest); while the modified Part I should not need to be submitted until after the Covered Entity has had sufficient time to investigate the incident. This would ensure the SEC receives timely notice of an incident while allowing entities to take the necessary steps to understand, contain, and remediate the incident. The subsequent Part I update would provide additional information and analysis for the Commission to assess the incident and associated trends, while minimizing the chance that inaccurate or incomplete information will be provided or that the regulatory requirements will overwhelm an entity's incident response. This approach would also avoid the significant burden of providing regular updates to Part I, as currently envisioned under CIRCIA.

3. *Certain Part I Line Items Are Not Aligned to the Commission's Objectives for Requiring the Information.*

The Commission should modify Part I of Form SCIR to omit sensitive, irrelevant, and non-actionable data. In particular, the Commission should remove its request for remediation, disclosure, and cyber-insurance information because this information is sensitive and not necessary to achieve the Commission's articulated objectives. For example, whether a significant cybersecurity incident is disclosed in accordance with the Rule 10 requirements or a Covered Entity's cyber insurance policy (or lack thereof), as requested in Line Item 14, is irrelevant to the potential impact of the incident or the Covered Entity's response. Line Item 13 (for a Covered Entity that is a carrying or introducing broker-dealer, indicating separately whether it made the required disclosure of Part II of proposed Form SCIR to its customers) specifically seems more like an enforcement trap designed to create legal peril as opposed to a reasonable effort to assess the impact of an incident on the Covered Entity and broader securities market. Additionally, the SEC is not statutorily authorized, nor does it have the analytical capabilities, to take effective action on some of the requested operational information—in contrast to the cyber responsibilities and capabilities of CISA or law enforcement.

As discussed in more detail below, member firms are also hesitant to provide sensitive data, such as ongoing remediation efforts, without understanding the security measures and controls the Commission intends to implement for EDGAR and its repository of information, and without the Commission committing itself publicly to the same cybersecurity standards to which it would hold Covered Entities.

The Commission should modify Part I of Form SCIR to elicit only information that is responsive to its stated objectives and that will not further harm a Covered Entity if leaked.

B. The Commission Should, Where Applicable, Pursue the Information It Seeks Through CISA or the Treasury Department.

Government agencies must collaborate and share elicited information to conduct nation-level incident response and protect critical infrastructure industries while minimizing the burden on victim and compliant entities. Recognizing the importance of this principle, Congress incorporated harmonization and interagency sharing requirements into CIRCIA. The associations recognize that while the scope of CIRCIA is more limited than proposed Rule 10, there would be significant overlap for those firms that would be subject to both requirements and, thus, significant implementation challenges if these requirements are not aligned. We encourage the Commission to refrain from establishing a separate cybersecurity notification regime while the industry awaits the implementation of CIRCIA. If the Commission does proceed, it should establish a requirement that avoids unnecessary duplication, or at minimum, explain and appropriately justify why it believes differing requirements are necessary and appropriate.

CIRCIA establishes multiple mechanisms for the Commission to receive the information it seeks without further burdening Covered Entities already victimized by a cybersecurity incident. First, CISA is tasked with leveraging information gathered about cyber incidents to "enhance the quality and effectiveness of information sharing and coordination efforts" and provide appropriate agencies with "timely, actionable, and anonymized reports."[54] CISA will also be required to "conduct a review of the details surrounding the covered cyber incident" and "identify and disseminate ways to prevent or mitigate similar incidents in the future."[55] Most notably, CISA must "as soon as possible but not later than 24 hours after receiving a covered cyber incident report…make available the information to appropriate Sector Risk Management Agencies [the Treasury Department, here] and other appropriate Federal agencies," as determined by the President.[56]

Each of these mechanisms aligns directly with one of the Commission's stated objectives for its notification and reporting requirements. For example, the Commission states that the information provided through Part I "could be useful in assessing other and future significant cybersecurity incidents" and assist in "identifying patterns and trends."[57] This exact function is already envisioned and assigned to CISA and Treasury, as the SRMA for the financial services sector. Because the Commission is not a SRMA for the financial services sector and may therefore not have the appropriate resources or analytical expertise, it should not seek to duplicate efforts that are more properly the province of CISA and the respective SRMA. Furthermore, the

[54] 6 U.S.C. § 681a(a)(3).
[55] 6 U.S.C. § 681a(a)(6).
[56] 6 U.S.C. § 681a(a)(10)-(b).
[57] Rule 10 Proposal at 20250.

overinvolvement of the SEC with respect to cyber incident reporting could threaten the development of cybersecurity regulatory frameworks that are "complementary to public-private collaboration."[58]

The Commission should instead defer to and seek the information it receives from CISA and/or the Department of the Treasury. Many of the Market Entities the Commission seeks to cover with this Proposal will be subject to CIRCIA.[59] By receiving the information through CISA, the Commission will still be able to achieve its asserted objectives while minimizing the burden imposed on entities attempting to effectively respond to and remediate a significant cybersecurity incident.[60]

C. The Commission Should Consider Exemptions to and Safeguards for Submitting Part I of Proposed Form SCIR.

Reporting a cybersecurity incident to the Commission could result in adverse operational and legal ramifications that the Proposal does not currently account for. The Commission should incorporate exemptions to the notification and reporting requirements for adverse impact from the act of reporting and requests to delay from law enforcement, national security, and other cybersecurity agency equivalents. The Commission should also protect Part I of Form SCIR from Freedom of Information Act ("FOIA") requests and causes of action based solely on the submission of the Form.

Reporting a significant cybersecurity incident, especially considering the security concerns associated with EDGAR, could result in further harm to the Covered Entity or securities markets. For example, an incident may have been caused by a threat actor's exploitation of a zero-day vulnerability.[61] Covered Entities should be afforded the opportunity to coordinate with the vendor of a product or information system with a zero-day vulnerability or exploit prior to submitting Part I to the SEC to avoid broader exploitation. This "responsible disclosure" exception would provide the vendor with an opportunity to develop a patch before the vulnerability or exploit becomes more widely known.[62] Such an exception is especially important given the level of detail requested by the Commission in its current Part I.

---

[58] White House, National Cybersecurity Strategy 8 (Mar. 2023).

[59] CIRCIA applies to "covered entit[ies]" which means an entity in a critical infrastructure sector that satisfies the criteria established by CISA's rulemaking process. 6 U.S.C. § 681.

[60] CIRCIA allows government entities, such as the SEC, to use the information obtained from a covered cyber incident report to regulate, including through an enforcement action, if it "expressly allows entities to submit reports to [CISA] to meet regulatory reporting obligations of the entity." 6 U.S.C. § 681e(a)(5)(A).

[61] NIST, *Zero Day Attack*, Glossary, https://csrc.nist.gov/glossary/term/zero_day_attack#:~:text=An%20attack%20that%20exploits%20a,NISTIR%208011%20Vol.

[62] *See* Coordinated Vulnerability Disclosure Process, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, available at https://www.cisa.gov/coordinated-vulnerability-disclosure-process.

Similarly, the Commission must incorporate a law enforcement/national security/cybersecurity agency exemption into the notification and reporting framework. The Commission acknowledges the importance of cooperation with these agencies but provides no exception for filing Part I of Form SCIR or ability to delay the filing if it would conflict with an ongoing investigation. National security and principles of responsible disclosure (i.e., disclosing the incident publicly only after it has been remediated) dictate the ability to file a disclosure. To the extent the Commission is concerned that the disclosure obligation would be undermined by abusive or excessive invocations of this exemption, the Commission would be reassured that the actual number of government requests and authorizations (or court orders) for delayed public reporting is actually quite low. To confirm the accuracy of this observation, the Commission should consult directly with officials of the Department of Justice, FBI, and CISA to apprise itself of both the critical need for delayed disclosure in appropriate cases, and the rarity of such requests and authorizations. Thus, there should be an exception to filing Part I of Form SCIR for cooperation with law enforcement, other relevant government agencies, as required by court orders, and adverse impact consistent with the standards for "responsible disclosure" of security vulnerabilities.

These exceptions may be less necessary if the Commission adopts our proposed bifurcated notification/reporting framework. Although the Commission pledges to keep Part I of Form SCIR confidential, the associations remain concerned as to the SEC's data security practices and the security of the EDGAR system. However, if the Commission only requires an initial, abbreviated notification followed by a more detailed report after a sufficient time for investigation, then our concerns associated with detailed, sensitive data leaking are less salient.

Reporting a cybersecurity incident unfortunately may expose entities to unwarranted reputational and legal harm. Covered Entities should be confident in the confidentiality of any submission in order to promote sharing information with government entities. Recognizing this, CIRCIA incorporated liability protections designed to incentivize proactive reporting and transparency.[63]

The Commission should adopt liability protections similar to those in CIRCIA with respect to notification and reporting of significant cybersecurity incidents. In particular, it should explicitly state that Part I of Form SCIR and any other reported information is exempt from FOIA requests and any other freedom-of-information laws that could potentially compel public disclosure. The Commission should also explicitly safeguard Part I of Form SCIR or any other reported information from serving as the sole basis of any cause of action before any tribunal. This would keep the evaluation of a Covered Entity's cybersecurity safeguards and programs within the regulatory environment.

[63] 6 U.S.C. § 681e(b)-(c).

The associations also recommend that the Commission clarify that proposed Form SCIR allow for affiliated firms to file one form, and that there should be harmonization between Part I of proposed Form SCIR and Form ADV-C under the Investment Advisers Act. This would minimize the burden and confusion associated with completing Part I.

Providing these exemptions and safeguards would also align the Proposal with other reporting frameworks, most notably CIRCIA, and minimize the existing concerns of the associations' members with the Commission's data security practices and EDGAR's cybersecurity risk profile.

D. Reporting the Level of Detail Required by Part I May Have Significant Detrimental Cybersecurity Implications.

We appreciate and support the Commission's decision to keep Part I of Form SCIR confidential. However, without more insight into the cybersecurity policies and procedures and plans for protecting the EDGAR system, we have legitimate concerns about providing sensitive cybersecurity data to the Commission. The Commission even recognizes the "sensitive nature of the [requested] information and the fact that threat actors could potentially use it to cause more harm."[64] Yet, it fails to provide Covered Entities with assurances as to its own data security practices and, in particular, the cybersecurity of the EDGAR system.

Providing and storing the requested information on EDGAR exposes Market Entities, especially Covered Entities, to additional risk. These concerns are not based on mere hypotheticals. A November 2022 Independent Evaluation noted that the SEC's "information security program did not meet [the requisite level] and, therefore, was not effective."[65] And, as the Commission is of course aware, at least two threat actors compromised the EDGAR system from May to October 2016 in order to extract non-public information.[66] This resulted in the Department of Justice bringing charges against nine individuals associated with the scheme.[67] Housing the type of information sought in Part I of Form SCIR increases the risk of cyber criminals or nation state actors targeting EDGAR for Non-Public Information ("NPI").

---

[64] Rule 10 Proposal at 20249.

[65] Office of Inspector General Office of Audits, Fiscal Year 2022 Independent Evaluation of the SEC's Implementation of the Federal Information Security Modernization Act of 2014 at ii (Nov. 15, 2022), https://www.sec.gov/files/fy-2022-independent-evaluation-sec-implementation-fisma-2014-report-no-574.pdf. As this report illustrates, the Commission's own information security record does not reach the levels it expects of its registrants. For example, in the areas of "Data Protection and Privacy" and "Information Security Continuously Monitoring," the Commission reaches only Level 3 "Consistently Implemented–Policies and procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking." *Id.* at ii, 2. For "Configuration Management" and "Identity and Access Management," the audit finds that the Commission reaches only Level 2 (has defined but not consistently implemented). *Id.*

[66] United States Government Accountability Office, *Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges*, GAO-19-384 (July 25, 2019).

[67] *Id.*


As expressed in our Investment Advisers comment, if the Commission is unable to adequately ensure that information will be properly safeguarded, we recommend that Covered Entities have the option to maintain their own cyber records—in a federated system that is not a high-value target for threat actors—and permit the Commission to examine that information onsite.

VI. Disclosure and Incident Reporting Requirements

A. The Public Disclosures of Cybersecurity Risks and Incidents Required by Part II of Form SCIR Provide Information to Threat Actors, Do Not Protect Investors, and Could Inappropriately Alarm Investors. (Request for Comment 55 and 56)

The Proposal calls for public disclosures of considerably too much, too sensitive, highly subjective information, at premature points in time, without explaining how information relating to a public disclosure will further the Commission's objectives. The Proposal would require the Covered Entity to provide in Part II of proposed Form SCIR a "summary" description of the cybersecurity risks that could materially affect its business and operations and a "summary" description of each significant cybersecurity incident that occurred during the current or previous calendar year. However, even that summary information required by Part II of Form SCIR would benefit cyber attackers more than it would investors. Requiring the Covered Entity to disclose ongoing significant cybersecurity incidents, effects on the Covered Entity's operations, and whether it has remediated or is currently remediating the incident presents an opportunity for threat actors. Public disclosures may make the impact of incident worse by giving malicious actors insight and intelligence into vulnerabilities within the victimized company. Additionally, public disclosures could unduly alarm investors, and thereby misleadingly disrupt market stability and unnecessarily lead to a lack of confidence in financial institutions or the financial system.

We recommend the Commission not move forward with the public disclosure requirements of Part II of Form SCIR as proposed, for the reasons outlined in this letter. If the Commission nonetheless decides to move forward, it must adopt a more flexible approach to disclosure that respects customer privacy and other privacy regulations and does not enable other threat actors to continue or launch new attacks—Covered Entities should only publicly disclose information after the incident has been fully investigated and remediated, when the Covered Entity may have a more accurate understanding of and judgment about the "significance" of an incident.

Rushed public disclosures deny the Covered Entity proper time to assess the impact of the incident or successfully manage and recover from the incident. While the associations appreciate the importance of providing greater transparency, the Proposal is antithetical to the precepts of "responsible disclosure." Responsible disclosure holds that newly discovered vulnerabilities

should be disclosed only after a patch or remediation is developed.[68] Discovering a defect within an IT infrastructure, identifying the vulnerability associated with the defect, and creating a solution to that vulnerability takes time.

The Commission's public disclosure obligations come into direct conflict with this doctrine. It is not unrealistic to imagine a scenario where the Proposal's public disclosure requirements would prompt a Covered Entity to disclose a vulnerability before having time to fix the defect, leading to a malicious actor's opportunity to exploit the vulnerability.[69] Additionally, the sophistication of cybercriminals and their resources could create a domino effect whereby an exploitation from a rushed disclosure of one Covered Entity without a patch for the vulnerability leads to exploitations of several Covered Entities who share a similar vulnerability. As the Commission itself recognizes, a breach at one Market Entity may be exploited and serve as a means of compromising another Market Entity.[70] Based on implementation of necessary or appropriate remediation, recovery and resilience efforts, an incident that could not be ruled out as potentially "significant" in the heat of initial incident response could indeed be characterized as more routine than extreme after greater perspective can be applied.

Moreover, the requirements to file premature public disclosures would have the effect of diverting resources from incident response to complying with collateral legal requirements. While the Association recognizes the importance of legal rules to protect investors and markets, the Commission's current Proposal mandates excessive disclosure irrespective of the best interests of investors and markets. This Proposal's bureaucratic overreach may lay inadvertent administrative traps for Covered Entities and expose them to unwarranted litigation and enforcement risks rather than helping Covered Entities to respond and recover from cybersecurity incidents—which would better protect investors and markets as opposed to over-detailed and potentially unduly concerning public disclosures. It is worth noting that the SEC's vendor for human resources information technology and services suffered a cybersecurity incident between January 12, 2023, and January 18, 2023, that led to unauthorized access to PII. The notification to affected personnel on behalf of the SEC did not occur until May 16, 2023—more than four months after the incident. The associations believe it is inconsistent for the Commission to demand prompt and near real-time disclosures by Covered Entities to their customers when the Commission's own practice allows for such disclosures to be made four months after an incident. It is also worth noting that allowing sufficient time for public disclosure, as in the case of the incident involving the SEC's vendor, the

[68] Sasha Hondagneu-Messner, Steve McInerney, and Alan Charles Raul, *'Cyclops Blink' Shows Why the SEC's Proposed Cybersecurity Disclosure Rule Could Undermine the Nation's Cybersecurity*, (Aug. 30, 2022, 8:01 AM), https://www.lawfareblog.com/cyclops-blink-shows-why-secs-proposed-cybersecurity-disclosure-rule-could-undermine-nations.

[69] *See* Cyber Safety Review Board, *Review of the December 2021 Log4j Event* at iv (July 11, 2022), https://www.cisa.gov/sites/default/files/publications/CSRB-Report-on-Log4-July-11-2022_508.pdf ("Such a disclosure of a significant vulnerability in any widely used piece of software immediately triggers a race between defense and offense: a race to apply upgrades before threat actors exploit vulnerable systems.").

[70] Rule 10 Proposal at 20284.

communication to the affected personnel was able to provide appropriate context of the incident and any attendant harm and allow the recipient to properly assess the impact of the incident. The requirements under proposed Rule 10 would impose such short deadlines that Covered Entities under the SEC's jurisdiction would not be afforded a similar opportunity.

B. The Commission Should Allow Delayed Disclosures and Updates for Coordination with Law Enforcement and for Cybersecurity and National Security Purposes. (Request for Comment 66)

The associations support a revision to Part II of proposed Form SCIR to allow the Covered Entity to delay publicly disclosing a significant security incident or an update where the Attorney General requests such a delay. In the Public Companies Proposal, the Commission conceded that "a delay in reporting may facilitate law enforcement investigations aimed at apprehending the perpetrators of the cybersecurity incident and prevent future cybersecurity incidents."[71] While the Commission declined to follow its own compelling observation in the Public Companies Proposal, it does propose to allow a sliver of a "national security" exception in this Proposal. *However, allowing delay only on the Attorney General's determination is unreasonably narrow and incongruously conflates national security with law enforcement*. As discussed by President Biden in his Executive Order on Improving the Nation's Cybersecurity, cybersecurity requires more than government action.[72] It requires a collaboration between the public and private sectors to successfully function. Even within such collaboration, the Commission must leave room for the Covered Entity to make its own determination that disclosure of a cybersecurity incident on Part II of proposed Form SCIR may serve as a roadmap for malicious actors.

Reg SCI, for example, authorizes entities to make such determinations. In that rule, the SEC allows for delayed public disclosures if the SCI Entity "determines that dissemination of such information would likely compromise the security of the SCI Entity . . . and documents the reason for such determination."[73] Additionally, Attorney General determinations may take months on end, but an organization assessing a national security risk could happen much faster. National security risk determinations must expand further than the Attorney General to lessen the risk of malicious actors preying on any infrastructure vulnerabilities. The associations encourage the Commission to expand its Attorney General exception to include cybersecurity agencies, compliance with court orders that may preclude public disclosures, and cooperation with law enforcement.

Furthermore, public disclosures could also disrupt the ability of other government agencies to perform their investigatory duties in responding to cybersecurity incidents. As former SEC Chairman Jay Clayton stated, "effective interagency coordination facilitates the identification,

[71] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 23 (Mar. 9, 2022), https://www.sec.gov/rules/proposed/2022/33-11038.pdf.
[72] Executive Order of the President, *Improving Nation's Cybersecurity*, 86 Fed. Reg. 26633 (May 17, 2021).
[73] 17 C.F.R. § 242.1002(c)(2) (2014).

mitigation and remediation of broad and potentially systemic cybersecurity risks."[74] Government agencies such as CISA and the FBI employ a purposeful approach in responding to cybersecurity incidents by providing assistance to the impacted entities, analyzing the potential impact of the technology infrastructure, and investigating those responsible for perpetrating the incident. And as Chairman Gary Gensler noted, while the SEC is an important player, the FBI and CISA are captains of Team Cyber.[75] This process requires collaboration and mutual engagement to assure the most effective cybersecurity incident response. In contrast, requiring Covered Entities to focus prematurely on SEC-required public disclosures will impede collaboration with other government agencies involved in responding to cybersecurity incidents. This is especially true in the event that such a cybersecurity incident has not been remediated. In these instances, it would be more advantageous for Covered Entities to focus their efforts alongside CISA and the FBI to remediate vulnerabilities rather than filing reports that will not be relevant to investigation or remediation.

The Commission itself recognizes the value of coordinated efforts with governmental entities in addressing cybersecurity matters through its role within the Financial and Banking Information Infrastructure Committee ("FBIIC") as well as the Financial Services Sector Coordinating Council ("FSSCC").[76] Though both committees take a proactive approach to cybersecurity risk management, they also recognize the value in collaborative efforts between the private sector and government. The Commission should similarly extend this collaborative approach to its Rule 10 disclosure requirements. ***The Commission should allow delayed disclosures where such a disclosure could impede a government agency's ability to perform its investigatory duties.*** If the ultimate goal of the disclosure requirement is to help investors, the Commission should allow for Covered Entities to prioritize agency collaboration.

Additionally, Part II of the proposed Form SCIR creates an unwarranted public catalogue of supposed cybersecurity failings of Market Entities that is not justified by the SEC's objective to protect markets and investors. Annual cybersecurity reporting would unduly alarm the marketplace. The Commission neither addresses this reality nor accounts for the extensive legal review necessary for such public disclosures. Numerous unnecessary legal—as well as cybersecurity—risks arise from requiring Market Entities to disclose highly sensitive information about their technology infrastructure without any explanation from the Commission on how it plans to use and protect that information.

The Commission's proposal that Part II disclosures must be posted on a firm's website and incorporated into the account opening process is excessive. The disclosures are already available on EDGAR, and we are not aware of any examples of other regulators requiring disclosure of cybersecurity incidents as part of the required disclosures to an individual when opening an account. While we agree that cybersecurity is important, the prescriptive and redundant method

[74] *See* Chairman J. Clayton, *Statement of Cybersecurity* (Sept. 20, 2017), https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20.
[75] *See* Gensler "Working on Team Cyber" Speech.
[76] *Id.*

for disseminating Part II disclosures serves only to stack administrative burdens on firms and customers when opening an account. At most, a firm should only be required to state that information concerning its cybersecurity is available on EDGAR (or the firm's website).

We are concerned about the negative implications of delivering Part II to customers because the SEC has provided no analysis or consideration of how customers or investors may react to the disclosure. In contrast, when it developed Form CRS, the Commission was very deliberate and thoughtful about how investors would perceive and understand disclosures—and undertook considerable research and analysis concerning Form CRS perception. No such careful assessment at all has been conducted or factored into the Commission's proposal to require public disclosure in Part II of Form SCIR, or as part of the account opening process. Yet, the Commission is requiring public disclosure as a part of the account opening materials without any commensurate analysis and justification.

Routinely, when the Commission has concerns about whether information was useful for investors, it conducts an analysis. However, here, for cybersecurity, it is forgoing any such analysis. Instead, it is asserting (and merely presuming) what it believes is necessary and pertinent information for investors, without any understanding of how such information might be misunderstood or potentially used to unfairly tarnish a company. Without proper context, federally mandated public disclosures can be misleading and easily improperly exploited by others to damage a company's reputation.[77]

VII. The Commission Should Modify the Requirements for Non-Covered Broker-Dealers. (Request for Comment 75)

We support the position that proposed Rule 10 should not be modified to specify certain minimum elements that would need to be included in a Non-Covered Broker-Dealer's policies and procedures. As the Commission notes, Non-Covered Broker-Dealers have limited business activities and, often, their information systems can be confined to smart phones and personal computers.[78] Additionally, such entities may have different threat concerns. Modification of minimum elements would create an administrative burden and lead to Non-Covered Broker-Dealers designing policies and procedures for purposes of SEC reporting rather than broader

[77] For example, when customers sued Scottrade following a data breach for hosting insufficient technological infrastructure, the Eighth Circuit concluded that "the implied premise that because data was hacked Scottrade's protections must have been inadequate is a 'naked assertion devoid of further factual enhancement.'" *Kuhns v. Scottrade, Inc.*, 868 F.3d 711, 717 (8th Cir. 2017). Additionally, as the FTC has noted, "the mere fact that a breach occurred does not mean that a company has violated the law." *See* Federal Trade Commission, *Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime* (Feb. 4, 2014), https://www.ftc.gov/system/files/documents/public_statements/prepared-statement-federal-trade-commission-privacy-digital-age-preventing-data-breaches-combating/140204datasecuritycybercrime.pdf. Therefore, mandating public disclosures, without proper context, may lead investors to make unfounded assertions that result in reputational damage for a covered entity.

[78] Rule 10 Proposal at 20262.

compliance goals based on risk specific to the organization. The Commission should allow Non-Covered Broker Dealers the flexibility to choose their relevant framework without the Commission re-inventing the cyber wheel. ***We also reiterate our recommendation that the Commission modify the immediate electronic written notice requirement to provide 72 hours for initial notification.***

VIII. Substituted Compliance Should Be Available. (Request For Comment 87-89)

We appreciate that the Proposal opens a path to substituted compliance through the amendment of Rule 3a71-6. We believe that, when dealing with non-U.S. security-based swap entities, making substituted compliance potentially available is the right policy decision because it would allow for an outcome-based determination of whether a particular home country law has comparable cyber security requirements. Lack of substituted compliance would create costly and burdensome hurdles for financial institutions, which would be forced to comply with a wide range of duplicative regulations.

In addition, when finalizing its rule and conformance timeline, we urge the Commission to be mindful that similar regulatory requirements have already been adopted elsewhere (e.g., the Digital Operational Resilience Act ("DORA") – Regulation (EU) 2022/2554), albeit with varying conformance periods (e.g., DORA's conformance period ends in January 2025). In those cases, the Commission should enable substituted compliance applications to be processed, and substituted compliance determinations to be made, on the basis of the finalized home country rules regardless of a conformance date that may be in the near future. Failing this, substituted compliance relief could be delayed, forcing non-U.S. SBS entities to establish a temporary and redundant compliance regime for the Commission's rule while awaiting the outcome of the substituted compliance determination.

We appreciate that the Proposal also requests feedback on the appropriateness of the factors employed by Rule 3a71-6. These factors, as proposed to be amended, are not the right ones for the Commission to consider in making a substituted compliance determination in connection with Proposed Rule 10, Form SCIR, and the related recordkeeping requirements. The factors identified in Rule 3a71-6(d)(1) apply to business conduct and supervision. Cyber risk management, however, is an important aspect of compliance and is distinct from business conduct and supervision. Consequently, cyber risk management should be given its own section. Furthermore, the new section should state that the primary factor to be considered in assessing whether substituted compliance should be granted to a foreign regulatory system is whether the system contains cybersecurity risk management policy and procedure requirements and notice provisions that achieve regulatory outcomes that are comparable to the regulatory outcomes associated with those requirements in the United States. The Commission should also clarify that following a substituted compliance determination, non-U.S. firms in comparable jurisdictions are permitted to submit their home country disclosure forms (as opposed to Form SCIR), and further allow non-U.S. firms to adhere to home country notification timelines. For prudentially regulated SBSD's, the Commission should also clarify Proposed Rule 10 would only apply to their SBS business.

Even with substituted compliance, however, it would be overly complex to apply the requirements of incident notification at an entity level for non-U.S. SBSDs. Therefore, we recommend that the Commission exclude from required notification those incidents that are solely related to non-U.S. transactions but allow reporting if desired. Scoping in incidents related solely to non-U.S. transactions may result in the Commission receiving information that is not relevant to U.S. securities markets. In addition to substituted compliance, this would address any possible additional jurisdictional and scoping issues (i.e., potential conflict or duplication with foreign regimes).

IX. Market Entities Subject to Reg SCI, Regulation S-P, Regulation ATS, and Regulation S-ID

A. The Proposal Should Simplify Its Prescriptive Policies and Procedures so that Market Entities May Comply with All Applicable Rules and Regulations. (Request for Comment 91)

The Commission should significantly simplify its prescriptive requirements so that Market Entities can develop and implement standards that allow them to comply with all SEC rules that apply to them without having to address myriad sets of cyber rules addressing the same risks differently. The Proposal highlights the overlap between proposed Rule 10, Proposed Amendments to Regulation S-P, and the Proposed Amendments to Regulation SCI, but rather than recognizing that overlapping requirements (policies and procedure requirements, disposal rule requirements, security incident disclosure, etc.) are detrimental to implementing a robust cybersecurity infrastructure, the Proposal blithely suggests it would not be unreasonably costly to Market Entities to implement all requirements. The associations do not agree with that position. It is incumbent on the SEC to work out the overlaps and reconcile and rationalize them.

As described further below, the cost to implement the various policies and procedures of cybersecurity requirements is exorbitant. In many cases, Market Entities have already complied with requirements imposed by CISA and other agencies and organizations gathering cybersecurity information, as well as current SCI rules concerning policies and procedures addressing cybersecurity. The associations fear that requiring too many overlapping and overly prescriptive rules diverts resources and focus away from compliance with and implementation of appropriate cybersecurity policies and procedures for Market Entities. Under proposed Rule 10, however, these resources would instead be devoted to the implementation of policies and procedures necessary to avoid enforcement and litigation. In reconsidering the policy and procedure requirements, the Commission should focus on providing simplicity, which will ultimately promote effective cybersecurity policies and procedures.


B. The Proposal Should Exempt SCI Systems from the Policies and Procedures Requirements. (Request for Comment 92)

To promote efficiency, the Commission should modify proposed Rule 10 to exempt current SCI Entities under Reg SCI from its policies and procedures requirements. The Proposed Amendments to Reg SCI sufficiently address requirements of SCI Entities.[79] Otherwise, any duplicative requirements of SCI systems by proposed Rule 10 would result in unnecessary and unjustified incremental costs for Market Entities. Additionally, the Commission outlined very detailed obligations and requirements of SCI Entities in Proposed Amendment to Reg SCI. Nothing within proposed Rule 10 significantly aids in modernizing and enhancing the SEC's oversight over the technological infrastructure of SCI Entities. In fact, SCI Entities often adhere to standards, frameworks, and processes issued by publications such as NIST, the Federal Financial Institutions Examination Council ("FFIEC"), and the Institute of Internal Auditors. If proposed Rule 10 does not provide for more protection of technological infrastructures than the Proposed Amendments to Regulation SCI and the above-mentioned standards, its requirements for SCI Entities serves only to burden Market Entities with duplicative and costly implementation.

C. Duplication of Notification and Reporting Requirements with Proposed Amendments to Reg SCI. (Request for Comment 94)

The Commission should also modify the immediate notification and reporting requirements of proposed Rule 10 for Covered Entities because they are duplicative of the Proposed Amendments to Regulation SCI and thus impose unnecessary costs on Covered Entities. If the Commission adopts a notification and reporting requirement of Market Entities, it is imperative that the requirement is tailored, and the method of reporting is efficient. It would be burdensome for Covered Entities, experiencing a cyber incident, to juggle multiple notification requirements, including potentially reporting to more than one place at the Commission. The current proposal, which requires reporting to multiple divisions within the Commission, would distract an organization from focusing on protecting customers in a crisis and restoring the confidentiality, availability, and integrity of information systems. Multiple, repetitive reporting requirements would inevitably tend to result in increased, frivolous enforcement actions as Covered Entities would find themselves subjected to enforcement for failing to report the same information to different divisions in the Commission.

Our members strongly believe that a more coordinated interaction between proposed Rule 10 and Proposed Amendments to Regulation SCI would achieve the Commission's goal of enhancing oversight of the Covered Entity's technology infrastructure without adding to an already

[79] Under the current Reg SCI, an SCI Entity is "an SCI self-regulatory organization, SCI alternative trading system, plan processor, or exempt clearing agency subject to ARP." Regulation SCI. Under the Proposed Amendments to SCI, an SCI Entity is "an SCI self-regulatory organization, SCI alternative trading system, plan processor, exempt clearing agency, SCI competing consolidator, SCI broker-dealer, or registered security-based swap data repository." Proposed Amendments to Regulation SCI at 23268.

complex landscape of overlapping cybersecurity regulations and detracting from critical security operations.

X. The Proposal Is Too Costly and Does Not Adequately Promote Efficiency, Competition, and Capital Formation

A. The Economic Burden on Market Entities Is Overly Burdensome. (Request for Comment 98 and 99)

The associations do not believe the estimated compliance costs for Market Entities to adopt cybersecurity policies and procedures, along with reviewing annually and drafting a summary report, are reasonable. As the Commission notes throughout the Proposal, implementation of proposed Rule 10 should be considered in light of the inevitable duplication with regulations and responsibilities of other agencies that have more directly relevant and specialized expertise with respect to cybersecurity issues. The Commission takes the position that a Market Entity's chosen level of cybersecurity protection may present an underinvestment relative to the optimal level necessary to maintain a secure technical infrastructure.[80] Yet the Commission provides no persuasive evidence for this position. In fact, the contrary is true. For instance, many of the associations' members have aligned with and heavily invested in implementing the NIST Cybersecurity Framework. This cybersecurity framework is well regarded throughout various sectors and many financial organizations, such as the FSSCC, modeled its cybersecurity standards—now referred to as the Cyber Risk Institute Profile—on the NIST Framework.[81] Unfortunately, the Proposal fails to sufficiently align with the NIST Framework and requires much more prescriptive requirements, thereby imposing deadweight costs on Market Entities.

The Proposal significantly underestimates the costs to comply with proposed Rule 10, particularly the cost to adopt and implement policies and procedures. The Proposal estimates that the internal initial burden hours for adopting and implementing policies and procedures is 50 hours.[82] In the experience and considered judgment of the associations' members, it would in reality take significantly longer to do so. Similarly, the notion that this would be done by one compliance attorney and an assistant general counsel ignores the way that business operates in practice, including that these attorneys would have supervisors and internal clients who need to be read in and oversee the work.

Additionally, because no single person within a Covered Entity has all the requisite knowledge to develop and implement policies and procedures, this work would require extensive coordination with various departments and separate business units, including legal, compliance, vendor management, and information technology. The Proposal also estimates that outside hourly

[80] Rule 10 Proposal at 20281.
[81] Cyber Risk Institute, *The Profile* (last visited May 26, 2023), https://cyberriskinstitute.org/the-profile/.
[82] Rule 10 Proposal at 20328.

legal expenses would cost $496 per hour,[83] which drastically underestimates the actual cost of outside counsel qualified to advise on important cybersecurity matters. The Proposals' estimate also fails to take into account the complicated process required to review and amend policies and procedures, which involves education, review, edits, signoffs, and implementation.

Furthermore, to avoid duplication and compliance with other overlapping requirements, these requirements must be understood in relation to other similar rules, which makes it complicated to reconcile these competing frameworks into a workable set of policies and procedures. A Covered Entity cannot develop policies and procedures to comply with proposed Rule 10 in isolation, but rather must weave the proposed Rule 10 requirements into existing policies and procedures. Moreover, the Proposal would require the drafters of these policies and procedures to undergo extensive training to understand the requirements and would require the employees subject to the policies and procedures to be aware of them, all of which require training and education costs that are not captured in the Proposal's estimated costs.

The Proposal also does not capture the costs associated with making a determination of a significant cybersecurity incident and providing immediate notice to the SEC or filling out Parts I and II of Form SCIR. The determination of whether there has been a "significant cybersecurity incident" may involve the Chief Information Security Officer ("CISO") consulting with other senior business leaders. The idea in the Proposal that this decision is made by a systems analyst, compliance manager, and general counsel is unrealistic. This determination has significant consequences, including whether to notify customers, and requires executive-level decision making. Additionally, filling out Form SCIR has the potential for significant legal liability, and must be completed at higher levels, in coordination with those who must dedicate time to determine all the answers. Moreover, because Part II is public, completing it requires extensive legal review and editing. Finally, the Proposal asserts that the costs of implementation is overshadowed by the benefits of proposed Rule 10 because cybersecurity risks of Market Entities often go unaddressed.[84] We strongly disagree with this position. Certain types of Market Entities are dually registered with the CFTC; are subject to the requirements of prudential regulators such as the FDIC, Federal Reserve Board, and the OCC; and will soon be subject to the requirements of CIRCIA. Between those various rules and regulators, a Market Entity's ability to conceal a cybersecurity risk or incident is low. This Proposal would require significant additional costs while providing minimal incremental benefit.

B. The Paperwork Reduction Act Analysis Does Not Represent the True Burden of Implementation of the Proposal

In light of these miscalculations, the Proposal's Paperwork Reduction Act analysis is also severely flawed. The Paperwork Reduction Act of 1995 ("PRA") requires that agencies justify the collection of information from the public by establishing the need and the intended use of the

[83] *Id.*
[84] Rule 10 Proposal at 20285.

information and estimating the burden imposed on the public in complying with the collection.[85] Additionally, in determining the burden, the law requires agencies to solicit public input on information collections to validate their estimates.[86] The associations do not believe the Commission performed its statutory obligation and due diligence in assessing the realistic burden associated with implementation of the Proposal.

In 2018, the U.S. Government Accountability Office ("GAO") performed a survey assessing the public input solicitation practices of four government agencies.[87] The results uncovered insufficient attempts of public solicitation of opinions on proposed rules, leading the GAO to recommend Congress amend the PRA to more explicitly require federal agencies to consult with potential respondents on each information collection beyond the publication of *Federal Register* notices using efficient and effective consultation methods.[88] Though the SEC was not one of the four government agencies surveyed, the Commission's solicitation practices seem to mirror the inadequate efforts of those agencies involved in the study. As mentioned, firms underwent a costly undertaking in implementing cybersecurity frameworks such as NIST, and as firms have mentioned in prior public comments addressing the Commission's proposals on cybersecurity, implementation of new SEC regulations will result in more costly undertakings far exceeding what the Commission has estimated. Because of the manifest inaccuracy of its PRA analysis, the SEC should reconsider the need for, and proceed only if it can sufficiently justify, the onerous (and in many cases, unnecessary or counter-productive) paperwork burdens it is imposing on Market Entities.

C. Portions of the Proposal, as Drafted, Would Negatively Affect Efficiency, Competition, and Capital Formation. (Request for Comment 128 and 129)

The associations appreciate the Commission's attention to cybersecurity, and fully agree that better policies and procedures could be beneficial. However, the disharmonious nature of the Proposal with other SEC cybersecurity regulations creates more cost than benefits for Market Entities. As it stands now, several aspects of the Proposal do not promote efficiency, as the Commission is required to consider under Section 3(f) of the Exchange Act.[89]

Our members strongly believe that many of the cost discussions included highly subjective, qualitative data, which is not an accurate reflection of the true cost associated with implementation of the requirements set forth in the Proposal. The Commission rests on assumptions about supposed underinvestment in cybersecurity protection. However, this conjecture discounts the

[85] Paperwork Reduction Act, 44 U.S.C. § 3501
[86] *Id.*
[87] U.S. Government Accountability Office, Paperwork Reduction Act: Agencies Could Better Leverage Review Processes and Public Outreach to Improve Burden Estimates (July 11, 2018), https://www.gao.gov/products/gao-18-381#:~:text=The%20law%20requires%20agencies%20to,public%20outreach%20to%20improve%20estimates.
[88] *Id.*
[89] Exchange Act Section 3(f), 15 U.S.C. § 78c(f).

reality that many Covered Entities have implemented cybersecurity frameworks and standards set forth by NIST, CISA, and banking agencies—and invest very significant resources to implement those standards. While we recognize the significance of securing the financial sector from devastating cyberattacks, we encourage the Commission to consider ways to work together as "Team Cyber" with cybersecurity agencies like CISA to achieve its intended goals rather than creating new, overly prescriptive requirements for Covered Entities. Moreover, in considering public disclosures, the Commission should also bear in mind the very real risk that too many, too detailed, and too early disclosures may be ignored by the marketplace at best, or unduly confuse or alarm it at worst, while also benefiting the bad actors in this space.

***

The associations appreciate the Commission's attention to cybersecurity and absolutely agree with the Commission regarding the importance of sound cybersecurity practices within the financial sector in order to decrease cybersecurity risk from threat actors. However, we respectfully submit the Proposal contains too many overly prescriptive, duplicative, and burdensome requirements on Covered Entities. The Commission should focus on harmonization among the various proposed rules, simplify requirements within the proposals, and design proposals that protect against cyberthreats without creating enforcement and litigation traps.

Accordingly, we respectfully urge that the Commission should use a revised notice of proposed rulemaking in line with harmonization and simplicity rather than proceed to a final rule. If you have any questions or would like to discuss these comments further, please reach out to Melissa Macgregor at mmacgregor@sifma.org.

Sincerely,

Securities Industry and Financial Markets Association
Bank Policy Institute
Institute of International Bankers
American Bankers Association

Cc: The Hon. Gary Gensler, Chair
The Hon. Hester M. Peirce, Commissioner
The Hon. Caroline A. Crenshaw, Commissioner
The Hon. Mark T. Uyeda, Commissioner
The Hon. Jamie Lizárraga, Commissioner
Dr. Haoxiang Zhu, Director, Division of Trading and Markets

Jen Easterly, Director, CISA
Eric Goldstein, Executive Assistant Director for Cybersecurity, CISA


Graham Steele, Assistant Secretary for Financial Institutions, U.S. Department of the Treasury

Todd Conklin, Deputy Assistant Secretary – Cybersecurity and Critical Infrastructure Protection, U.S. Department of the Treasury

Brian Peretti, Director, Domestic and International Cybersecurity Policy, U.S. Department of the Treasury

Christopher Wray, Director, FBI

Bryan Vorndran, Assistant Director, Cyber Division, FBI

Richard Revesz, Administrator, Office of Information and Regulatory Affairs, US Office for Management and Budget

James J. Halpert, General Counsel, Office of the National Cyber Director

Alan Charles Raul, Sidley Austin LLP
Andrew P. Blake, Sidley Austin LLP


Appendix A – Signatory Associations

The **Securities Industry and Financial Markets Association ("SIFMA")** is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets. On behalf of our industry's one million employees, we advocate on legislation, regulation and business policy affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association ("GFMA").

SIFMA Contact: Melissa MacGregor, Deputy General Counsel and Corporate Secretary

The **Bank Policy Institute ("BPI")** is a nonpartisan group representing the nation's leading banks. BPI members include universal banks, regional banks, and the major foreign banks doing business in the United States. Collectively, BPI members hold $10.7 trillion in deposits in the United States; make 68% of all loans, including trillions of dollars in funding for small businesses and household mortgages, credit cards, and auto loans; employ nearly two million Americans and serve as a principal engine for the nation's financial innovation and economic growth. Business, Innovation, Technology and Security ("BITS"), BPI's technology policy division, provides an executive-level forum to discuss and promote current and emerging technology, foster innovation, reduce fraud, and improve cybersecurity and risk management practices for the financial sector.

BPI BITS Contact: Heather Hogsett, Senior Vice President, Technology and Risk Strategy, BITS

The **Institute of International Bankers ("IIB")** represents internationally headquartered financial institutions from over thirty-five countries around the world doing business in the United States. The membership consists principally of international banks that operate branches, agencies, bank subsidiaries, and broker-dealer subsidiaries in the United States. The IIB works to ensure a level playing field for these institutions, which are an important source of credit for U.S. borrowers and comprise the majority of U.S. primary dealers. These institutions enhance the depth and liquidity of U.S. financial markets and contribute greatly to the U.S. economy through direct employment of U.S. citizens, as well as through other operating and capital expenditures.

IIB Contact: Beth Zorc, Chief Executive Officer

The **American Bankers Association ("ABA")** is the voice of the nation's $23.7 trillion banking industry, which is composed of small, regional, and large banks that together employ more than 2.1 million people, safeguard $18.7 trillion in deposits, and extend $12.2 trillion in loans.

ABA Contact: John Carlson, Vice President, Cybersecurity Regulation and Resilience