May 22, 2023

VIA ELECTRONIC SUBMISSION

Vanessa A. Countryman
Secretary
Securities and Exchange Commission
100 F Street NE
Washington, D.C. 20549-1090

Re: Proposed Cybersecurity Risk Management Rule, 87 Fed. Reg. 13524 (Mar. 9, 2022)

Dear Ms. Countryman:

The American Investment Council (the "AIC") appreciates that the Securities and Exchange Commission (the "SEC") reopened the comment period for the Proposed Rule for Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, 87 Fed. Reg. 13524 (Mar. 9, 2022) (the "Proposed Rule") to consider the impact of multiple proposed rules on investment advisers. We will limit our comments to the impact on private fund advisers registered under the Advisers Act ("Private Fund Advisers").

The AIC is an advocacy, communications, and research organization established to advance access to capital, job creation, retirement security, innovation, and economic growth by promoting responsible long-term investment. In this effort, the AIC develops, analyzes, and distributes information about the private equity and private credit industries and their contributions to the U.S. and global economy. Established in 2007, and formerly known as the Private Equity Growth Capital Council, the AIC is based in Washington, D.C. The AIC's members are the world's leading private equity and private credit firms, united by their commitments to growing and strengthening the businesses in which they invest.[1]

The AIC supports transparency as it relates to cybersecurity risks, and appreciates the opportunity to submit this letter to reiterate our position as expressed in our April 11, 2022 comment letter ("Initial Comment Letter").[2] As we indicated in that letter, there are a number of challenges that the implementation of the Proposed Rule would have on Private Fund Advisers. We would like to reemphasize the urgent need for alternative solutions (including extending the reporting timeline and clarifying the notification trigger), especially in light of the challenges posed by the overlap with the following newly proposed rules (collectively, "New Cybersecurity Frameworks"):

[1] For further information about the AIC and its members, please visit our website at http://www.investmentcouncil.org.

[2] AIC Comment Letter to SEC on Cybersecurity Incident Reporting Requirement for Investment Advisers (Apr. 11, 2022) ("Initial Comment Letter"), at 3, *available at* https://www.investmentcouncil.org/aic-comment-letter-to-sec-on-cybersecurity-incident-reporting/.

- Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 87 Fed. Reg. 16590 (Mar. 23, 2022) (the "Proposed Issuers Rule");

- Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Swap-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, 88 Fed. Reg. 20212 (Apr. 5, 2023) (the "Proposed BD Rule");

- Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information, 88 Fed. Reg. 20616 (Apr. 6, 2023) (the "Proposed Reg S-P Amendments"); and

- Regulation Systems Compliance and Integrity, 88 Fed. Reg. 23146 (Apr. 14, 2023) (the "Proposed Reg SCI Amendments").

This letter contains two sections. The first section explains the burden on Private Fund Advisers resulting from the overlapping notification requirements under the New Cybersecurity Frameworks and the tremendous overload created for the SEC by the likely flood of precautionary placeholder notifications from Private Fund Advisers and other registrants. The second section outlines potential alternative solutions—including extending the notification deadlines, revising the relevant notification triggers, and creating an option for submitting a single consolidated notification to the SEC to the extent more than one notification obligation is triggered. This section also explains how such solutions would advance the Biden Administration's stated goals for regulatory harmonization.[3]

I. The Burden of Overlapping and Rigid Incident Notification Requirements

Private Fund Advisers are already subject to multitudinous existing and at times overlapping cybersecurity notification requirements, including under the data breach notification laws in 50 U.S. states and various U.S. territories (the District of Columbia, Guam, Puerto Rico, and the Virgin Islands), Health Insurance Portability and Accountability Act ("HIPAA") at the federal level, and, internationally, the European Union's General Data Protection Regulation ("GDPR"), UK GDPR, and the data protection regimes of Brazil, Canada, China, and Singapore, to cite just a few. The SEC's New Cybersecurity Frameworks will create further inconsistencies and duplication in the multiple cybersecurity-related obligations imposed on Private Fund Advisers. Notably, the proposed short-fuse notification requirements to the SEC under the Proposed Rule and the New Cybersecurity Frameworks would overload this already complex notification regime, and, if adopted in their current form, do not present any opportunity for synergies given their divergent triggers and timelines.

The AIC requests the SEC to consider aligning any reporting deadlines to those that are already in existence in order to avoid premature disclosure to the SEC that is likely to be incomplete if not stale. As AIC expressed in our Initial Comment Letter, "[r]equiring notification within 48 hours will mean that Private Fund Advisers will be spending precious time in the first hours of an incident drafting a notification to the SEC (instead of dedicating resources to incident response); revising the disclosure as new information becomes available; and subsequently amending the

[3] National Cybersecurity Strategy (Mar. 1, 2023), at 13, *available at* https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

original disclosure after submission when new facts emerge that render the original notification incomplete or misleading."[4] Because Private Fund Advisers customarily make simultaneous disclosures to all of their regulators in order to ensure consistency across the board and avoid any potential scrutiny over any divergence in treatment, the Proposed Rule's 48-hour notification deadline will likely lead many Private Fund Advisers to submit placeholder notifications to the SEC and all potentially in-scope regulators.[5] Relatedly, the 48-hour notification reporting deadline could also disincentivize Private Fund Advisers to conduct comprehensive investigations during the initial phase of an incident for fear that robust inquiries could unearth new facts that might require additional updates to the SEC on very tight time frames. This unintended consequence would undermine the apparent goal of the reporting requirement—which is to safeguard the marketplace from cybersecurity risks.

Furthermore, the existing burden on Private Fund Advisers described in AIC's Initial Comment Letter is particularly severe for those Private Fund Advisers with an affiliated broker-dealer and potentially also an issuer parent. For those Private Fund Advisers with an affiliated broker-dealer, the Proposed BD rule adds two distinct notification timelines—one with an immediate notification trigger. The challenge is even greater for those Private Fund Advisers that have *both* an affiliated broker-dealer and an issuer parent because such Private Fund Advisers are also subject to the four-business-day 8-K disclosure standard under the Proposed Issuers Rule, on which the AIC separately submitted a comment letter on May 9, 2022.[6]

This complicated array of New Cybersecurity Frameworks exacerbates the burdens faced by Private Fund Advisers during the intense chaos of the initial hours and days of an incident: Private Fund Advisers will have to simultaneously respond to the incident itself and safeguard their information systems and data assets, all while juggling resources to meet the conflicting notification requirements and addressing any questions raised by regulators that contact the Private Funds Advisers to seek information about the notification. The AIC observes that there is a lack of adequate economic impact analysis of the overlapping notification requirements in the Proposing Releases for the New Cybersecurity Frameworks.

For instance, a Private Fund Adviser with an affiliated broker-dealer and an issuer parent would be subject to three separate SEC disclosure regimes and a multitude of other U.S. and global disclosure regimes in connection with a single cybersecurity incident. In turn, such a Private Fund Adviser would potentially need to make at least four separate disclosures (and any required updates) all while addressing and moving swiftly to mitigate the harm from a significant incident: (*1*) immediately notify the SEC in writing under the Proposed BD Rule; (*2*) within 48 hours, file both Forms ADV-C and, depending on the scope of the affiliated broker-dealer, also file Form SCIR Part I; and (*3*) within four (4) business days of a determination that the incident was material, make an 8-K filing. Further, a Private Fund Adviser would be required to update both Form ADV-C (and, as applicable, Form SCIR Part I) within 48 hours of: (*1*) a determination that information has become materially inaccurate; (*2*) the discovery of new material information; (*3*) the resolution of the incident; or (*4*) the closure of an internal investigation. Moreover, because the Proposed Rule does not provide for an omnibus notification for a Private Fund Adviser that experiences an enterprise-wide incident impacting multiple registered

[4] Initial Comment Letter, at 3.
[5] *Id.*
[6] AIC Comment Letter on SEC's Cybersecurity Incident Reporting Requirement for Issuers (May 9, 2022), *available at* https://www.investmentcouncil.org/four-business-days-cybersecurity-incident-reporting-requirement-under-the-proposed-amendment/.

investment advisers within a Private Fund Adviser, each registered investment adviser within a Private Fund Adviser would be subject to a separate and standalone Form ADV-C notification obligation—thus multiplying the filing burden on the Private Fund Adviser by a significant order of magnitude. As noted above, the SEC should aim to harmonize the reporting requirements to reduce the burdens on Private Fund Advisers and other registrants.

Moreover, the definitions of a reportable incident trigger under the Proposed Rule and the Proposed BD rule create further burdens because they are inconsistent, and should therefore be harmonized so that entities subject to multiple SEC cybersecurity rules can meet the applicable requirements in a consistent manner. While the definition of "significant adviser cybersecurity incident" under the Proposed Rule includes those incidents "where the unauthorized access or use of [**adviser information**] **results in** [substantial harm]" (emphasis added), the Proposed BD rule's definition is much broader because it encompasses incidents "where unauthorized access or use of such **information or information systems** [of the market entity] results in **or is reasonably likely to result in** [substantial harm]." (emphasis added). For this reason, a Private Fund Adviser with an affiliated broker-dealer jointly impacted by the same incident would have to navigate two different standards in determining its incident notification obligations to the SEC.

As a result, as the AIC previously observed in our Initial Comment Letter, the SEC will be "inundated with numerous placeholder notifications that are of little value because they either contain no real information, or information that is likely to change swiftly as the Private Fund Adviser continues to investigate the incident. This flood of notices will make it very difficult for the SEC to identify and focus on the incidents that are actually significant and warrant the SEC's attention."[7] The issuance of the New Cybersecurity Frameworks now compounds this problem because Private Fund Advisers with other affiliated registrants will need to file even more notifications about incidents of questionable import, and will most likely result in overreporting of incidents initially viewed as significant but later determined not to be significant. As such, the Proposed Rule's notification standard will paradoxically undermine any benefit to the SEC. Instead of receiving precise and targeted details about incidents that will enable the SEC to identify "patterns and trends across registrants,"[8] the SEC instead will be inundated with vague and indefinite filings that provide no meaningful insight into current and emergent cybersecurity risks. The notification framework therefore will fail to advance the SEC's aim to "understand better the nature and extent of cybersecurity incidents occurring at advisers and funds, how firms respond to such incidents to protect clients and investors, and how cybersecurity incidents affect the financial markets more generally."[9]

Furthermore, Private Fund Advisers are eager to cooperate with law enforcement after cybersecurity incidents. Yet the current rigid notification timelines and prescriptive content requirements do not account for the potential need for Private Fund Advisers to coordinate with law enforcement in the investigation of a potential incident to assist with the identification and pursuit of threat actors—which is an additional strain on resource allocation. Both Form ADV-C under the Proposed Rule and Part I of Form SCIR under the Proposed BD Rule contain a line item asking whether the registrant has notified law enforcement at the time of the SEC notification. This requirement would essentially compel registrants to rush to notify law enforcement within the first 48 hours of an incident to signal to the SEC that they are taking the incident seriously. Yet law enforcement has asked certain AIC members—after becoming aware

[7] *Id.*
[8] Proposed Rule, at 13536.
[9] *Id.*

of an incident—to delay full containment of an incident to enable the government to better trace threat actor activities. Taken together, a Private Fund Adviser could be forced into a situation where it is prohibited from closing a vulnerability in its system because it felt compelled to notify law enforcement within 48 hours—and perhaps before the registrant was ready to provide a meaningful and useful notification to law enforcement— to fulfill a component of the SEC's notification requirement. A Private Fund Adviser that is compelled to file a premature notification to the SEC will not be able to coordinate effectively with law enforcement, which could result in the unintended consequence of undermining efforts to protect the nation's cybersecurity infrastructure.

Moreover, given the well-documented shortage of qualified cybersecurity personnel,[10] Private Fund Advisers cannot simply ease this burden by hiring more employees. Notably, the most severe incidents—which require the full attention of a Private Fund Adviser's management and cybersecurity professionals—are the very same ones that are likely to trigger the SEC's notification requirements. As a practical matter, the burden of these multiple notification requirements will force Private Fund Advisers experiencing an incident to divert resources from taking steps to safeguard client data to instead focusing on notifying—and continually updating—the SEC about a developing incident, the facts of which are likely to become stale as soon as an update is provided.

In short, the Proposed Rule will compel Private Fund Advisers in many cases to file premature and cursory notifications, which in the aggregate will overwhelm the SEC and fail to provide it with meaningful, precise, and robust data about cybersecurity risks impacting Private Fund Advisers. The proposed regulatory regime will not only jeopardize Private Funds Advisers' ability to bolster their cybersecurity defenses, but will also undermine the SEC's stated policy objectives of safeguarding the marketplace from cybersecurity risks.

II. Proposed Alternative Solutions

To resolve the significant challenges created for registrants under the current proposals and advance the Biden Administration's stated goal for regulatory alignment in cybersecurity, the SEC should consider the following proposed solutions.

Harmonizing the Notification Timelines Applicable to Registrants, with Added Flexibility

First, as AIC proposed in our Initial Comment Letter, the SEC should provide at least an additional 24 hours on top of the current 48 hours for reporting a qualifying event under the Proposed Rule,[11] ideally extending that timeline to four (4) business days to align with the deadline contemplated in the Proposed Issuers Rule. Consistent with that, the SEC should revise

[10] *See, e.g.*, Steve Morgan, *Cybersecurity Jobs Report: 3.5 Million Unfilled Positions in 2025*, Cybercrime Magazine (Apr. 14, 2023), https://cybersecurityventures.com/jobs/ ("Despite the disarray of the tech industry, cybersecurity remains a near-zero unemployment marketplace for those with extensive backgrounds, and the shortage means that IT teams must also shoulder a security burden. Staff must train in modern threat awareness, including phishing, social engineering, Business Email Compromise (BEC), and financial fraud. They must also know how to protect and defend apps, data, devices, infrastructure, and people."); Justin Rende, *Why Overcoming the Cybersecurity Labor Shortage Matters to Company Success*, Forbes (Mar. 1, 2023), https://www.forbes.com/sites/forbestechcouncil/2023/03/01/why-overcoming-the-cybersecurity-labor-shortage-matters-to-company-success/?sh=6547a9977766 ("As the shortage of skilled cybersecurity workers continues, it has begun impacting companies' ability to achieve compliance.").

[11] Initial Comment Letter, *supra* note 2, at 4.

the "immediate notice" deadline and the 48-hour Part I Form SCIR deadline under the Proposed BD Rule along these same time frames. In addition, the SEC should consider introducing appropriate flexibility in the notification timelines to account for a registrant's need to coordinate with law enforcement agencies.

Clarifying the Definition of Notification Triggers

Second, because an extension of time is not on its own sufficient to alleviate the challenges posed by the notification requirement, the SEC should also modify the definition of a qualifying event for notification purposes under the Proposed Rule. As AIC explained in its Initial Comment Letter, the SEC should modify the definitions of a "significant cybersecurity incident" and "substantial harm" to enumerate specific types of operational impacts that will trigger the notification obligation, such as limiting qualifying events to incidents that result in substantial harm to "a material portion of a Private Fund Adviser's client base, including clients and investors in a private fund, whose information was accessed."[12] The Proposed Rule, as currently formulated, suggests that substantial harm to even one client or investor in a private fund (such as significant monetary loss or the theft of personally identifiable or proprietary information) would be a sufficient trigger for a notification to the SEC, even if subsequently reimbursed by the Private Fund Adviser. Such an outcome should not be the case. By contrast, the cybersecurity incident notification requirement for banking organizations and their bank service providers is triggered only by "an occurrence that results in **actual harm** to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits" that "has **materially** disrupted or degraded, or is reasonably likely to **materially** disrupt or degrade," a banking organization's activities and processes (including failures that would "pose a threat to the financial stability of the United States") (emphasis added).[13] The SEC should adopt a similar notification standard that is tethered to actual harm and material impact to a Private Fund Adviser.

Additionally, the SEC should also change the notification trigger from a "reasonable belief" that a significant cybersecurity incident has occurred to a "determination" that such an incident has occurred to provide a firmer (and less imprecise) anchor for notification and to alleviate the burden both on Private Fund Advisers and the SEC resulting from what is effectively a requirement to file multiple vague cautionary placeholder notifications. For this reason, the Proposed Rule likewise should not include the Proposed BD Rule's notification obligation for wholly speculative and unknown future harm that is "reasonably likely to occur."

Allowing for Combined Notifications to the SEC to Satisfy Multiple Notification Requirements

Third, because the New Cybersecurity Frameworks share common objectives, the SEC should also simplify and harmonize notification requirements to the SEC for entities subject to multiple notification requirements. For example, if a Private Fund Adviser subject to both the Proposed Rule and the Proposed BD Rule experiences a significant cybersecurity incident, the SEC should amend the requirements under both proposed rules to permit the Private Fund Adviser to file a single notification (that satisfies the requirements of both rules) to the SEC on a single unified time frame and allow for a similar coordinated approach for material incident updates. The SEC should also permit a Private Fund Adviser with multiple registered investment advisers to file one omnibus notification on behalf of all registered investment advisers impacted by the same

[12] *Id*. at 4−5.
[13] Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 86 Fed. Reg. 66424 (Nov. 23, 2021).

cybersecurity incident. This way, the SEC can ensure that registrants are able to leverage any synergies in their preexisting processes without expending unnecessary resources and while helping to advance the SEC's mission to "bolster the efficiency and effectiveness of [its] efforts to protect investors, other market participants, and the financial markets in connection with cybersecurity incidents."[14]

Harmonization as a Step towards Regulatory Alignment

The proposed harmonization solutions would align with the Biden Administration's March 2023 National Cybersecurity Strategy (the "Strategy")'s emphasis on the need for cross-agency coordination on cybersecurity-related regulatory requirements. Specifically, the Strategy stated that "effective regulations minimize the cost and burden of compliance, enabling organizations to invest resources in building resilience and defending their systems and assets." It also cautioned that "[w]here Federal regulations are in conflict, duplicative, or overly burdensome, regulators ***must work together to minimize these harms***" (emphasis added). In fact, the Financial Stability Board (the "FSB") (on which SEC Chair Gary Gensler serves) has also made similar proposals, including with its October 2022 report on "Achieving Greater Convergence in Cyber Incident Reporting," where it recommended that financial authorities "explore ways to align their [cyber incident reporting] regimes . . . to minimize fragmentation and improve interoperability" and "identify common data requirements, and, where appropriate, develop or adopt standardized formats for the exchange of incident reporting information."

Against this policy backdrop, the AIC encourages the SEC to consider the proposed harmonizing solutions to alleviate the burden that the New Cybersecurity Frameworks would impose on Private Fund Advisers and firmly believes that such measures would ultimately lead to more robust cybersecurity risk management and better protection of investor interests overall.

Finally, given the complexity of the Proposed Rule and the certain implementation and compliance challenges for Private Fund Advisers—especially for smaller registered investment advisers—posed by its requirements, the SEC should provide for a sufficiently lengthy compliance period after the effective date of the Final Rule. The AIC respectfully requests the SEC to consider providing a compliance period of at least 18 months.

*****

The AIC appreciates the opportunity to provide additional comments to the SEC on the Proposed Rule and would be pleased to answer any questions that you might have concerning our comments.

Respectfully submitted,

/s/ Rebekah Goshorn Jurata

Rebekah Goshorn Jurata

General Counsel

American Investment Council

[14] Proposed Rule, at 13526.