April 11, 2022

Via Electronic Mail

Securities and Exchange Commission
100 F Street NE
Washington, DC 20549-1090
Attn: Secretary, Securities and Exchange Commission

Re: Cybersecurity Risk Management for Investment Advisors, Registered, Investment Companies, and Business Development Companies (File Number S7-04-22)

Ladies and Gentlemen:

The Bank Policy Institute ("BPI")[1], through its technology policy division known as BITS[2], appreciates the opportunity to comment on the proposed rulemaking issued by the Securities and Exchange Commission ("SEC" or "Commission") regarding cybersecurity risk management and incident reporting for investment advisors, registered investment companies, and business development companies. As the trade association for the nation's leading banks, many BPI/BITS-affiliated firms operate lines of business and deliver access to investment adviser and wealth management products and services from within their wider corporate structures as a convenient way to facilitate a comprehensive offering for a customer's financial life. We therefore write to offer comments with the goal of achieving clarity and alignment on the requirements as proposed and where appropriate, address some of the Commission's thoughtful questions.

Technology plays an enormous role in the relationship between complexity and efficiency in the operation of today's financial markets. As a result, critical business operations face escalating cybersecurity risks via a rapidly broadening and intensifying attack surface. The reliance on technology to facilitate efficient and resilient markets coupled with the growing sophistication of, and exposure to, cyber threat actors means that the industry must remain constantly vigilant. Given the growing threat environment, the Commission is justifiably concerned about cybersecurity risk management and incident awareness. This pertains equally to concerns about active market operations that rely on uninterrupted stability, as well as ensuring that investors enter markets with access to adequate information to inform their investment decisions.

[1] The Bank Policy Institute is a nonpartisan public policy, research, and advocacy group, representing the nation's leading banks and their customers. Our members include universal banks, regional banks and the major foreign banks doing business in the United States. Collectively, they employ almost 2 million Americans, make nearly half of the nation's small business loans and are an engine for financial innovation and economic growth.
[2] BITS – Business, Innovation, Technology, and Security – is BPI's technology policy division that 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 nation's financial sector.

We agree with the Commission regarding the importance of ensuring that, like other elements of the financial sector, SEC-supervised entities are subject to reasonably designed cybersecurity programs and are providing relevant entities with visibility into significant cyber incidents that could potentially impact market stability. As the Commission rightfully recognizes, poorly designed or executed risk management practices and protections of information systems can lead to significant consequences, including loss of adviser, fund, or client data; inability to execute on investment strategies leading to client losses; or even the theft of intellectual property, confidential information, or client assets. Likewise, we share the general view with the Commission that it is important for investors to be able to evaluate the risk associated with an investment decision, and that cybersecurity risk exposure and incident effects may be elements of that assessment.

Still, we believe that the Commission should consider the wider application of its proposal in coordination with existing risk management, and notification, reporting, and disclosure requirements. Investors should bear no more risk in their investment decisions than would reasonably be anticipated with any investment product, but we also appeal to the Commission to meaningfully account for the existing structure and application of our member firms' organization-wide cybersecurity risk management program that demand efficiency as a matter of governance, resourcing, and effectiveness. As currently drafted the proposal could create operational and compliance challenges for even the most capable firm, as noted below.

1. **The Commission should more fully recognize that a lack of harmonization with existing requirements can lead to unnecessary corporate complexity and could interrupt incident response and remediation**

    a. The Commission should ensure new risk management and reporting obligations are consistent with existing regulation and guidance

As BPI/BITS members as well as the Commission are acutely aware, the interconnectedness of both the US and global financial systems means that robust cybersecurity risk management practices and information sharing are in everyone's interest. Beyond recognizing the value of strong cybersecurity protections as competitive table stakes to acquiring new investment clients, BPI/BITS member firms are also supervised by their primary prudential regulators throughout the corporate organization for cybersecurity, operational resilience and risk management compliance. While the Commission nods toward the overlapping compliance burdens from other regulators, our concerns about redundancy, complexity, and inefficiency for organizations already subject to another primary regulator's supervision are not limited merely to additional filings.

The SEC is the primary regulator for Registered Investment Advisers ("RIAs") and investment companies, yet not all these entities exist in a standalone capacity. As a function of their primary supervisory relationship, BPI/BITS member firms that may include subsidiary RIAs or investment companies are required to maintain comprehensive and organization-wide compliance programs to address information security, third-party and vendor risk management, and business continuity. They are also required to adequately notify or report on certain cybersecurity vulnerabilities to numerous

federal and state regulators, on a varying spectrum of timelines. Further, most BPI/BITS members operate in multiple international jurisdictions and are therefore exposed to the regulatory risk management and incident reporting requirements of various other global financial regulators.

b. Our member firms typically rely on group processes for technology and controls to create a "one for many" cybersecurity risk management and incident reporting product for all entities and sub-entities within the wider organization

The Commission appropriately notes that, "advisers and funds may be part of a larger company structure or organization that shares common cybersecurity and information technology personnel, resources, systems, and infrastructure.[3] However, it neglects to follow that observation with additional clarity recognizing that a material difference in systems or security administration may come into play when larger organizations are involved. Like other institutions throughout the private sector, BPI/BITS member firms often exist as interrelated arrangements of businesses and product lines organized under a larger corporate structure. This structure operates to ensure that customers can engage with an entire suite of financial products and services under a unified customer experience. It is beneficial to customers that they can experience seamless interactions with as much of their financial lives at one location as the firm can offer in terms of cohesive products and services.

In pursuit of this consistent experience, and to establish a reliable operating environment and responsibly manage resources, larger firms will often establish group processes for technology management and controls development to create a "one for many" internal IT product that captures the various subsidiary businesses under one IT "umbrella" as architecture, design, and regulation allow. In doing so, the parent organization can consolidate expertise and experience as well as ensure full-scope visibility into its cybersecurity systems and operations. While not every subsidiary's system will benefit from this streamlining and coordination, as a common practice it is a recommended approach realized in terms of allocation of expertise and security fortification.

Expressly requiring advisers and funds to set up discrete cybersecurity-related policies and procedures when they are already applicable through a robustly regulated parent organization may create duplicative policies as well as operating, security, and compliance friction. With this in mind, we believe it is important for the Commission to go a step beyond merely acknowledging the structural and organizational circumstances of many registered investment advisers and funds and modify the rule to reflect the operational realities that would make setting up bespoke, one-off compliance systems for individual business lines disruptive to existing unified and coordinated organizational cybersecurity efforts.

c. The Commission should retain a flexible, principles-based, and consistent approach to account for existing frameworks and requirements in complex banking organizations

[3] https://www.govinfo.gov/content/pkg/FR-2022-03-09/pdf/2022-03145.pdf at 13528.

We applaud the Commission for recognizing that the proposed requirements "should be tailored based on its business operations, including its complexity, and attendant cybersecurity risks."[4] BPI/BITS member firms are some of the most capable institutions in the financial services industry when it comes to implementing and maintaining appropriate cybersecurity risk management practices. However, because of the unified nature of these firms' group technology management and controls teams we urge the Commission to recognize that flexibility is crucial to establishing those same teams and affording them the agility to respond according to the firm's corporate structure. We further note that the recently enacted *Strengthening America's Cybersecurity Act* law requires the federal government to improve coordination between federal agencies and to review cyber incident regulatory reporting regulations to ensure that they avoid conflicting, duplicative, or burdensome requirements; and further to coordinate with regulatory authorities that receive incident reports for the purposes of identifying opportunities to streamline reporting processes and facilitate interagency report sharing agreements.[5]

d. The Commission should permit advisers and funds to rely on commonly accepted reports or certifications to demonstrate compliance

Once triggered by a significant incident as described by the proposal, the registered fund will likely need to have any related ADV-C filing pre-approved by outside Fund Counsel and possibly some participation by the independent Board. This will add a significant layer of administrative complexity, as it is unclear whether it is functionally possible to get all necessary eyes or appropriate internal approvals on a duly filled out ADV-C filing within 48 hours. Further, if all advisors try to audit or receive bespoke assurances from their providers, it will drive a large amount of compliance work into specialist cybersecurity teams. This creates more strain on available resources at a time they are most needed to remediate an incident, and in a field where demand already far outstrips supply. Therefore, we urge the Commission to consider clarifying that advisors and funds can rely on commonly accepted reports or certifications from their providers to gain assurance of the providers cybersecurity risk assessments and practices, such as the Cyber Risk Institute's Profile or other common framework.

e. The use of a single, formalized reporting mechanism such as the proposed Form ADV-C is ill-suited to cybersecurity incidents, which may change frequently

The Commission proposes that details on significant incidents be funneled through a modified Form ADV-C as a way to enhance its ability to monitor activities efficiently.[6] The proposed version of the Form ADV-C is intended to be filed through the existing Investment Adviser Registration Depository ("IARD") platform. While we appreciate attempts by the Commission to streamline its reporting and compliance process, we believe the proposed Form ADV-C is ill-suited as a mechanism for this application. Instead, we note that US Federal regulators (OCC, FRB, and FDIC) in their recently finalized joint rule on computer security incident notification do not prescribe specific means

[4] https://www.govinfo.gov/content/pkg/FR-2022-03-09/pdf/2022-03145.pdf at 13527
[5] P. L. 117-103, Div. Y, Sec. 103
[6] Id. at 13538.

of notifying of a cybersecurity incident. The primary reason for doing so is an affirmative recognition that at the early stages of incident response, determination could still be underway, information can be fluid and resources are better prioritized toward mitigation. Therefore, we suggest the Commission consider a simpler notification method that allows for discrete, streamlined, and minimized transmission of sensitive information until such time as the incident can be securely disclosed in full detail for evaluation.

Directing use of the proposed Form ADV-C as the sole method of electronically communicating incident activity also creates several security considerations for BPI/BITS member firms as well as the Commission. First, it places the Commission in the position of being a centralized repository of extremely sensitive data related to a significant cyber breach. While the information may be useful to the Commission in performing its duties, the level of detail transmitted would also make the Commission an attractive cybersecurity target. Many of the 16 reporting questions on the proposed Form ADV-C are general in nature, but several are specific enough around sensitive topics related to remediation to raise serious security concerns. Further, with regard to the final ADV-C question requiring disclosure of whether the incident is covered under a cybersecurity insurance policy, we believe the Commission should reconsider the necessity of this question. Considering the Commission's objective to understand the potential effects on investors or advisers' clients, it is unclear how an answer here would provide any meaningful information. For example, whether an adviser has cyber insurance or not is not probative of the potential effect the incident could have on an adviser's clients, the adviser's response to the incident, its cyber hygiene, or its ability to cover the costs associated with a significant cybersecurity incident.

Second, combined with the relatively short reporting timeline, it is possible that malicious threat actors are still active in the IT system and would be able to intercept extremely sensitive data and further guide their actions. The Commission must remain sensitive to the fact that a rush to report to the degree of specificity that is required by the proposed Form ADV-C may cause greater harm by demanding too much information, too soon after the incident takes place. And finally, depending on the type of cyber incident, the ability to report via IARD and the proposed Form ADV-C may be degraded or eliminated, necessitating an alternative means of securely transmitting the relevant details.

Therefore, we encourage the Commission to consider revising its approach such that submission of Form ADV-C can come if at all, at a later point at which the extent of the cybersecurity incident is understood. This will help avoid a situation in which a firm is forced to release information before it is certain, creating further damage and potential market distorting effects for an incident that may in retrospect turn out to be less than material.

f. BPI supports the Commission's decision to ensure that any required reporting submissions remain confidential

The Commission notes that it "considered requiring public disclosure of Form ADV-C in the proposal"[7] in line with an intent to provide an investor visibility into a regulated adviser or fund's level

[7] Id. at 13559

of cybersecurity preparedness when evaluating where and how to invest their funds. This objective is technically furthered by fulsome awareness of cyber incidents and risk management policies and procedures. However, regarding ongoing and recently remediated incidents, a reasonable balance of information disclosure must be maintained to ensure that investor visibility does not betray an institution's active cybersecurity defenses or unintentionally divulge ongoing mitigation and remediation efforts that could further guide a malicious cyber actor to cause greater harm.

g. The Commission should reexamine the proposed frequency and timeline of ADV-C reporting updates

BPI/BITS members appreciate the Commission's efforts to "protect investors in connection with cybersecurity incidents by providing prompt notice of these incidents."[8] The Commission states that it "[believes] this proposed reporting would allow the Commission and its staff to understand the nature and extent of a particular cybersecurity incident and the firm's response to the incident."[9] However, in so requiring, the Commission seeks ongoing updates as new information is discovered, becomes inaccurate, or after the incident is resolved or closed out from internal investigation. As an example of how the proposed reporting and update requirements are useful, the Commission notes that materially relevant updates would assist it in identifying patterns and trends, including widespread cybersecurity incidents affecting multiple advisers and funds.

These ensuing material reporting updates are accompanied by a similar 48-hour requirement to resubmit updated Form ADV-Cs after each such instance. It is no doubt useful to the Commission for it to have as much information as it can reasonably acquire in its mission to protect investors. However, for the previously discussed reasons related to internal process and resource allocation, it is both impractical and potentially counterproductive to ongoing mitigation and remediation efforts to assign the same 48-hour timeline to reporting updates for ongoing incidents.

For every instance where materially new information is either discovered or corrected, it sets in motion an organization-wide activation of the corporate administrative layer required to approve Form ADV-C filings, which as previously noted may not be realistic within a 48-hour window. Feasibility aside, the internal process to file a Form ADV-C to update on a previously reported incident also takes active resources from mitigation and remediation off the response table and redirects them toward administrative process and compliance. This works against the Commission's efforts to protect investors. Additionally, the 48-hour timeline potentially overlooks the frequency with which these updates are likely occur so early on in addressing a significant cyber incident, meaning that several approval processes could overlap as the incident unfolds and is further ascertained, further interrupting the organization's response mechanisms. For these reasons, we urge the Commission to consider lengthening the timeline as it pertains to reporting updates and material changes to previously reported incidents via a Form ADV-C filing.

[8] Id. at 13536
[9] Id.

2. BPI supports the Commission's desire to maintain confidential incident reporting and information sharing safeguards

We strongly support the Commission's efforts to ensure that reporting of significant incidents is delivered on a confidential basis. Institutions should not be compelled to publicly disclose information about their cybersecurity environment or potential system vulnerabilities as to alert perpetrators of attacks or empower additional threat actors to gain unauthorized access to compromised networks.

BPI/BITS member firms recognize the importance of timely detection of significant cybersecurity threats, and appreciate the Commission's responsibilities to its oversight role in understanding the nature and extent of cybersecurity incidents. For BPI/BITS member firms with existing cybersecurity risk management practices throughout their organizations, we encourage the Commission to recognize the proposed requirement to timely notify the Commission of critical cybersecurity incidents will represent the formalization of a voluntary practice that already exists.

a. BPI requests more clarity from the Commission regarding how the proposal will interact with existing regulatory notification and reporting requirements

While the Commission commendably attempted to reduce burdens in drafting the proposal, the fact remains that an additional reporting requirement for regulated institutions like BPI/BITS member firms and their subsidiary registered investment services entities adds an unnecessary layer to the already-complex existing threat detection, notification, and reporting process. As noted earlier, BPI/BITS member firms are already required to maintain organization-wide and comprehensive compliance programs to address information security, third-party and vendor risk management, business continuity. Additionally, they are required to adequately disclose significant and/or material cybersecurity incidents to numerous federal regulators, including the Office of the Comptroller of Currency ("OCC"), the Federal Reserve System ("Federal Reserve"), the Federal Deposit Insurance Corporation ("FDIC"), in addition to state agencies.

State and federal regulators are essential monitors of the soundness of the information security systems of such institutions, but we strongly believe imposing additional and redundant notice obligations on these institutions serves not only to distract them from focusing on protecting systems and securing consumer information but also creates a dynamic in which an entity may be looking to multiple regulators with different timelines and priorities for guidance in responding to such an incident. Just within the existing domestic notification and reporting requirements there are at least four different notification and reporting timelines within the first 72 hours of determination of an event. More significantly, adding the Commission's requirement to these pre-existing obligations could unnecessarily interfere with the discretion of a firm's primary federal regulator and result in confusion.

b. BPI appreciates the relatively high materiality threshold set for reportable incidents

We applaud the Commission for recognizing that a sufficiently elevated materiality threshold is essential to the effective management of any incident notification or reporting requirement. This approach aligns with similar requirements at other financial regulators. When identifying and evaluating a potential cyber incident, it is important to focus resources on assessment and response. By ensuring that only incidents of a certain significance are required to be reported to the Commission, it frees BPI/BITS member firms' cybersecurity response teams to focus on the important work of response and recovery to continue the firm's essential business, as well as eliminates reporting "noise" for Commission staff involved in overseeing the reporting system. To further enhance understanding of the newly established materiality threshold, we recommend that this be supported by a list of non-exhaustive examples. We further note the list of examples provided in the recently finalized *Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers* rule[10] was well-conceived and well-received by cybersecurity specialists who found it helpful in setting internal thresholds for reporting.

c. More information is needed regarding SEC policies and procedures to secure the confidentially reported information once transmitted

We welcome further discussion on how the Commission intends to share and secure information provided in connection with a reported incident. BPI/BITS member firms as well as their regulators have a shared interest in protecting the sector. Although the Commission seeks to increase visibility into cybersecurity practices in the name of investor awareness, it is equally important to assure regulated firms that their sensitive data is protected. For example, greater clarity on how the Commission envisions securing the reported information once it has been received via the proposed ADV-C form, and whether and under what circumstances the Commission would share the information with other authorities. Given the sensitivity of the subject matter, we believe that the Commission should withhold or delay transmitting any sensitive information and details from incident reports provided by an adviser or fund while active remediation is ongoing.

3. BPI urges the Commission to ensure disclosure requirements do not unintentionally create additional vulnerabilities

The Commission should take care to confine public disclosures of vulnerabilities to a limited description and non-identifiable format that does not unintentionally disclose information about an organization's cybersecurity architecture or potential system vulnerabilities to ongoing threat actors**.** While the Commission is rightfully concerned with investor disclosure and awareness of cyber incidents in evaluating investment decisions, we observe that confidentiality in the reporting of detailed incident information provided to the Commission is essential and would be consistent with general norms of financial institution information sharing to enhance cybersecurity.

As an industry it is our belief and experience that the Commission will incentivize more comprehensive reporting—and accordingly facilitate more robust information sharing—if reporting institutions are confident that nonpublic material will not be disclosed. As noted above, robust

[10] 12 CFR 53, 225, 304

cooperation between private and public sectors is essential for effective cybersecurity, and it involves not just mitigating disruptive intrusions, but also preventing future attacks. Companies must be able to share valuable information with the government and their industry peers without fear of undue reputational harm and unnecessary loss of investor trust and confidence in financial institutions.

BPI/BITS appreciates the opportunity to comment on this Proposed Rule. If you have questions or would like to discuss these comments further, please reach out to Brian Anderson at [redacted].

Sincerely,

Christopher Feeney
EVP and President, BITS
Bank Policy Institute