April 11, 2022

Via Electronic Filing

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

Re: Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies (SEC Rel. Nos. 33-11028; 34-94197; IA-5956; IC-34497; File No. S7-04-22)

Dear Ms. Countryman:

The Investment Adviser Association (**IAA**)[1] appreciates the opportunity to comment on the Commission's proposed cybersecurity rules that would require investment advisers to adopt and implement written cybersecurity policies and procedures with specified elements, report significant adviser cybersecurity incidents to the Commission, disclose significant adviser cybersecurity risks and incidents to clients, and maintain related books and records.[2]

The IAA shares and supports the Commission's overarching goals to enhance the preparedness and resiliency of advisers against cybersecurity threats and attacks that are generally reflected in the Proposal. In particular, we support the proposed cybersecurity risk management policies and procedures for advisers, but with modifications that we believe would significantly improve the Proposal. We do, however, have concerns that the reporting and disclosure requirements, as proposed, would impede advisers' efforts to respond to cybersecurity incidents as they are occurring, and impose unnecessary operational and compliance burdens. We are also concerned that the disclosure requirements as proposed would be counterproductive to the Commission's goals.

[1] The IAA is the leading organization dedicated to advancing the interests of investment advisers. For more than 80 years, the IAA has been advocating for advisers before Congress and U.S. and global regulators, promoting best practices and providing education and resources to empower advisers to effectively serve their clients, the capital markets, and the U.S. economy. The IAA's member firms manage more than $35 trillion in assets for a wide variety of individual and institutional clients, including pension plans, trusts, mutual funds, private funds, endowments, foundations, and corporations. For more information, please visit www.investmentadviser.org.

[2] *Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies*, 87 Fed. Reg. 13524 (Mar. 9, 2022), available at https://www.govinfo.gov/content/pkg/FR-2022-03-09/pdf/2022-03145.pdf (**Proposal**). The IAA is primarily commenting in this letter on the Proposal as it relates to investment advisers. However, we endorse similar recommendations for funds.

As cybersecurity threats continue to increase in prevalence and sophistication, investment advisers are motivated to take their responsibilities to protect their clients and businesses very seriously. Indeed, as fiduciaries, advisers are always required to act in the best interest of their clients.[3] This includes taking reasonable steps to protect clients from being placed at risk from cybersecurity incidents.[4] Moreover, pursuant to existing SEC rules, advisers are already required, among other things, to maintain and implement policies and procedures reasonably designed to address risks commensurate with their operations, and the SEC has effectively deployed these rules in bringing actions related to cybersecurity matters.[5] Additional guidance published in recent years by the SEC's Divisions of Investment Management and Examinations has helped advisers continuously reassess their policies and procedures, tailored to their businesses, to ensure that they reasonably address the latest cybersecurity threats and vulnerabilities.[6] Beyond

---

[3] *See Commission Interpretation Regarding Standard of Conduct for Investment Advisers*, 84 Fed. Reg. 33669 (July 12, 2019), available at https://www.govinfo.gov/content/pkg/FR-2019-07-12/pdf/2019-12208.pdf.

[4] *See Compliance Programs of Investment Companies and Investment Advisers*, 68 Fed. Reg. 74714 at n.22 (Dec. 24, 2003), available at https://www.sec.gov/rules/final/ia-2204.pdf (**Compliance Program Rule Release**) ("We believe that an adviser's fiduciary obligation to its clients includes the obligation to take steps to protect the clients' interests from being placed at risk as a result of the adviser's inability to provide advisory services…The clients of an adviser that is engaged in the active management of their assets would ordinarily be placed at risk if the adviser ceased operations.").

[5] *See, e.g.*, Advisers Act Rule 206(4)-7 (**Compliance Program Rule**); Privacy of Consumer Financial Information (**Regulation S-P**); and Identity Theft Red Flags Rules (**Regulation S-ID**). An adviser's policies and procedures are designed to protect clients by, among things, addressing an adviser's ability to continue operations in response to threats such as natural disasters or cyber attacks (*e.g.*, business continuity plans). *See* Compliance Program Rule Release at 74716 (policies and procedures under the Compliance Program Rule should, at a minimum, include business continuity plans).

[6] Staff guidance has confirmed the obligation of advisers to have adequately designed cybersecurity-related policies and procedures pursuant to the Compliance Program Rule. *See* SEC Division of Investment Management Guidance Update, *Cybersecurity Guidance* (Apr. 2015)(citing the Compliance Program Rule and an adviser's fiduciary duty in stating that "Funds and advisers could also mitigate exposure to any compliance risk associated with cyber threats through compliance policies and procedures that are reasonably designed to prevent violations of the federal securities laws. For example, the compliance program of a fund or an adviser could address cybersecurity risk as it relates to identity theft and data protection, fraud, and business continuity") available at https://www.sec.gov/investment/im-guidance-2015-02.pdf (**2015 Guidance Update**).

See also, e.g., SEC Office of Compliance Inspections and Examinations Risk Alert, *Cybersecurity Examination Sweep Summary* (Feb. 3, 2015), available at https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf, SEC Office of Compliance Inspections and Examinations Risk Alert, *OCIE's 2015 Cybersecurity Examination Initiative* (Sep. 15, 2015), available at https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf, SEC Office of Compliance Inspections and Examinations Risk Alert, *Cybersecurity: Ransomware Alert* (May 17, 2017), available at https://www.sec.gov/files/risk-alert-cybersecurity-ransomware-alert.pdf, SEC Office of Compliance Inspections and Examinations Risk Alert, *Observations from Cybersecurity Examinations* (Aug. 7, 2017), available at https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf, SEC Office of Compliance Inspections and Examinations Risk Alert, *Investment Adviser and Broker-Dealer Compliance Issues Related to Regulation S-P - Privacy Notices and Safeguard Policies* (Apr. 16, 2019), available at https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Regulation%20S-P.pdf, SEC Office of Compliance Inspections and Examinations Risk Alert, *Safeguarding Customer Records and Information in Network Storage - Use of Third Party Security Features* (May 23, 2019), available at https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Network%20Storage.pdf, SEC Office of Compliance Inspections and Examinations, *Cybersecurity and Resiliency Observations* (Jan. 27, 2020), available at

these regulatory obligations, advisers are keenly aware of and concerned about significant consequences of cybersecurity breaches to their clients and the existential threat these risks represent to their businesses.[7] Thus, advisers share the Commission's goal of protecting investors from cybersecurity incidents and strive to maintain cybersecurity programs tailored to their businesses and risks.

I. Executive Summary

The IAA remains committed to supporting efforts by the Commission to protect investors, other market participants, and the financial markets more broadly from the dangers presented by cybersecurity threats. We offer comments and recommendations that we believe would further the Commission's objectives while better protecting investors and streamlining unnecessary operational and compliance burdens on advisers. In particular:

- We support the Commission's efforts to codify existing SEC cybersecurity guidance to make it easier for compliance professionals to adhere to generally-agreed-upon best practices, and strongly support that advisers be able to tailor these practices to their businesses and risks. In many respects, the proposed cybersecurity policies and procedures at a high level generally reflect what firms are already required to have in place under the Compliance Program Rule. However, we recommend certain modifications to better reflect industry best practices for both larger and smaller firms, and not impose requirements that are overly prescriptive, cost prohibitive, or unrealistic. In particular, we believe that:
    - The set of service providers for which advisers must assess compliance should be risk-based and narrowed.
    - The proposed requirement to have a written contract relating to cybersecurity controls of third-party service providers would be infeasible in practice for most advisers, particularly smaller advisers that lack any leverage to engage in contractual negotiations with certain service providers.
- We support a reporting requirement but believe that any reporting requirements should not be duplicative of or inconsistent with other breach notification requirements that advisers are subject to, thereby adding another unnecessary

https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf, SEC Office of Compliance Inspections and Examinations Risk Alert, *Cybersecurity: Ransomware Alert* (July 10, 2020), available at https://www.sec.gov/files/Risk%20Alert%20-%20Ransomware.pdf (**Ransomware Risk Alert**), and SEC Office of Compliance Inspections and Examinations, *Cybersecurity: Safeguarding Client Accounts against Credential Compromise* (Sep. 15, 2020), available at https://www.sec.gov/files/Risk%20Alert%20-%20Credential%20Compromise.pdf.

[7] According to our 2020 *Investment Management Compliance Testing Survey* conducted of 384 investment advisers, an overwhelming 94 percent of respondents reported having a formal cybersecurity program, 79 percent reported that their Business Continuity Plan addressed cyber attacks, and 85 percent considered cybersecurity to be the hottest compliance topic for the ***6th consecutive*** year. The results of our annual surveys are available at https://www.investmentadviser.org/publications/investment-testing.

regulatory layer of complexity and compliance burdens. Thus, the IAA strongly recommends that the Commission coordinate with other federal regulators towards adopting a uniform risk-based federal requirement for reporting cybersecurity and data breach incidents. We believe that taking a more holistic and coordinated approach to cybersecurity threats is the most effective means to protect the overall U.S. cybersecurity infrastructure, including the financial markets.

- We nevertheless offer recommendations with respect to incident reporting that we believe would significantly improve the Proposal. We suggest clarifications that we believe would provide a clearer and more understandable definition of reportable cybersecurity breaches. We are particularly concerned that the proposed 48-hour window for reporting and the continuous updating requirements would unduly impede real-time response efforts in the critical first hours and days of managing a cybersecurity incident without necessarily providing the benefits the Commission seeks to achieve. Thus, we offer recommendations that address these and other concerns that we believe would provide the SEC with critical information in a timely and efficient manner. We also recommend that the Commission exclude smaller advisers from the reporting requirement.

- While we generally support cybersecurity-related disclosures, we are concerned that the Proposal would not provide investors with decision-useful information. We are also concerned that the proposed specificity of disclosure may provide a roadmap to cybersecurity threat actors for further attacks. Thus, we recommend modifications to the Proposal to permit advisers to provide a more concise discussion of cybersecurity risks and related incidents.

- We believe that the Commission severely underestimates the costs and burdens that would be imposed on investment advisers, particularly smaller firms, by certain elements of the Proposal. Thus, we recommend that the Commission undertake a more expansive, accurate, and quantifiable assessment of the specific costs, burdens, and economic effects that would be placed on advisers.

- The Commission should provide a compliance period of at least 18 months to allow advisers to holistically reassess their current cybersecurity risk, align current practices with prescriptive regulatory requirements, prepare for brand new reporting, implement written policies and procedures, and update public disclosures in light of any new requirements that are adopted.

We provide our specific comments and recommendations on each of these and other topics below.

II. Cybersecurity Risk Management Policies and Procedures

Proposed Cybersecurity Risk Management Rule 206(4)-9 would require investment advisers to adopt and implement written cybersecurity policies and procedures reasonably designed to address cybersecurity risks. Broadly speaking, we support the Commission's efforts to codify existing SEC cybersecurity guidance into one rule to make it easier for compliance professionals to adhere to generally-agreed-upon best practices. We commend the Commission for recognizing that cybersecurity policies and procedures should be tailored based on an adviser's business operations, complexity, and risks. We agree that there should not be a one-size-fits-all approach, and that an adviser should have discretion to determine which elements are relevant to its business and how they should be implemented, and which are not necessary or appropriate.

A. Background for Recommended Modifications.

We make several points as a threshold matter.

i. Cybersecurity policies and procedures are already effectively required under the Compliance Program Rule.

The Compliance Program Rule has been remarkably successful, and its significance should not be minimized. Its principles-based features have enabled the Commission and its staff to adapt the rule to new and evolving issues that were not even contemplated when the Compliance Program Rule was adopted, including cybersecurity. Because of the rule's evergreen feature, in many respects, the proposed cybersecurity policies and procedures reflect what firms are already required to have in place. Over the past several years, the SEC staff has issued specific expectations around cybersecurity policies and procedures through guidance and risk alerts. Those expectations form the basis for the Proposal, which is a testament to the Compliance Program Rule's flexibility and effectiveness.[8]

We understand that the Commission believes there are regulatory gaps to fill. However, we believe that any such gaps ideally should be filled using the existing Compliance Program Rule. We do not agree that "While some funds and advisers have implemented cybersecurity programs under the existing regulatory framework, there are no Commission rules that specifically require firms to adopt and implement comprehensive cybersecurity programs."[9] As discussed above, in addition to being part of an adviser's fiduciary duty, cybersecurity is already effectively required under the Compliance Program Rule in the business continuity context.[10]

[8] Some of the specific elements of the Proposal appear to be derived from prior SEC staff guidance and risk alerts, which reaffirms the importance of the principles-based approach under the Compliance Program Rule.

[9] Proposal at 13527.

[10] *See supra* n.5.

And, in fact, the SEC has brought cybersecurity-related enforcement actions against investment advisers.[11]

ii. A flexible, evergreen approach to cybersecurity, rather than prescriptive requirements, is key to achieving the Commission's overall goals.

Just as flexibility has been key to the Compliance Program Rule's success, an evergreen approach[12] is even more important when it comes to a fast-evolving area such as cybersecurity. We recognize that the Commission intended the Proposal to give each adviser some flexibility to tailor its cybersecurity policies and procedures to its business. We appreciate that the Proposal speaks in terms of policies and procedures that are "reasonably designed" to address cybersecurity risks. This reasonableness standard is key as advisers should not be expected to prevent all cybersecurity incidents or adopt a one-size-fits-all cybersecurity program but rather implement a program that is reasonable in light of their unique circumstances. The required elements, however, suggest a more particular set of regulatory expectations. Overly-prescriptive rules will not achieve the Commission's overall goals; a principles-based approach that allows for maximum flexibility consistent with an adviser's fiduciary duty and regulatory obligations is more in keeping with the Commission's intent and the spirit of a more collaborative approach to addressing cybersecurity risk, and likely to be more effective.

To the extent that examiners believe that some policies and procedures may not be adequate for an adviser's risks and operations, those concerns are best addressed through risk alerts and examination deficiencies rather than through prescriptive rule requirements.[13] It is increasingly difficult to keep pace with threat actors, particularly those that are state sponsored. No one – whether in the private or public sector – is immune. We appreciate that the Proposal recognizes that, "Even when cybersecurity preparations are high, a cybersecurity attack may

---

[11] The SEC has brought enforcement actions against advisers for cybersecurity-related violations, including not adopting and implementing adequate policies and procedures, under Regulation S-P and the Compliance Program Rule. *See, e.g.*, *In the Matter of R.T. Jones Capital Equities Management, Inc.*, Rel. No. 4204 (Sep. 22, 2015) (charging investment adviser with failing to adopt proper policies and procedures designed to safeguard customer information prior to breach); and SEC Press Release, *SEC Announces Three Actions Charging Deficient Cybersecurity Procedures* (Aug. 30, 2021) (sanctioning eight firms in three actions for failures in their policies and procedures that resulted in email account takeovers exposing the personal information of customers and clients, as well as misleading breach notifications).

[12] The Commission explicitly considered the importance of evergreen regulations "in the face of evolving technology and methods of communication" in adopting the new Marketing Rule for investment advisers *See Investment Adviser Marketing*, 86 Fed. Reg. 13024 (Mar. 5, 2021), available at https://www.govinfo.gov/content/pkg/FR-2021-03-05/pdf/2020-28868.pdf (**Marketing Rule Release**).

[13] As discussed throughout this letter, we strongly urge the Commission to work collaboratively with advisers to address cybersecurity threats when circumstances allow (*e.g.*, work together to help advisers, individually and collectively, to implement lessons learned and not focus on mere regulatory foot-fault violations that did not result in actual harm).

succeed."[14] All that can be expected is for firms to take reasonable steps to mitigate risks, contain incidents, learn from those, and improve going forward.

iii. Proposed new Rule 206(4)-9 is an anti-fraud rule.

We are concerned that the imposition of prescriptive cybersecurity requirements as part of an anti-fraud rule[15] seems fundamentally unfair. Foot-fault violations for failure to follow prescribed requirements would not necessarily reflect any substantive violation that harmed or even impacted clients. Moreover, technical violations of prescriptive requirements will likely be found in situations where advisers are themselves victims of cyber attacks. The fear of being found to have committed a fraud for what may have been an oversight in failing to comply with each of the prescriptive requirements under the rule could have the unintended consequence of making any response to a developing cybersecurity breach more difficult by unnecessarily raising the regulatory stakes of cybersecurity incidents. At a minimum, we ask the Commission to confirm in the adopting release that it would not characterize a technical finding of a deficiency in cybersecurity policies and procedures, or the mere fact that an adviser experiences a cybersecurity incident, as "fraudulent, deceptive, or manipulative acts, practices, or courses of business within the meaning of section 206(4) of the [Advisers] Act."

B. Recommended Modifications to Cybersecurity Risk Management Policies and Procedures.

While we generally support the proposed cybersecurity risk management policies and procedures, we offer comments and recommend certain modifications below to better reflect industry best practices for both larger and smaller firms, and not impose requirements that are overly prescriptive, cost prohibitive, or unrealistic. Given our concerns expressed below regarding the real potential of prescriptive requirements quickly becoming outdated, we recommend that the Commission consider a more flexible framework. The Commission could identify areas of Rule 206(4)-9 where it might be appropriate to give examples of measures advisers should consider taking,[16] rather than specifying specific controls. Our comments on specific provisions of the rule are below.

---

[14] Proposal at 13552. We agree with the point in the Proposal that "Although 'adequate' cybersecurity preparations can be expected to reduce cybersecurity incidents, they are unlikely to eliminate them entirely. For example, a firm may suffer a cybersecurity breach due to an attacker discovering a 'zero-day exploit' (*i.e.*, an exploit that is not generally known to exist) in some underlying IT system. As a practical matter, even the best preparation (*e.g.*, keeping up to date with vendor patches, quickly addressing vulnerabilities, etc.) may not be effective against such exploits. Similarly, for many firms, it may not be feasible to fix a known vulnerability immediately (*e.g.*, weakness in an encryption algorithm) as the fix may require upgrades to numerous systems. In this case, many firms could be exposed to a vulnerability for some time. Because the time it takes for an attacker to exploit such a vulnerability successfully is likely to involve some element of chance, firms that ultimately suffer an incident resulting from such a vulnerability may simply be 'unlucky.'" Proposal at n.197.

[15] Rule 206(4)-9 is proposed under Section 206(4) of the Advisers Act.

[16] As discussed above, the SEC examination program has taken this approach by sharing observations from examinations and explicitly encouraging firms to assess their own compliance programs in light of the observations.

i. The requirement for a prescriptive written information-protection contract between advisers and their service providers is unrealistic.

Under the proposed cybersecurity policies and procedures, an adviser would be explicitly required through written contracts to oversee any service providers that receive, maintain, or process adviser or fund information, or are otherwise permitted to access their information systems and any information residing therein. We generally support requiring reasonable oversight of service providers as part of an adviser's fiduciary and compliance responsibilities. We are concerned, however, about the provision to document – ***pursuant to a written contract*** between the adviser and any such service provider – that service providers are required to implement and maintain appropriate measures designed to protect adviser information and systems.

Commonly, advisers engage service providers through a "click-through agreement" or addendum in which an adviser agrees to accept the service provider's terms (including the service provider's security measures) with no opportunity to negotiate those terms. Even when a more traditional contract is presented, we understand that individual investment advisers (particularly smaller advisers) lack leverage to engage in contractual negotiations with certain service providers. We do not understand in these cases how an adviser can be expected to require service providers to include specific contractual language. Moreover, depending on the nature of a service provider's business, the service provider may not permit separate "oversight" of its cybersecurity policies by a third party. The Proposal, in effect, puts an adviser in the untenable position of acting as the guarantor of its service provider's information security program.

We understand that this provision likely derives from SEC staff guidance that states, "Funds, as well as advisers, may wish to consider reviewing their contracts with their service providers to determine whether they sufficiently address technology issues and related responsibilities in the case of a cyber attack."[17] However, we believe that the Proposal's requirement goes too far. We recommend that advisers instead be given the flexibility to oversee their service providers based on the nature and size of their businesses and in light of the risks posed by the facts and circumstances. We would not object to the Commission's suggesting in the adopting release that as part of an adviser's oversight obligations, the adviser ***may wish to consider*** updating, where possible, its contracts with its service providers to address any cybersecurity concerns. We also recommend that the Commission work with other entities under its jurisdiction (*e.g.*, broker-dealers and transfer agents) as well as with other federal agencies to regulate more directly the entities subject to those agencies' jurisdiction (*e.g.*, bank custodians) that act as service providers to advisers.

ii. The Commission should narrow the set of service providers for which advisers must assess compliance through risk assessments.

As proposed, the rule would require advisers to (i) categorize and prioritize cybersecurity risks based on an inventory of the components of their information systems, the information

[17] 2015 Guidance Update.

residing therein, and the potential effect of a cybersecurity incident on the advisers and funds, and (ii) identify their service providers that receive, maintain or process adviser or fund information,[18] or that are permitted to access their information systems, including the information residing therein, and identify the cybersecurity risks associated with the use of these service providers.[19]

The requirement to base an inventory on "components" of information systems, in our view, is too granular and appears to prescribe a disproportionately time-consuming mapping exercise that would apply to a much too broad set of service providers. We recommend permitting advisers to select which service providers to assess based on the adviser's periodic evaluation of which providers holistically raise the greatest risk of unauthorized access and potential client harm. We believe that this approach would have a more meaningful impact on an adviser's cybersecurity program.

iii. The Commission should clarify certain user security and access controls.

The proposed rule would require controls designed to minimize user-related risks and prevent unauthorized access to information and systems. Policies and procedures would have to include: (i) requiring standards of behavior for individuals authorized to access adviser or fund information systems and any adviser or fund information residing therein, such as an acceptable use policy; (ii) identifying and authenticating individual users, including implementing authentication measures that require users to present a combination of two or more credentials for access verification; (iii) establishing procedures for the timely distribution, replacement, and revocation of passwords or methods of authentication; (iv) restricting access to specific adviser or fund information systems or components thereof and adviser or fund information residing therein solely to individuals requiring access to such systems and information as is necessary for them to perform their responsibilities and functions on behalf of the adviser or fund; and (v) securing remote access technologies used to interface with adviser or fund information systems.[20]

We generally support requiring advisers to include these user security and access elements, which we view as current standard "blocking and tackling" security measures that clients and investors often expect as part of their due diligence. The Commission could consider including an additional cybersecurity program administration requirement for training staff responsible for day-to-day management of the program.

We note that prescribing specific elements (*e.g.*, authentication measures that require users to present a combination of two or more credentials for access verification, and even the very concept of "passwords") risks those requirements becoming outdated as technology evolves

[18] "Adviser information" is proposed to be defined as any electronic information related to the adviser's business, including personal information, received, maintained, created, or processed by the adviser.

[19] Proposed Rule 206(4)-9(a)(1).

[20] Proposed Rule 206(4)-9(a)(2).

and encourage the Commission to consider a more evergreen approach. If the Commission nevertheless prescribes certain user security and access controls, clarification would be helpful with respect to (i) the Commission's views on the use of single sign-on (SSO) authentication methods that enable users to securely authenticate multiple applications and websites by using a single set of credentials and (ii) examples of multi-factor authentication methods that may be acceptable.[21]

iv. We support the proposed threat and vulnerability management policies and procedures.

We support the proposed requirement that advisers detect, mitigate, and remediate cybersecurity threats and vulnerabilities with respect to adviser or fund information and systems.[22] We agree with the Commission that taking reasonable measures to manage threats and vulnerabilities is essential to preventing cyber incidents before they occur.

v. We support advisers having cybersecurity incident response and recovery policies and procedures.

The Proposal would require advisers to have measures to detect, respond to, and recover from a cybersecurity incident.[23] These include policies and procedures that are reasonably designed to ensure: (i) continued operations of the adviser; (ii) the protection of adviser information systems and the fund or adviser information residing therein; (iii) external and internal cybersecurity incident information sharing and communications; and (iv) reporting of significant adviser cybersecurity incidents to the Commission.[24]

We generally support this requirement with modifications, but believe that the definition of "cybersecurity incident" is very broad and should be principles-based. As it is not possible to anticipate every type of incident and it is unclear what "jeopardizes" means, we ask the Commission to clarify that the definition enables advisers to take into account the severity of the incident and have a plan in place that is tailored to the size and nature of their business.[25] We do not recommend requiring that advisers respond to cybersecurity incidents within a specific

[21] "Advisers and funds may wish to consider multi-factor authentication methods that are not based solely on SMS-delivery (*e.g.*, text message delivery) of authentication codes, because such methods may provide less security than other non-SMS based multi-factor authentication methods." Proposal at n.40.

[22] Proposed Rule 206(4)-9(a)(4).

[23] "Cybersecurity incident" is proposed to be defined for purposes of this section of the proposed rule as "an unauthorized occurrence on or conducted through an adviser's information systems that jeopardizes the confidentiality, integrity, or availability of an adviser's information systems or any adviser information residing therein." *See* Proposed Rule 206(4)-9(c) Definitions; Form ADV Glossary of Terms.

[24] Proposed Rule 206(4)-9(a)(5).

[25] The National Institute of Standards and Technology Cybersecurity (NIST) framework or International Organization for Standardization (ISO) framework could serve as a model for the definition. *See, e.g.*, ISO 27001: "information security incident" means a "single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security."

timeframe because cybersecurity incidents vary in scope and severity, as well as in the time it takes for advisers to get their arms fully around an incident. In addition, the Commission should recognize that having redundant systems is extremely expensive and is not the only way to address continuity of operations concerns.

vi. We support the proposed annual review and written reports with a clarification regarding the nature and scope of reviews.

The Proposal would require advisers, at least annually, to: (i) review and assess the design and effectiveness of the cybersecurity policies and procedures, including whether they reflect changes in cybersecurity risk over the time period covered by the review; and (ii) prepare a written report. The report would, at a minimum, describe the annual review, assessment, and any control tests performed, explain the results thereof, document any cybersecurity incident that occurred since the date of the last report, and discuss any material changes to the policies and procedures since the date of the last report.[26]

While we support an annual review, we think the Commission should make clear that, like regular compliance reviews, advisers should have the flexibility to tailor and scale these reviews based on their assessment of what they believe would be most effective in light of the firm's business and risks (*e.g.*, conduct tabletop exercises rather than check-the-box reviews). In response to questions posed in the Proposal, we do not believe it would be problematic for the same adviser personnel to implement the cybersecurity program and also conduct the annual review. In fact, this may be necessary at smaller firms. We also believe it would be burdensome and entirely unnecessary if advisers were required to have their cybersecurity policies and procedures periodically audited by an independent third party to assess their design and effectiveness and would strongly oppose such a requirement.[27] Moreover, we ask for confirmation that the cybersecurity annual review can be part of the Compliance Program Rule annual review.

vii. Fund Board duties should be oversight, and not management, in nature.

The Proposal would require a fund's board of directors (**Board**), including a majority of its independent directors, initially to approve the fund's cybersecurity policies and procedures, as

[26] Proposed Rule 206(4)-9(b).

[27] We agree with the Commission that the costs of an external audit would likely be considerably higher in part because, in order to provide assurances regarding an adviser's program, an audit firm would need "a thorough understanding of a registrant's systems and practices; in many cases, developing such an understanding would involve considerable effort." In addition, the Proposal notes, "it is possible that the inherent ambiguity of what represents 'effective' practices in an evolving context like cybersecurity would lead to a reluctance among third parties to provide the necessary certification services." Proposal at 13558. We believe that these costs would be unnecessarily high for advisers of all sizes.

well as to review the written report on cybersecurity incidents and material changes to the fund's cybersecurity policies and procedures that would be required to be prepared at least annually.[28]

We are concerned that some of the language in the Proposal could be interpreted as indicating that fund directors should take roles that are more appropriate for fund management than they are for the Board's oversight role. For example, the Proposal notes that "Board oversight should not be a passive activity"[29] and "a board may review the service provider contract and risk assessment…including the information residing therein and the cybersecurity risks they present…. Generally, the board should follow up regarding any questions on the contracts or weaknesses found in the risk assessments as well as the steps the fund has taken to address the fund's overall cybersecurity risks."[30] We agree that Board oversight should include reasonable inquiries about a fund's policies and procedures and written reports as part of the Board review process, but we recommend that the Commission clarify the description of the Board's duties so that they are oversight – and not management – in nature, particularly with respect to the oversight of contracts with service providers and service provider policies and procedures. We believe that negotiating service provider contracts and reviewing third-party policies and procedures are more indicative of fund management, especially where the contract involves highly technical and evolving issues.[31] Also, large firms that rely on a firm-wide cybersecurity program should not be required to have separate fund boards review, comment on, and approve the same set of cybersecurity policies and procedures.

viii. The proposed recordkeeping requirements should be narrowed and clarified.

The Proposal would require advisers to maintain records documenting the occurrence of "any cybersecurity incident" occurring in the last five years, including records related to any response and recovery from such an incident.[32]

We note that the proposed recordkeeping requirements under Rule 204-2 are for "the last five years," and are thus different from "a period of not less than five years from the end of the fiscal year during which the last entry was made on such record," which is the standard timeframe in Rule 204-2(e). Rule 204-2(e) explicitly excepts from its timeframe those provisions of 204-2 that have alternative recordkeeping periods. Only one of the five proposed recordkeeping provisions is explicitly identified in the proposed amendment to Rule 204-2(e). Therefore, we recommend a conforming amendment to Rule 204-2(e) as follows:

> **(1)** All books and records required to be made under the provisions of paragraphs (a) to (c)(1)(i), inclusive, and (c)(2) of this section (except for

[28] Proposed Rule 38a-2(c).

[29] Proposal at 13534.

[30] Proposal at 13535.

[31] As discussed above, we oppose the proposed requirement to have a written contract relating to cybersecurity controls of third-party service providers that would necessitate this specific type of contract negotiation.

[32] Proposed Rule 204-2(a)(17)(vi).

> books and records required to be made under the provisions of paragraphs (a)(11), (a)(12)(i), (a)(12)(iii), (a)(13)(ii), (a)(13)(iii), (a)(16), ~~**and**~~ (a)(17)(i), **(a)(17)(iv), (a)(17)(v), (a)(17)(vi), and (a)(17)(vii)** of this section), shall be maintained and preserved in an easily accessible place for a period of not less than five years from the end of the fiscal year during which the last entry was made on such record, the first two years in an appropriate office of the investment adviser.

III. Reporting of Significant Adviser Cybersecurity Incidents

Proposed new Rule 204-6 under the Advisers Act would require investment advisers to submit new Form ADV-C to the Commission on a confidential basis within 48 hours after having a reasonable basis to conclude that a significant adviser cybersecurity incident has occurred or is occurring. Advisers would need to amend any previously filed Form ADV-C "promptly," but in no event more than 48 hours after: (i) any information previously reported to the Commission on Form ADV-C pertaining to a significant adviser cybersecurity incident becoming materially inaccurate; (ii) any new material information pertaining to a significant adviser cybersecurity incident previously reported to the Commission on Form ADV-C being discovered; or (iii) any significant adviser cybersecurity incident being resolved or any internal investigation pertaining to such an incident being closed.[33]

We make the following comments and provide the following recommendations to improve the proposed reporting requirement:

- The Commission should coordinate with other federal regulators to adopt a holistic, uniform federal requirement for reporting cybersecurity and data breach incidents.
- The Commission should consider the confidentiality and potential vulnerability of the reports to further threats.
- Information sharing and collaboration based on aggregate Form ADV-C information are critical to addressing cybersecurity threats. Using reporting to assess "real-time" compliance efforts would be counterproductive.
- The Proposal may result in overreporting, unduly impede real-time response efforts, and add unnecessary operational and compliance burdens.
- The proposed 48-hour reporting filing window would be counterproductive to the Commission's goals of isolating and detecting market-wide attacks.
- The Commission should exclude smaller advisers from the reporting requirement.
- We support layered reporting of significant adviser cybersecurity incidents, consisting of a concise initial Form ADV-C within four business days and a final submission following the incident. Advisers should not be required to amend Form ADV-C prior to the final filing.

[33] Proposed Rule 204-6(a)(2)(iii).

- Advisers should not be subject to unnecessary regulatory scrutiny of information provided on Form ADV-C that was made in good faith based on information known at the time but turns out to be materially inaccurate.
- An adviser and sub-adviser should be permitted to file one report per incident and agree on who should report.
- Duplicative reporting on Form ADV-C and Form PF should be avoided.

A. The Commission Should Coordinate with Other Federal Regulators to Adopt a Holistic, Uniform Federal Requirement for Reporting Cybersecurity and Data Breach Incidents.

The IAA has long supported a uniform, national approach to cybersecurity regulation, including a consistent cybersecurity and data breach notification regime, to create consistency and reduce complexity.[34] Advisers currently face a burdensome, complex maze of federal and state requirements relating to cybersecurity and the reporting of data breaches that is difficult to navigate.[35] Multiple federal agencies have issued regulations or statements regarding data security.[36] And all 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have adopted an array of inconsistent data breach notification laws and regulations that add to the confusion and regulatory burdens.[37] For example, most, if not all, state laws require reporting of a data breach to affected individuals and state attorneys general, but these laws differ from one another and from federal regulation in several respects, including the timing and content of the notice. To add to this complexity, many states also are considering or have issued their own cybersecurity regulations.

If the Commission adopts its own cybersecurity incident reporting requirements, it would add yet another layer of complexity and related costs, making implementation and compliance

---

[34] *See* Letter from IAA President & CEO Karen Barr to SEC Chair Gary Gensler, *Regulation of Investment Advisers* (May 17, 2021), available at https://investmentadviser.org/resources/regulation-of-investment-advisers/.

[35] As discussed below, we urge the SEC to consider the cumulative costs of regulations on advisers. In our view, this analysis would be incomplete without also carefully considering the costs and burdens imposed on advisers by other federal and state agencies that have their own requirements regarding cybersecurity (*e.g.*, incident reporting).

[36] For example, as noted in the Proposal, "Recently, the Federal Deposit Insurance Corporation, the Board of Governors of the Federal Reserve System, and the Office of the Comptroller of the Currency adopted a new rule that would require certain banking organizations in the United States to notify Federal banking regulators of any cybersecurity incidents within 36 hours of discovering an incident" (Proposal at 13581). We also note that the Cyber Incident Reporting for Critical Infrastructure Act of 2022 will require "critical infrastructure entities," including those in the financial services sector, to report to the U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (**CISA**) (i) substantial cybersecurity incidents within 72 hours of reasonably believing that one has occurred, and (ii) ransom payments within 24 hours of payment. Section 2246 of the Strengthening American Cybersecurity Act of 2022, recently passed by the Senate, would create a Cyber Incident Reporting Council "to coordinate, deconflict, and harmonize Federal incident reporting requirements, including those issued through regulations."

[37] *See*, *e.g.*, National Conference of State Legislatures, Security Breach Notification Laws, available at https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

for advisers even more challenging. We believe it would be better for the Commission to withdraw the incident reporting aspect of the Proposal and instead coordinate with other federal regulators to adopt a uniform standard regarding cybersecurity and data breach notification that is risk-based and dependent on the facts and circumstances surrounding a breach. We also strongly support preemption of state regulation in this area.[38]

We nonetheless offer our recommendations for incident reporting below, which we believe will improve the Proposal should the Commission move forward. But first, we offer some important considerations for the Commission to bear in mind.

B. The Commission Should Consider Several Overarching Points Prior to Adopting Incident Reporting Requirements.

Prior to adopting any incident reporting regime for investment advisers, we strongly urge the Commission to carefully consider the following points.

i. The Commission should ensure the confidentiality of information in Form ADV-C, which is critically important to protecting the markets, advisers, and clients from more cybersecurity attacks.

It is critical to preserve the confidentiality of information in Form ADV-C, which would include sensitive information about an adviser's vulnerabilities, such as a description of the nature and scope of the incident, names of entities involved, planned actions to recover from the incident, whether any data was stolen, altered, accessed, or used for any unauthorized purpose, whether and how the incident has affected the adviser's critical operations, including which systems or services have been affected, and how any degradation in services provided by a service provider has affected the adviser's operations.[39]

We are very concerned with the statement in the Proposal that "our ***preliminary*** view is that Form ADV-C should be confidential given that public disclosure is neither necessary nor appropriate in the public interest or for the protection of investors" (emphasis added). We urge the Commission to confirm, prior to any adoption, that Form ADV-C will in fact be kept confidential. The information proposed to be reported to the Commission includes, among other things, highly specific details regarding an adviser's cybersecurity program, including protocols and incident response plans. If this information were to be made public, we believe that it has the

[38] We have supported legislative efforts to enact a uniform, preemptive federal data breach notification regime. Absent a legislative approach, federal agencies can and have coordinated on rulemakings affecting a broader swath of firms (*e.g.*, the Federal Trade Commission's recently-amended Standards for Safeguarding Customer Information (**FTC Safeguards Rule**) with respect to data security requirements to protect customer financial information). Accordingly, the IAA urges the SEC to engage with other Federal agencies and departments on a joint rulemaking for a coordinated and comprehensive breach notification regime.

[39] *See* Proposal at 13539.

real potential to provide threat actors with an easily accessible roadmap to an adviser's vulnerabilities.

We note that Form PF reports are explicitly made confidential under Section 204(b) of the Advisers Act pursuant to amendments made by the Dodd-Frank Act. We are concerned that Form ADV-C filings would not be entitled to the same explicit statutorily-provided confidential treatment.

Section 210(a) of the Advisers Act states that "[t]he information contained in any . . . report or amendment thereto filed with the Commission pursuant to any provision of this title shall be made available to the public, unless and except insofar as the Commission, by rules and regulations upon its own motion, or by order upon application, finds that public disclosure is neither necessary nor appropriate in the public interest or for the protection of investors." It is critical to protect this sensitive information and we urge the Commission to use its authority under Section 210(a) to keep this information from public disclosure. Thus, we ask for explicit confirmation that the Commission will attempt to ensure the confidentiality of the proposed reports on Form ADV-C and that these confidential reports will not be released to the public (*e.g.*, pursuant to Freedom of Information Act requests).[40] We also urge the Commission to maintain robust measures to implement adequate protections to ensure that Form ADV-C information is not inadvertently disclosed.

ii. Despite the Commission's best efforts, cybersecurity information filed with the agency has the potential to be accessed by bad actors, in some instances as the reported incident is occurring, to the detriment of the markets, advisers, and clients.

No one – not even the Commission itself – is immune from its systems and the information residing therein being accessed by a bad actor. The SEC in fact is a particularly obvious target for cybersecurity incidents with significant market-wide consequences given its status as a high-profile federal agency responsible for regulating the U.S. financial markets. As proposed, the reporting requirements would require advisers to file detailed sensitive data regarding a cybersecurity incident electronically, in many instances as the threat is occurring. We are concerned that the electronic transmission and the collection and storage of this information in a centralized electronic repository would make the SEC an even higher-value target for bad actors.[41] Any unauthorized access to sensitive information regarding an adviser's cybersecurity incidents, protocols, and response measures could provide a roadmap for bad actors to further

[40] We urge the Commission, to the extent that it shares information regarding cybersecurity incidents with other regulators, to develop strong protocols to ensure the confidentiality of such information.

[41] We are particularly concerned that the Commission proposes to use the Investment Adviser Registration Depository (IARD) system for this purpose. This is the same system used for Form ADV filings, which are intended to be made public. We are thus not confident that this system as currently designed can adequately protect the confidentiality of the proposed reports. We note that the SEC and NASAA developed an alternative registration system, the Private Fund Reporting Depository, for Form PF filings, presumably to ensure nonpublic disclosure. We urge the Commission at a minimum to develop a similar nonpublic SEC system for Form ADV-C filings with appropriate cybersecurity system protocols prior to the compliance date for any new filing requirements.

target the adviser and other investment advisers or adjust its ongoing attacks accordingly, and has the potential to disrupt the broader financial markets.

For the same reasons, we recommend that the Commission consider alternative methods – other than electronic – for reporting incidents,[42] for example, in situations where an adviser's systems are under threat or reporting electronically would increase the risk of further harm, hamper the chances of recovery of stolen funds, or impede the detection of wrongdoers.[43]

iii. Information sharing and collaboration are critical to addressing cybersecurity threats overall; using reporting to assess "real-time" compliance efforts would be counterproductive.

We support the Commission's efforts to collect data to monitor for broader cybersecurity threats. Moreover, we also believe that it is equally vital, if not more, that the Commission use the data it collects on an unidentified and aggregated basis for the purpose of sharing information with market participants more broadly to collectively address emerging cybersecurity threats.[44] Information sharing with respect to cybersecurity incidents (*e.g.*, ransomware) is critical to helping advisers with their preparation and responses.[45] We believe that sharing of information that is timely, but accurate, is the single best tool the SEC can and should use against cybersecurity threats generally.[46] Advisers welcome this collaborative approach and have found past SEC alerts regarding cybersecurity incidents to be extremely useful in addressing emerging cybersecurity threats. For example, we continue to support timely and accurate risk alerts

---

[42] Alternative reporting methods could include (i) a secure telephone hotline, (ii) an encrypted email system (*i.e.*, like the one used by advisers to submit requested documents to SEC staff pursuant to an examination), and/or (iii) a dedicated encrypted email address to receive such reports, similar to that used for the Share Class Selection Disclosure Initiative. *See SEC Division of Enforcement Announcement*, available at https://www.sec.gov/enforce/announcement/scsd-initiative.

[43] For example, a "Temporary Hardship Exemption" permits advisers "to extend the deadline for a filing for seven business days if unexpected difficulties, such as a computer malfunction or electrical outage, prevent the firm from filing electronically. The Temporary Hardship Exemption is available automatically upon filing a paper Form ADV-H. Note: After the Temporary Hardship expires, the Investment Adviser must electronically submit its ADV filing." *See* IARD, *Hardship Exemptions*, available at https://www.iard.com/support_hardship#:~:text=A%20Temporary%20Hardship%20Exemption%20permits,the%20firm%20from%20filing%20electronically.

[44] We would expect the Commission to be able to notify market participants of attacks that could be or are affecting many firms (*e.g.*, ransomware or malware) without revealing firm-specific information.

[45] This information would also enable Commission staff to respond to investor inquiries in the event of an incident at a specific adviser. We understand that the staff has fielded such calls in the past when investors were unable to reach their advisers. Moreover, we note that this information could also be used by the staff in connection with ongoing outreach efforts to individual firms.

[46] *See Executive Order on Improving the Nation's Cybersecurity* (May 12, 2021), available at https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (**Executive Order**). ("Removing these contractual barriers and increasing the sharing of information about such threats, incidents, and risks are necessary steps to accelerating incident deterrence, prevention, and response efforts and to enabling more effective defense of agencies' systems and of information collected, processed, and maintained by or for the Federal Government.")

published by the Division of Examinations regarding ransomware and other types of attacks.[47] In this regard, as we discuss below, for this information sharing to be useful in addressing such emerging threats, it is important that advisers be given sufficient time and leeway to file incident reports that are accurate based on information known at the time of filing. However, the Proposal also appears to suggest that the reporting requirements would serve to support the Commission's examination program in assessing firms' preparedness and resiliency to cyber attacks once they begin to occur.[48]

We do not believe that incident reporting should be used to assess compliance in "real time" or play "gotcha" in this manner. We would have significant concerns if the proposed reporting requirements were intended to target advisers that are experiencing cybersecurity incidents to make unnecessarily expedited "real-time" compliance assessments of their cybersecurity policies and procedures. This approach would add an unfortunate distraction to the detriment of investors and significantly hamper an adviser's ability to contain and mitigate attacks as it attempts to balance addressing the ongoing threat and responding to regulatory filing obligations or scrutiny by the SEC staff.

The very nature of cybersecurity attacks has the potential to be highly complex and fast-evolving, thus placing tremendous pressure on advisers as they attempt to respond to and contain incidents as they are happening. We think it would be counterproductive for the examinations staff to pass judgment on advisers for their incident response efforts in light of this pressure. Not only would we object to examiners conducting any review during the time advisers are engaged in incident response, but we also believe it would be counterproductive for staff to second guess after the fact how the adviser exercised its judgment in the heat of the moment.

Any effort by the Commission to evaluate controls in light of an attack should occur ***after*** the attack no longer presents an ongoing threat and during the normal course of the SEC's examinations. In addition, to the extent the proposed reporting obligation leads to further scrutiny of the adviser's specific policies and procedures and its handling of a breach, we urge examinations staff to attempt to work collaboratively with the adviser by sharing relevant observations and providing useful feedback for improvements to its program rather than looking to find deficiencies or make enforcement referrals. We also believe that staff should use these exams as an opportunity to help other advisers improve their cybersecurity program (*e.g.*, through risk alerts summarizing observations and sharing how other firms may have responded to the same incident).[49] We believe that such efforts would better assist firms constructively in assessing and managing their cybersecurity risks going forward.

---

[47] *See supra* n.6.

[48] "We believe that collecting information in a structured format would enhance our staff's ability to carry out our risk-based examination program and other risk assessment and monitoring activities effectively." Proposal at 13538.

[49] *See, e.g.*, Executive Order (noting, among other things, that "[p]rotecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector").

C. The Proposed Cybersecurity Reporting Requirements may Result in Overreporting Incidents, Unduly Impede Real-Time Response Efforts, and Add Unnecessary Operational and Compliance Burdens.

The IAA agrees that an appropriately-tailored breach notification regime would "allow the Commission and its staff 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." The Commission elaborates that "requiring advisers and funds to report the occurrence of significant [adviser] cybersecurity incidents would bolster the efficiency and effectiveness of our efforts to protect investors, other market participants, and the financial markets in connection with cybersecurity incidents."[50]

While we generally support the proposed incident reporting requirements in principle, subject to the above overarching considerations, we are concerned that the specific wording of the requirements could be interpreted as being overly expansive. This could result in overreporting incidents to the Commission, which may hinder the agency's ability to isolate and address threats to the markets more broadly. We are also concerned that the proposed 48-hour deadline for reporting incidents would potentially impede real-time response efforts by advisers to protect clients from further potential harm and add unnecessary operational and compliance burdens, contrary to the Commission's stated objectives.[51] We offer recommendations in this Section C and in Section D below that we believe will tailor the proposed reporting requirements in a way that will more effectively achieve the Commission's goals while reducing the burdens on advisers or the risk of impeding their ability to respond to significant cybersecurity incidents.

i. The proposed definition of "significant adviser cybersecurity incident" could be interpreted too broadly and potentially detract from the Commission's ability to detect market-wide cybersecurity incidents.

Under the Proposal, a significant adviser cybersecurity incident that would need to be reported on new Form ADV-C within 48 hours would be defined as "a cybersecurity incident, or a group of related cybersecurity incidents, that significantly disrupts or degrades the adviser's ability, or the ability of a private fund client of the adviser, to maintain critical operations, or leads to the unauthorized access or use of adviser information, where the unauthorized access or use of such information results in: (i) substantial harm to the adviser, or (ii) substantial harm to a client, or an investor in a private fund, whose information was accessed."[52] We are concerned

[50] Proposal at 13526.

[51] The proposed reporting requirements would be particularly onerous for smaller advisers with limited resources and in-house technical expertise. *See* Section V below.

[52] Proposed Rule 204-6(b).

that a broad interpretation of the triggering event for reporting would lead to significant overreporting and be counterproductive to the Commission's goals.

a. Prong one – Significant disruption or degradation of critical operations lacks sufficient clarity and could result in overreporting.

As stated in the Proposal, the first prong of the definition involves a ***significant*** disruption or degradation of ***critical*** operations and is primarily intended to help the Commission monitor and evaluate the effects of a breach on an adviser and its clients in furtherance of detecting industry-wide cybersecurity threats requiring the Commission's attention or action to protect the markets and investors.[53] We appreciate the Commission's proposal to limit the types of incidents required to be reported in this manner. However, we are concerned that the phrases "significantly disrupts or degrades" and "critical operations" lack sufficient clarity and could be broadly interpreted and thus result in advisers overreporting incidents that are highly unlikely to involve other advisers or impact the markets, contrary to the Commission's intent.

We suggest that the Commission confirm that these terms are intended to set a high threshold for reportable incidents to ensure that only information regarding truly significant cybersecurity incidents, *i.e.*, truly significant to that particular adviser based on all the facts and circumstances, is reported, in furtherance of the agency's objective to monitor and detect industry-wide cybersecurity threats.[54]

We agree, for example, that a ransomware or malware attack where clients are unable to access their money or financial-transaction processing is impeded would, unless quickly remediated, generally constitute a significant "disruption" or "degradation" of critical operations absent other circumstances (*e.g.*, backup systems). By contrast, we would expect that an incident involving a relatively time-limited computer system failure resulting in a loss of electronic communications (*e.g.*, e-mail) with clients, but where the adviser maintained the ability to call or text clients and effect trades, would likely not constitute a significant disruption or degradation of critical operations. Moreover, while we agree that systems involving portfolio management and trading should generally be deemed critical to an adviser's operations, we do not believe, for example, that all systems used by an adviser to "operate in accordance with the federal securities laws" should be regarded as critical in the context of triggering a reporting requirement. For

[53] We understand that the Commission also intends to use this data to evaluate the effects of the incidents on the adviser and its clients. As discussed above, we would have significant concerns if the proposed reporting requirements were intended to target advisers that are experiencing cybersecurity incidents to make "real-time" compliance assessments. We note that the data collected from advisers regarding cybersecurity incidents would also be records subject to inspection during examinations.

[54] We would oppose any quantitative threshold at which operations must be impaired by a cybersecurity incident before an adviser's or fund's obligation to report is triggered (*e.g.*, as suggested by the Commission, "maintaining operations at minimally 80% of current levels on any function") because we question whether advisers would be able to make such an assessment reliably, especially under the reporting time constraints.

example, a system used for recordkeeping under Rule 204-2 under the Advisers Act should not by itself be considered "critical," absent other facts and circumstances.

b. Prong two – Unauthorized access or use that results in substantial harm to the adviser or a client should be clarified and involve more than one client.

The second prong of the proposed definition focuses on the "unauthorized access or use of adviser information, where the unauthorized access or use of such information results in: (i) substantial harm to the adviser; or (ii) substantial harm to a client, or an investor in a private fund, whose information was accessed." We generally support requiring advisers to report to the SEC information on data breaches that resulted in actual substantial harm to clients. However, we recommend that the SEC only require reporting under prong two with respect to substantial harm to more than one client and clarify the meaning of "substantial harm" to clients for reporting purposes.

1. Prong two should be limited to substantial harm to more than one client.

We recommend that the Commission limit the unauthorized access or use reporting requirements to an incident involving more than one client rather than a single client as proposed. Erring on the side of overreporting could result in the Commission being inundated with frequent incident report filings regarding data breaches, most of which would likely not serve the agency's stated objectives and conversely could overwhelm the SEC staff and its systems. Specifically, we are concerned that the sheer number of filings involving only a single client would make it unnecessarily more difficult for the Commission to sift through them to detect and isolate an ongoing widespread cybersecurity threat. As a practical matter, we believe that a data breach incident involving only a single client, absent other facts, is generally not indicative of a broader cybersecurity threat involving the adviser, and, more typically, is the result of human error – including by clients (*e.g.*, a client's personal email containing sensitive account information is breached due to the client sharing the password) – or individual identity theft involving client information maintained at an unrelated entity.

We recognize, however, that an incident involving a single client could potentially reveal a broader cybersecurity threat that is significantly affecting the adviser's critical operations that could be required to be reported under prong one of the definition. We also acknowledge that an incident involving a single client has the potential to be a precursor to more incidents involving other clients. However, we believe that real-time monitoring of isolated incidents involving a single client to enable the Commission to proactively contain or accurately recognize the incident for what it is could be an extremely difficult task. In our view, limiting the filings to those involving more than one client – unless, as noted above, prong one is also satisfied – would substantially increase the Commission's chances of detecting widespread threats, which we support.

2. A "substantial harm" determination should not be second guessed.

As proposed, the Commission describes "substantial harm" as including "among other things, significant monetary loss or theft of intellectual property" of a client.[55] We note that whether harm to a client or private fund investor is substantial can be subjective and not necessarily known at the outset of a breach. Depending on the type and duration of the breach, and the resources, investment profile, and risks of a particular client, the amount of harm to client assets or investments[56] could vary greatly from client to client. We believe that it is thus important for the Commission not to second guess a "substantial harm" determination made in good faith by an adviser under the facts and circumstances known at the time.

The Commission also requests feedback on whether an "inconvenience" should be included as a threshold in determining substantial harm to shareholders, clients, and investors. We strongly oppose this inclusion because it would be enormously burdensome for advisers and highly subjective to determine whether a single breach is an "inconvenience" to a particular client. We also caution against this inclusion because, in our view, it would likely result in a magnitude of filings that would be irrelevant to the Commission's overarching goals, especially given the tremendous increase in time and effort that would be imposed on the SEC staff to review these filings.

ii. The proposed 48-hour reporting filing window and related amendments would be counterproductive to the Commission's goals of isolating and detecting market-wide attacks while unduly impeding real-time response efforts, to the detriment of investors.

The Commission is proposing that advisers electronically file a Form ADV-C "within 48 hours after having a reasonable basis to conclude that a significant adviser cybersecurity incident occurred or is occurring" with respect to itself or any of its covered clients. We are concerned that such an extremely narrow 48-hour window, with no flexibility built in, to report detailed information regarding a cybersecurity incident to the agency would unduly impede real-time responses of advisers that could lead to further harm to investors.

When an investment adviser experiences a significant cybersecurity incident, the first few hours and days are the most critical to contain the incident. An adviser may be working to lock out the attackers, protect and recover information and contain other damage, ascertain the scope of the incident, partner with law enforcement, and notify clients under myriad state data breach

---

[55] The Commission notes that with respect to investors in private funds, this list could also include "the theft of personally identifiable or proprietary information [(**PII**)]." We suggest that the Commission clarify why PII is included in the list of harm to private fund investors but not to clients.

[56] As the Proposal notes: "For example, cybersecurity incidents caused by malicious software (also known as malware) can cause the loss of adviser, fund, or client data. Cybersecurity incidents can prevent an adviser or fund from executing its investment strategy or an adviser, fund, client, or investor from accessing an account, which can lead to financial losses for clients or investors. In addition, cybersecurity incidents can lead to the theft of intellectual property, confidential or proprietary information, or client assets." Proposal at 13525.

notification laws. As advisers increasingly rely on third-party service providers and infrastructure outside of their firms such as the cloud to hold data, these steps take even more time.

We appreciate that the Commission would expect an adviser to "generally gather relevant information and perform an initial analysis to assess whether to reasonably conclude that a cybersecurity incident has occurred or is occurring and follow its own internal communication and escalation protocols concerning such an incident before providing notification of any significant cybersecurity incident to the Commission."[57] However, we believe that the proposed 48-hour window for reporting significant cybersecurity incidents to the Commission is too short and would put too much pressure on advisers to focus on reporting rather than on containing and remediating the threat. It is often not possible for an investment adviser to assess the depth and breadth of an incident right away, particularly with respect to the number of clients affected and whether the attack is ongoing. It is commonly agreed that cybersecurity incidents are often complex and fast-changing. They may involve partnering with many different IT and operations personnel, human resources, boards of directors (if applicable), third-party service providers, insurance companies, and legal counsel. Fact finding often includes interviewing staff, conducting forensic testing, and working with law enforcement. Because the experts with technical expertise are not necessarily the same personnel who are responsible for Form ADV filings, coordination is needed, which also takes time.

The Commission notes its view that the "48-hour period would give an adviser time to confirm its preliminary analysis and prepare the report while still providing the Commission with timely notice about the incident."[58] However, we note that the 48-hour period appears to start regardless of whether the incident has concluded or is ongoing. Making even a "preliminary analysis" as to the nature of the threat, including whether systems are still at risk, can take time, particularly for smaller to mid-sized firms that have limited resources or rely on outside experts for assistance. We also note that advisers are already subject to other regulatory reporting requirements as well as reports to insurance companies that are contractually required to be filed within a limited timeframe, and a 48-hour reporting SEC requirement would simply add an additional regulatory burden while the adviser is attempting to ward off a cyber attack.

We are also concerned that prior to any definitive assessment by advisers – in most cases by IT experts or outside consultants – virtually all cybersecurity incidents affecting critical systems have the *potential* to be reportable under the proposed definition, because typically, so much is still unknown. We are concerned that, given the regulatory risks of potentially violating an SEC rule,[59] advisers would likely err on the side of overreporting cybersecurity incidents, which would be of little use to the Commission's objective.

---

[57] Proposal at n.65.

[58] Proposal at 13537.

[59] The fact that a rule violation in this instance would essentially result in a violation of the anti-fraud provisions of the Advisers Act further exacerbates this concern.

Last, but perhaps most importantly, we believe it would be potentially harmful to clients to compel an adviser to make such specific determinations under such a tight deadline. In our view, firms should be encouraged to devote their time and resources to addressing and containing an attack to protect their clients and themselves from further harm prior to any time-consuming reporting obligation. We appreciate the Commission's desire to be notified timely, but strongly believe that regulatory reporting should not take precedence over protecting advisers and their clients. Advisers should be permitted the time they reasonably need to identify, respond to, and contain cybersecurity attacks that are ongoing.

We make recommendations below that we believe would address our concerns about the timing and content of the required reporting and better balance the Commission's objectives and the adviser's ability to respond effectively to a significant cybersecurity incident. But first, we discuss our recommendation that the Commission exclude smaller advisers from the reporting requirement.

iii. The Commission should exclude smaller advisers from the reporting requirement.

While 48-hour reporting would present a challenge even for the largest advisers, it would be especially difficult for smaller advisers that may not have the resources, staffing, and expertise to report within the proposed timeframe. Most smaller advisers, for example, may only have part-time IT staff rather than a dedicated chief information security officer (CISO). Smaller advisers thus would likely need to engage outside information security experts.

We believe that the Commission should exclude smaller advisers from the requirement to report significant adviser cybersecurity incidents.[60] Because a cyber attack against a smaller adviser is much less likely to have market-wide implications, we do not believe that the Commission should impose unnecessary burdens on these small businesses in an effort to monitor incidents involving them. In addition, we expect that the Commission would generally be made aware of incidents that could be affecting multiple advisers, including smaller advisers, through reporting that would be required by other larger advisers, related distribution platforms, or service providers that are subject to the Commission's jurisdiction.

Excluding smaller advisers from reporting would also have the advantage of limiting the number of immaterial filings on Form ADV-C, enabling Commission staff to focus on incidents at advisers that are much more likely to have broader implications, including harm to a larger swath of investors.

Perhaps the most important consideration in favor of excluding smaller advisers from coverage of proposed new Rule 204-6 and the corresponding proposed Form ADV-C is the significant reporting-related costs and burdens that would be imposed on smaller advisers that would be ***in addition*** to the cumulative impact of existing regulations that have already

[60] Proposal at 13538, Question 42. We provide our recommendations regarding the definition of a small adviser for purposes of this exclusion below.

tremendously burdened these small businesses. We also note that the SEC is considering many new regulations that would place still more regulatory – and cost – pressure on smaller advisers.

Moreover, as we discuss below, we are concerned that the Commission is underestimating the quantifiable costs of the Proposal, particularly on smaller advisers. These firms tend to be more resource constrained, and are more likely to need to consult with outside experts to assist with reporting. On balance, we believe that these burdens significantly outweigh the minimal usefulness to the Commission of receiving this information from smaller advisers through a Form ADV-C report. We note that the Commission would still maintain the ability to separately evaluate smaller firms' handling of significant adviser cybersecurity incidents as part of the agency's examination program.

Given the short comment period for the Proposal, we have not had sufficient time to analyze the data to provide a thoughtful recommendation on how to define "small adviser" for purposes of the exclusion.[61] We and our members would be pleased to discuss with the staff an appropriate definition for purposes of the reporting requirement that is more in line with what the data shows is the reality of today's business environment.

D. IAA Recommendations for Reporting Significant Adviser Cybersecurity Incidents.

We support layered reporting of significant adviser cybersecurity incidents, consisting of an initial and final submission on Form ADV-C. Under this approach, an initial submission would be submitted within four business days after determining that a significant adviser cybersecurity incident has occurred or is occurring. The second and final submission would be submitted after the resolution of the incident or after closing any internal investigation related to a previously disclosed incident. As we discuss below, we do not believe that ongoing reporting between these two reports is necessary or that it would be particularly useful.

We also request clarification of the circumstances that trigger a reporting obligation. We also ask that the SEC confirm that advisers that act in good faith should not be subject to strict regulatory scrutiny for reporting information on Form ADV-C that, in hindsight, was materially inaccurate. Finally, we ask the Commission to clarify sub-adviser reporting and provide an exception to the proposed Form PF reporting – should that be required under the Commission's Form PF proposal – when the adviser has filed a Form ADV-C, to avoid duplicative reporting.

The IAA's recommendations and requests are detailed below.

---

[61] For example, the median number of non-clerical employees of SEC-registered investment advisers was eight at the end of 2020, with 58 percent of SEC-registered advisers having fewer than 10 non-clerical employees and 87.9 percent having fewer than 50 non-clerical employees. *See IAA-NRS Investment Adviser Industry Snapshot 2021* (July 2021), available at https://higherlogicdownload.s3.amazonaws.com/INVESTMENTADVISER/aa03843e-7981-46b2-aa49-c572f2ddb7e8/UploadedImages/publications/industry-snapshots/Investment_Adviser_Industry_Snapshot_2021.pdf (**Industry Snapshot**).

i. A concise, initial Form ADV-C should be submitted to alert the Commission to important information once a determination has been made that a significant adviser cybersecurity incident has or is occurring.

We recognize the Commission's interest in learning early of a significant adviser cybersecurity incident to allow it to identify and monitor potential market-wide threats. We believe that this goal can be effectively met by requiring advisers to submit an initial concise high-level Form ADV-C filing within four business days of a determination by the adviser that such an incident has occurred or is occurring. For the reasons discussed below, we recommend that the initial report include key information in the check-the-box format such as that proposed in Items 1-10 of Form ADV-C: (1) SEC file number, (2) full legal name, (3) business name, (4) address of principal place of business, (5) contact information for an individual, (6) whether the reportable incident involves any covered clients (a registered investment company, business development company, or private fund, along with its applicable ID number or SEC file number), (7) approximate date(s) the reportable incident occurred, if known, (8) approximate date the reportable incident was discovered, (9) whether the reportable incident is ongoing, and if not, the approximate date the reportable incident was resolved or any internal investigation was closed, and (10) whether law enforcement or a government agency (other than the Commission) has been notified about the reportable incident, and if yes, which ones have been notified.[62] We suggest also adding to this initial report a new Item (11): the general nature and type of attack, if known (*e.g.*, malware, ransomware, phishing) and whether the reportable incident is included on a CISA or FS-ISAC list and, if so, the name of the incident (*e.g.*, SolarWinds, Kaseya, Log4j, Okta).

In our view, the information requested in Items 1-10 is more than sufficient for the Commission to be alerted regarding the fact that a significant adviser cybersecurity incident has occurred or is occurring. In addition, our new proposed Item 11 would provide information on the type of incident and whether it is part of a known attack. We believe that these reporting items would provide the Commission with the critical and relevant information it needs to monitor and detect emerging cybersecurity attacks and to assess whether the reported incident presents a threat to other firms and markets more broadly. This information could also form a basis for the Commission to prioritize its outreach to advisers to obtain more information, as necessary, if there are multiple Form ADV-C filings in the same time period."[63] We believe this data should easily allow the Commission to identify patterns that are occurring at other advisers and take steps to help contain potential market-wide effects, including, for example, informing advisers on an anonymized and aggregated basis of similar incidents that are occurring at other firms.

We believe, however, that the information required in proposed Items 11-16 is significantly more detailed than would be reasonably necessary to alert the Commission to developing threats and that these items should not need to be included in the initial report. In

[62] As noted by Commission, proposed Item 10 would assist the Commission in coordinating with governmental authorities, which the IAA strongly supports.

[63] Proposal at 13538.

addition to imposing unnecessary burdens on advisers while they are in the process of responding to an incident, the level of specificity proposed in these items would, in our view, result in reporting a substantial amount of information that would not add to the Commission's ability to identify and monitor market-wide risk.

We do not support including proposed Item 16 regarding insurance coverage because we do not believe that it serves any regulatory purpose. Whether or not firms have insurance policies bears no direct relevance to the adequacy of required policies and procedures. While advisers may choose to obtain insurance coverage, among other reasons, to ensure that adequate resources are available during or after a cybersecurity incident, the adviser bears the ultimate responsibility to ensure it has adequate resources, whether developed internally or outsourced to a third-party incident response service. We also do not believe there is much, if any, benefit to the Commission from obtaining this information through a Form ADV-C report given that the purpose of the report is to help the Commission monitor, detect, and address market-wide impacts. Moreover, we understand that a common tactic of threat actors is to determine which companies have cybersecurity insurance and then target those companies on the belief that they have the ability to pay. Therefore, any perceived benefit to the Commission of obtaining this information would be significantly outweighed by concerns regarding the potential of threat actors to target the SEC's systems to access this highly-sensitive information and specifically target those firms with insurance.

The Commission suggests that this information would assist it "in understanding the potential effect that [a significant cybersecurity] incident could have on an adviser's clients" and "in evaluating the adviser's response to the incident given that cybersecurity insurance may require an adviser to take certain actions during and after a cybersecurity incident."[64] We do not disagree that this information could be useful to the Commission. However, we note that it would be maintained by the adviser as part of its recordkeeping obligations and be made available to the Commission in a more secure manner through an examination staff's request to obtain these records. The Commission would be able to meet its objective of understanding the specific impacts of an incident on an adviser and its clients without collecting through the Form ADV-C reports more sensitive information than is necessary for its market-monitoring purposes.

ii. The initial filing of Form ADV-C should be submitted within four business days of determining that a significant adviser cybersecurity incident has occurred or is occurring.

As an initial matter, to limit the number of potential false positive reports and to provide advisers with a greater degree of certainty around their reporting obligations, we suggest that, instead of the reporting requirement being triggered when the adviser has a "reasonable basis to conclude" that a significant adviser cybersecurity incident has occurred or is occurring, it be triggered when the adviser has made a determination that a significant cybersecurity incident has

[64] Proposal at 13539.

occurred or is occurring.[65] We also suggest that it is not necessary for the Commission to include the word "promptly" in the window for reporting because it is unnecessary given an explicit deadline for reporting. Providing clearer parameters for the reporting trigger would significantly reduce uncertainty for advisers while they are in the heat of responding to an incident while also providing the Commission with the information it needs on a timely basis. In some cases, the date of the adviser's initial significance determination will coincide with the date of discovery of an incident, but in other cases the determination will be made after the discovery date. We agree with the Commission that advisers would be expected to be diligent in making this determination in as prompt a manner as feasible. To address any concern that some advisers may delay making such a determination to avoid a reporting obligation, the instructions to Form ADV-C could state: "an adviser shall make a determination regarding whether an adviser cybersecurity incident is significant as soon as reasonably practicable after discovery of the incident."[66]

With respect to the amount of time an adviser should have for the initial filing of a Form ADV-C, as described above, we urge the Commission to allow for filing within four business days after the adviser determines that a significant adviser cybersecurity incident has occurred or is occurring.[67] This timing would be consistent with the SEC's proposed cybersecurity notification rules for public companies,[68] and would allow advisers a more reasonable time to respond to the situation.

We believe that the timing and trigger we recommend would afford advisers a more reasonable window to get their arms around the magnitude of a cybersecurity incident and to

---

[65] A report would not be required, for example, in a situation where the adviser initially believes (has a reasonable basis for concluding) that its systems have been attacked by ransomware, but, following some additional preliminary investigation, is able to make a determination that the incident is insignificant. The adviser could, for example, end up determining that the bad actor's ransom demand was without merit (*e.g.*, the bad actor does not have the client information it claims to have) or was in the guise of a broad attack but was in fact a very limited physical theft (*e.g.*, the bad actor only has limited client data that is relatively harmless and/or affecting very few clients).

[66] The Proposal states that: "Once the adviser makes the determination that an incident would meet the definition of a significant cybersecurity incident, it is required to report on Form ADV-C within 48 hours." Proposal at 13583. We believe that this construction of the trigger provides greater certainty than use of the terms "a reasonable basis to conclude" and "promptly." This would also be more consistent with Instruction 1 to proposed Item 1.05 of the Commission's cybersecurity proposal for public companies, which states "a registrant shall make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident." *See Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, 87 Fed. Reg. 16590 (Mar. 23, 2022), available at https://www.govinfo.gov/content/pkg/FR-2022-03-23/pdf/2022-05480.pdf (**Public Companies Cyber Proposal**).

[67] As noted in Section III.B.ii above, in addition to our concerns regarding bad actors gaining access to sensitive information through electronic filings, we also note that if an adviser is experiencing a breach that significantly impacts its systems (*e.g.*, a ransomware attack), it may be prevented from meeting the filing deadline and should be able to rely on a temporary hardship filing to automatically extend an adviser's electronic filing deadline for seven business days (consistent with other Form ADV hardship provisions), as discussed in note 42. *See* https://www.sec.gov/divisions/investment/iard/iardfaq.shtml#hard.

[68] *See* Public Companies Cyber Proposal (proposing to require registrants to disclose information about a cybersecurity incident within four business days after the registrant determines that it has experienced a material

allocate their internal resources more effectively to protect themselves and their clients from an ongoing threat, as well as to be able to file a more accurate report. At the same time, we believe that this window should also allow the Commission to monitor market-wide impacts of a significant incident and timely share important information regarding such incidents with market participants.

iii. A final Form ADV-C updating the initial report should be submitted after the resolution of, or closing any internal investigation related to, the significant cybersecurity incident.

We understand that the Commission believes it would be helpful to receive "post-mortem" confidential information following resolution of the significant cybersecurity incident. Such information could potentially assist the Commission in identifying broader cybersecurity incident patterns and trends. Thus, under our recommendation, an adviser would be required to provide the Commission such data and also amend or update any information provided in the initial filing that has materially changed.

In particular, under our recommendations, the final filing would require the adviser to provide the Commission with substantive information about the nature and scope of the incident that was reported in the initial filing, including actions the adviser took to recover from the incident, and the extent to which any data was stolen, altered, accessed, or used for any other unauthorized purpose.

iv. Advisers should not be required to amend Form ADV-C prior to the final filing.

We strongly oppose requiring advisers to continuously file amendments to the initial Form ADV-C as they discover new material facts regarding an incident.[69] Indeed, the continuous reporting requirement may be the single most onerous and unnecessary aspect of the Proposal. Given the fact that most – and certainly any significant – cybersecurity incidents are fast moving – information is rarely known all at once and is typically changing rapidly – it is very likely that numerous Form ADV-C amendments would be necessary. For example, a ransomware incident where the attacker claims to have client data may result in numerous communications between the adviser and the attacker to confirm the extent to which client data has been breached, including the number of clients affected. Each exchange with the attacker may reveal new information regarding the attack requiring the adviser to constantly focus on whether this information is material rather than on the developing situation itself. The proposed 48-hour reporting window and "reasonable basis to conclude" standard would magnify these concerns because it is virtually certain that amendments would be needed almost as soon as the initial

---

cybersecurity incident). We find it incongruous that the Commission proposes a longer reporting timeframe for public companies than for investment advisers, most of which are small businesses.

[69] The Proposal would require advisers to amend a previously filed Form ADV-C promptly, but in no event more than 48 hours, in connection with certain incidents, including if any previously reported information about a significant adviser cybersecurity incident becomes materially inaccurate or if the adviser discovers new material information related to an incident.

Form ADV-C and any amendments to that filing are filed. This element of the Proposal would be extraordinarily burdensome, highly impractical, and, in our view not at all useful for the Commission.

Reporting obligations must be taken seriously, requiring advisers to dedicate substantial time and attention to completing any written report to the Commission to ensure that it is complete and accurate. This is time and attention an adviser does not have while it is also triaging a significant cybersecurity incident, particularly if an attack is ongoing.[70] Multiple steps and layers of review would likely be necessary to prepare a Form ADV-C amendment to ensure that advisers do not misspeak or omit material information.[71] Depending on an adviser's protocols, they would need to consult with potentially a large number of internal and external stakeholders (*e.g.*, risk management, legal, including possibly outside counsel, COOs, operations, fund administration, etc.) to gather and analyze information, make a materiality determination, draft responses, and go through the internal and often external review process, among other steps. Moreover, the open-ended responses to questions on proposed Form ADV-C would take additional time to draft, analyze, and obtain accurate and complete input from stakeholders.[72]

Accordingly, the IAA urges the Commission not to require advisers to file amendments to Form ADV-C prior to the final filing. We believe that the initial and final filings that we recommend will be sufficient to achieve the Commission's stated goals of monitoring for and detecting potential cyber attacks that present a wider threat to other firms and the markets more generally, while not imposing unnecessary operational and compliance burdens on advisers in the middle of a cybersecurity incident.[73] Should the Commission nonetheless decide to require

---

[70] Typically, when an adviser has a material amendment to Form ADV that requires an other-than-annual update, the amendment is filed within 30 days. Experience has shown that significant time and resources are needed to prepare and file amendments to Form ADV in general, and we expect fast-changing cybersecurity amendments to be even more challenging.

[71] We note that an adviser is subject to regulatory risks (*e.g.*, potential for enforcement action) for inaccurate or incomplete information in SEC filings: "It shall be unlawful for any person willfully to make any untrue statement of a material fact in any registration application or report filed with the Commission under section 203 or 204, or willfully to omit to state in any such application or report any material fact which is required to be stated therein." Advisers Act Section 207.

[72] The list of stakeholders would depend on the adviser and the nature and scope of the incident. Different advisers may also have different processes for involving legal and other personnel to review regulatory filings and it is very likely that the personnel preparing the reports are not the same as those providing the information. Depending on the scope of the cybersecurity incident and nature of the adviser, organizations could potentially be subject to many different notice requirements managed by different people. For example, large organizations may have many registered investment advisers, both U.S. and global, with different legal personnel managing each entity's filings. It would involve enormous effort to prepare and maintain consistency in the amended reports, opening advisers up to increased regulatory risk.

[73] We agree with the Commission that "it is likely that an adviser could regularly engage in a productive dialogue with applicable Commission staff after the reporting of an incident…and, as part of that dialogue, could provide Commission staff with any additional information as necessary, depending on the facts and circumstances of the incident and the progress in resolving it." Proposal at 13537. Engaging in productive dialogue with Commission staff is very different from making regulatory filings subject to antifraud standards.

amendments before the final filing – which we believe would be a mistake – we urge the Commission to provide a safe harbor or assurances, discussed below.

v. Advisers acting in good faith should not be subject to regulatory enforcement in connection with information on Form ADV-C that turns out to be materially inaccurate.

Given that facts and what an adviser knows at any given time will likely evolve quickly due to the very nature and scope of a significant adviser cybersecurity incident, we appreciate the statement in the Proposal that "Advisers should only share information about what is known at the time of filing."[74] We request that the adopting release include a statement to the same effect and make clear that advisers will not be subject to regulatory scrutiny for misstatements or omissions in connection with the filing if they did not know of the inaccuracy at the time of the filing, absent other compelling facts, *e.g.*, evidence that the adviser was not proceeding in good faith. This will be especially important if the Commission retains the proposed requirement to file a Form ADV-C report that includes all of the proposed items.

vi. Clarify sub-adviser reporting.

We ask for clarification with respect to situations in which a sub-adviser to a mutual fund experiences a reportable incident. It is unclear under the Proposal whether the sub-adviser, and/or the adviser and the fund, would be required to report. To avoid duplicative burdens, we believe that only one report per incident should be required and recommend that the adviser and sub-adviser be permitted to agree on who should report based on the particular facts and circumstances.[75]

vii. Avoid duplicative reporting on Form ADV-C and Form PF.

We note that the Commission has proposed to require current reporting of a cybersecurity event that disrupted the trading volume of a reporting fund by 20 percent of its normal capacity in its proposal to update Form PF for large hedge fund advisers.[76] In our comments to the Commission on that proposal, we strongly urged the Commission to remove any reference or obligation to report any cybersecurity event in Form PF, given that the Commission has proposed cybersecurity reporting requirements here. Should the Commission nevertheless include a cybersecurity reporting requirement in any final Form PF requirements, to alleviate burdens and avoid a duplicative and inconsistent obligation to report the same cybersecurity event on multiple forms to the Commission, we again request that the Commission provide an

---

[74] Proposal at 13539.

[75] We also note confidentiality concerns that would arise if an unaffiliated sub-adviser were required to report internal data to a fund or fund adviser so that the fund adviser could then report such information to the SEC on Form ADV-C.

[76] *Amendments to Form PF To Require Current Reporting and Amend Reporting Requirements for Large Private Equity Advisers and Large Liquidity Fund Advisers*, 87 Fed. Reg. 9106, 9114 (Feb. 17, 2022), available at https://www.govinfo.gov/content/pkg/FR-2022-02-17/pdf/2022-01976.pdf (**Form PF Proposal**).

exception to the Form PF current reporting requirements when the adviser has filed a Form ADV-C in connection with the incident.

IV. Public Disclosure of Cybersecurity Risks and Incidents

Currently, advisers are required to deliver interim brochure amendments to existing clients if the amendment includes certain disciplinary information.[77] In addition, as a fiduciary, an adviser has "an ongoing obligation to inform [its] clients of any material information that could affect the advisory relationship."[78] As a result, the adviser must disclose to clients material changes that occur between interim brochure amendments even if those changes do not trigger delivery of an interim amendment.

The Commission is proposing amendments to Rule 204-3(b) under the Advisers Act and Form ADV Part 2A to require that clients and prospective clients be provided with information regarding cybersecurity risks and incidents that could materially affect the advisory relationship.[79] Specifically, the Proposal would add Item 20 to Form ADV Part 2A to add disclosure of a cybersecurity incident and amend Rule 204-3(b) to require advisers to deliver interim brochure amendments to existing clients promptly "if the adviser adds disclosure of a cybersecurity incident to its brochure or materially revises information already disclosed in its brochure about such an incident." We support disclosure of material information and believe that advisers would already be required to make disclosures to clients regarding material incident-related information, as we discuss below.

The Commission elaborates that the proposed disclosures would "give the Commission and staff greater insight into cybersecurity risks affecting advisers and funds." According to the Proposal, this information would "enhance the Commission's ability to oversee compliance with the proposed cybersecurity risk management rules, and to gain understanding about the specifics of the policies and procedures that funds adopted under the rules."[80]

We believe that client disclosure and regulatory reporting of cybersecurity incidents should serve distinct purposes – (i) public disclosure to clients and potential clients of the risks of cyber attacks to help them evaluate an advisory relationship, versus (ii) providing critical and timely information to regulators regarding emerging threats, as discussed above, (a) for the collective benefit of monitoring market-wide impacts and improving cybersecurity overall, and

---

[77] *See* Form ADV Part 2A, Item 9.

[78] Instructions for Part 2A of Form ADV: Preparing Your Firm Brochure includes Note to Question 2: "As a fiduciary, you have an ongoing obligation to inform your clients of any material information that could affect the advisory relationship. As a result, between annual updating amendments you must disclose material changes to such information to clients even if those changes do not trigger delivery of an interim amendment. *See* General Instructions for Part 2 of Form ADV, Instruction 3."

[79] *See*, *e.g.*, Proposal at 13540.

[80] Proposal at 13539-13540.

(b) to help regulators make risk-based decisions on which regulated entities to examine, but not in real time.

In our view, the potential negative consequences of highly-detailed public disclosure, as proposed, must be weighed against the Commission's monitoring and examination rationale. While we strongly support providing material cybersecurity-related disclosures to clients and investors to help inform their decision making regarding a particular investment adviser, we are concerned by the amount of information the Commission proposes requiring be publicly disclosed given that the Commission would already have alternative means to obtain this information for its compliance and risk assessment purposes. For example, advisers will be required to report extensive information about a significant cybersecurity incident through Form ADV-C and keep related records, which also would provide the Commission useful and timely data to satisfy its oversight function. In addition, advisers will be required to have a specified cybersecurity risk management program, about which they will keep records and for which they will be examined. If an adviser lacks appropriate cybersecurity controls, it will be susceptible to an examination finding by the SEC staff. We thus do not see the need to increase "accountability" of advisers on cybersecurity issues through public disclosure of cybersecurity risks and are concerned about the many negative consequences that could result from over disclosure. Accordingly, our comments below are intended to ensure that any required cybersecurity-related disclosures provide information that an investor would consider material with respect to the advisory relationship.[81] Public disclosure of more than that is neither warranted nor prudent.

As proposed, Item 20 of Form ADV Part 2A would require an adviser to provide narrative disclosures in its Form ADV brochure of:

(i) Any ***cybersecurity risks***[82] that could ***materially*** affect the advisory services the adviser offers. Advisers would also be required to describe how they ***assess***, ***prioritize***, and ***address*** cybersecurity (**Risk Disclosure**); and

(ii) **Any** ***cybersecurity incident*** that has occurred within the ***last two fiscal years*** that has significantly disrupted or degraded the adviser's ability to maintain critical operations, or has led to the unauthorized access or use of adviser information,

[81] We support using a "materiality" standard with respect to disclosure requirements generally because we agree that disclosures provided by advisers to clients should be focused on information a reasonable client is substantially likely to consider to be important in making a decision regarding an advisory relationship. We also note that this standard generally aligns with other disclosure requirements that advisers are already subject to and familiar with. For example, under federal and state law, an adviser is a fiduciary and must make full and fair disclosure to its clients of all *material* facts relating to the advisory relationship. *See also* General Instruction No. 4 to Part 2 of Form ADV (All information in your brochure and brochure supplements must be true and may not omit any *material* facts), Advisers Act Section 204A (advisers must have written policies and procedures reasonably designed to prevent the misuse of *material* nonpublic information), and Investment Company Act Rule 38a-1(e)(2) (requiring reporting of *material* compliance matters to fund boards).

[82] As proposed, "cybersecurity risk" is broadly defined to mean the "financial, operational, legal, reputational, and other adverse consequences that could stem from cybersecurity incidents, threats, and vulnerabilities."

resulting in substantial harm to the adviser or its clients (**Incident Disclosure**).[83]

We address each of these disclosure items below.

A. Risk Disclosure should be a concise high-level description of an adviser's material cybersecurity risks.

According to the Commission, a "cybersecurity risk, regardless of whether it has led to a significant cybersecurity incident, would be material to an adviser's advisory relationship with its clients if there is a substantial likelihood that a reasonable client would consider the information important based on the total mix of facts and information."[84] The Commission states that in this context, the facts and circumstances relevant to determining materiality may include, among other things, the likelihood and extent to which the cybersecurity risk or resulting incident: (i) could disrupt (or has disrupted) the adviser's ability to provide services, including the duration of such a disruption; (ii) could result (or has resulted) in the loss of adviser or client data, including the nature and importance of the data and the circumstances and duration in which it was compromised; and/or (iii) could harm (or has harmed) clients (*e.g.*, inability to access investments, illiquidity, or exposure of confidential or sensitive personal or business information).[85]

We agree that cybersecurity risks involving these particular facts and circumstances would generally be material to investors, but we do not agree that the apparent level of detail proposed would be material and are concerned regarding this much public disclosure with respect to an adviser's cybersecurity risks.

We do not believe that highly detailed Risk Disclosure would be particularly decision useful for clients and investors and may, in fact, be counterproductive to achieving the Commission's stated goals. The Commission acknowledges that it is not aware of any studies that examine the role perceptions of cybersecurity play in how clients approach choosing an adviser.[86] We understand that in practice most clients and prospective clients do not ask for this much detail about an adviser's cybersecurity posture because they understand that such risks exist everywhere that technology is used and they appreciate that the adviser clearly understands the risks posed to its overall business. We believe that clients and investors primarily engage investment advisers for their expertise to provide ongoing advice and portfolio management over the long term, help individuals navigate the complex financial markets, and meet their financial

[83] Proposed Item 20 of Form ADV Part 2A.

[84] Proposal at 13540.

[85] *Ibid.*

[86] As noted in the Proposal, "The markets for advisory services and funds present clients and investors with a complex, multi-dimensional, choice problem. In choosing an adviser or fund, clients and investors may consider investment strategy, ratings or commentaries, return histories, fee structures, risk exposures, reputations, etc. While we are not aware of any studies that examine the role perceptions of cybersecurity play in this choice problem, the extant academic literature suggests that investors focus on salient, attention-grabbing information such as past performance and commissions when making such choices." Proposal at 13553.

goals, including investing for retirement, home ownership, and education. Clients likely want to know that an adviser has reasonably-designed controls in place to manage its business and its risks, including cybersecurity risks. But we do not believe that clients would typically want more than a brief, high-level description of these controls.

We are concerned that the amount of detail in and volume of the proposed disclosures would be too much "noise" for investors, and that providing so much information could be both overwhelming and desensitizing. We also believe that this level of detail being publicly disclosed would provide the cyber bad actor community with easily accessible ripe information to exploit an adviser's perceived vulnerabilities, which could result in more cyber attacks with potential to harm even more clients. Accordingly, we recommend that the required disclosure call for a concise high-level description of an adviser's material cybersecurity risks and how – again at a high level – an adviser assesses, prioritizes, and addresses these risks.[87]

B. Incident Disclosure should be limited to a high-level description of material breaches of an adviser during the past fiscal year.

The Commission is essentially proposing to require public disclosure of much of the same, ***if not more***, information that would also be confidentially reported to the Commission under the two-prong definition of significant adviser cybersecurity incident as described above. While we generally support layered reporting of this information *to the Commission,* as we recommend above, we have significant concerns regarding making this information *publicly* available, especially with the level of detail that is proposed to be disclosed. In particular, as proposed, the description of each incident would be required to "include the following information to the extent known: the entity or entities affected; when the incident was discovered and whether it is ongoing; whether any data was stolen, altered or accessed, or used for any other unauthorized purpose; the effect of the incident on the adviser's operations; and whether the adviser, or service provider, has remediated or is currently remediating the incident."[88]

We have serious concerns that the proposed highly-detailed and specific Incident Disclosure regarding cybersecurity incidents an adviser has suffered would be extremely useful to threat actors and not particularly useful to investors.[89] Moreover, this proposed disclosure could, in many cases, lead an investor to make unjustified and perhaps even misleading conclusions about an adviser's cybersecurity preparedness and thus not engage an adviser that otherwise is highly suitable for its investment goals. For example, a data breach may occur at an

[87] Rather than describing cybersecurity incidents in detail, we suggest treating cybersecurity disclosure similar to code of ethics disclosure. Item 11 of Form ADV Part 2A states: "If you are an SEC-registered adviser, briefly describe your code of ethics adopted pursuant to SEC rule 204A-1 or similar state rules. Explain that you will provide a copy of your code of ethics to any client or prospective client upon request." Likewise, it should be sufficient for an adviser to briefly describe its cybersecurity risks and undertake to provide more details upon request.

[88] Proposed Item 20 of Form ADV Part 2A.

[89] As discussed above, advisers are already obligated under state data breach notification laws to disclose information about a cybersecurity event involving personally identifiable information to affected clients. The proposed Form ADV brochure disclosure regarding incidents is thus not needed for these clients.

adviser that had implemented reasonably-designed policies and procedures to address the cybersecurity risks implicated in the breach, including appropriate oversight of third parties. And this breach could just as easily have occurred at other advisers with equally-robust controls. Similarly, we also do not see the benefit to investors of obtaining disclosure of incidents that occurred on third-party systems or platform tools (*e.g.*, a failure by Microsoft to provide a patch for its software). Incidents are not only possible, but may even be probable, even with the best controls. We believe that providing investors with all of the information proposed would make it increasingly difficult for them to make an appropriate assessment of an adviser's cybersecurity preparedness, contrary to the goal of helping them evaluate an advisory relationship. This is compounded by the likelihood that the adviser will have already fully remediated the vulnerability, making the information even less relevant.

We believe that a more targeted approach with respect to the level of required Incident Disclosure would more effectively achieve the Commission's goal of providing decision-useful information to clients while addressing our concerns above. More targeted disclosure would make it more likely that clients would read and understand the information being provided – *i.e.*, it would not overload clients with overly-detailed and hard-to-understand technical details – while reducing the chances of clients making inaccurate assessments and providing threat actors with a detailed roadmap for further attacks.

We also strongly oppose the proposed requirement that an adviser provide a detailed description of each significant cybersecurity incident that occurred within the prior ***two fiscal years***. We recommend that the Commission modify the proposed lookback period of two fiscal years to line up with the schedule for updating an adviser's Form ADV, which is annual. Requiring a two-year lookback would overburden advisers without adding meaningful benefits to investors. In addition, because the nature and sophistication of cybersecurity incidents and the tools available to counter such attacks are continuously evolving, any information provided beyond the past fiscal year would very likely be stale and irrelevant for purposes of a client's assessment of an adviser's current cybersecurity preparedness.

For these reasons, we recommend that any Incident Disclosure requirement be limited to a high-level description of significant cybersecurity incidents to which an adviser was subject during the past fiscal year that resulted in the unauthorized access or use of information, if any, and that the adviser determines would be material – *i.e.*, decision useful – to an investor's assessment of the advisory relationship.[90] Such disclosure could include a brief description of how the adviser addressed the cybersecurity incident and the impact, if any, on the adviser's provision of advisory services. We also ask the Commission to confirm that advisers may treat a group of related incidents as a single incident and that it provide flexibility for advisers to aggregate similar types of incidents for disclosure purposes as well as to exclude incidents that

[90] For example, larger firms with multiple business lines and Form ADV brochures might be compelled under the Incident Disclosure requirement as proposed to disclose an incident that is wholly unrelated to the services being provided to a particular client or type of client. For example, the fact that a separate business line with separate technology suffered a breach is very likely irrelevant to clients of an entirely different business line and different technology. We do not see the utility to investors of requiring such an expansive new disclosure requirement with respect to each incident that would justify the burden to the adviser in these and similar circumstances.

the adviser believes are not relevant in the context of a particular client or type of advisory relationship.

C. Advisers should be given flexibility with respect to the timing of disclosure.

With respect to the timing of any disclosure, the Commission should also permit advisers the flexibility to determine when to update and deliver their cybersecurity disclosures based on the facts and circumstances involving a cybersecurity incident, including the nature of the incident, and the usefulness of the disclosures to existing clients at any particular point in time.

We disagree with the Commission's implicit characterization that virutally all cybersecurity incidents are "exigent" by nature, warranting "swift delivery" of an interim brochure amendment under proposed Rule 204-3(b)(4) to clients. On the contrary, depending on the facts and circumstances, it may be premature for an adviser to make a public disclosure of a cybersecurity incident until initial facts have been confirmed or while an investigation is ongoing.[91] We believe that it is vital that advisers be given flexibility with respect to the timing of disclosure to ensure that any disclosures that are provided to investors are accurate and consistent with an adviser's fiduciary obligations.

Finally, we ask that the Commission confirm that an adviser may delay disclosure if it could increase the risk of further harm, hamper the chances of recovery of stolen funds or information, or impede the detection of wrongdoers in the expert opinion of law enforcement officials.

V. The Commission is severely underestimating the quantifiable costs of the Proposal, particularly relating to smaller advisers.

While we appreciate the Commission's views on the *qualitative* costs and benefits of the Proposal, we are concerned that the Commission has not yet considered – or put out for public comment – the very real *quantifiable* costs of not only developing the proposed cybersecurity policies and procedures to the extent they are not already in place or not in place in precisely the way proposed, but also of implementing the systems necessary to operationalize other aspects of the Proposal. At a minimum, we would have expected the Commission to be able to estimate these costs with specified assumptions for at least the purpose of seeking public comment.[92]

---

[91] Of course, the adviser should have already notified the affected clients directly as required by state law and will be working to resolve the issue accordingly irrespective of any required disclosures.

[92] Given the serious time constraints for providing comments to the Commission, we are unable to provide more specific feedback on the costs of the Proposal at this time. We would welcome the opportunity to work with Commission staff to try to obtain more information from our members. We would also urge the Commission to carefully consider cost estimates by other commenters and to proactively attempt to determine the likely costs involved by any means reasonably available (*e.g.*, the Commission could publish a request for additional information regarding costs and benefits).

A. The Proposal will have wide-ranging foreseeable costs for advisers of all sizes.

Advisers will likely need to increase their budgets for cybersecurity support staff and vendors with technical expertise in response to any new rules, even if they have existing cybersecurity policies and procedures, because the Commission's proposed requirements are much more granular and prescriptive. For example, foreseeable costs under the Proposal may include revising how an adviser responds to cybersecurity incidents, engaging legal counsel to assist in reporting on significant adviser cybersecurity incidents, adding information security staff, developing a third-party 24/7 security operations center (SOC) or retaining a SOC-as-a-service vendor to monitor an adviser's network and infrastructure, implementing antivirus defenses, deploying unified endpoint management (UEM), retaining auditors to provide audit assurance, adding user access restrictions on client relationship management (CRM) systems, portfolio management software, trading platforms, shared file storage, shared email addresses, and human resources information, monitoring and modifying user access as needed, securing the adviser's website, email, file storage systems, video, and VOIP communications, developing policies and procedures, including, but not limited to, a Digital Security Program (DSP), Cybersecurity Incident Response Plan (CIRP), Vendor Compliance Program (VCP), Vulnerability & Patch Management Program (VPMP), Continuity of Operations Program

---

Moreover, the Proposal is one of several concurrent rule proposals that, if adopted, will have an enormous effect on investment advisers, investors, the markets, and the U.S. financial system as a whole. Each of these proposals, standing alone, is complex and potentially consequential, with the accompanying releases asking a very large number of questions and seeking a very large amount of data. Given the significant amendments proposed, many of which are interrelated, we continue to be concerned that the very short comment period – for this and all the other proposals – is insufficient for us and other commenters to provide comprehensive and sufficiently thorough responses, including "data or information that would enable a quantification of the proposal's economic effects." Proposal at 13543. We are especially concerned that the Commission was unable to quantify the economic effects of the Proposal and that "much of the discussion of economic effects is qualitative in nature." *Id.*

As we recently expressed, we do not believe the SEC has provided sufficient time for considered public input on the Proposal; a comment period for *this* Proposal of *at least* 60 days from publication in the *Federal Register* would have been more appropriate. *See* IAA and Joint Trade Associations' Letter on Importance of Appropriate Length of Comment Periods (Apr. 5, 2022), available at https://investmentadviser.org/resources/iaa-and-trade-associations-urge-sec-to-lengthen-short-comment-periods/ and IAA and Joint Trade Associations' Letter Requesting Extension of Comment Period for Private Fund, Form PF Proposals (Mar. 1, 2022), available at https://investmentadviser.org/wp-content/uploads/2022/03/Extension-Request-File-Nos.-S7-03-22-S7-01-22.pdf. We strongly urge the Commission to formally extend the comment period in order to undertake a more quantifiable assessment of the costs the Proposal would impose on investment advisers.

Some of the other significant rule proposals concurrently or recently out for comment are: the Form PF Proposal, *Private Fund Advisers; Documentation of Registered Investment Adviser Compliance Reviews*, 87 Fed. Reg. 16886 (Mar. 24, 2022), available at https://www.govinfo.gov/content/pkg/FR-2022-03-24/pdf/2022-03212.pdf, *Shortening the Securities Transaction Settlement Cycle*, 87 Fed. Reg. 10436 (Feb. 24, 2022), available at https://www.govinfo.gov/content/pkg/FR-2022-02-24/pdf/2022-03143.pdf, *Modernization of Beneficial Ownership Reporting*, 87 Fed. Reg. 13846 (Mar. 10, 2022), available at https://www.govinfo.gov/content/pkg/FR-2022-03-10/pdf/2022-03222.pdf, *The Enhancement and Standardization of Climate-Related Disclosures for Investors*, 87 Fed. Reg. 21334 (Apr. 11, 2022), available at https://www.govinfo.gov/content/pkg/FR-2022-04-11/pdf/2022-06342.pdf, *Further Definition of "As a Part of a Regular Business" in the Definition of Dealer and Government Securities Dealer*, Release No. 34-94524 (Mar. 28, 2022), available at https://www.sec.gov/rules/proposed/2022/34-94524.pdf, and *Special Purpose Acquisition Companies, Shell Companies, and Projections*, Rel. Nos. 33-11048; 34-94546; IC-34549 (Mar. 30, 2022), available at https://www.sec.gov/rules/proposed/2022/33-11048.pdf.

(COOP), and Bring Your Own Device Policy (BYOD), training staff, conducting phishing and penetration testing, adding encryption to advisers' systems, and obtaining cybersecurity insurance.

It is important for the Commission to ensure that any additional reporting requirements relating to cybersecurity-related incidents are warranted for advisers of all sizes, considering current data breach and privacy reporting requirements. Also, the benefits to the SEC of being able to assess possible market-wide attacks need to be weighed against the potential costs of adding an additional layer of regulatory burden that may impede advisers' ability to respond to a cyber threat in real time. In addition, the Commission should carefully weigh any potential benefits of public disclosure against the costs. For example, as the Commission notes, "to the extent that clients and investors 'overreact' to disclosures of cybersecurity breaches, advisers and funds may pursue a strategy of 'overinvestment' in cybersecurity precautions (to avoid such overreactions) resulting in reduced efficiency." To the extent possible, existing rules such as the Compliance Program Rule, Regulation S-P, Regulation S-ID, and the FTC Safeguards Rule should be considered as regulatory alternatives to the proposed reporting and disclosure requirements that would not impose the increased costs of a brand new rule.[93]

It is also crucial that the public disclosure aspect of the Proposal be backed up with data. The current cost-benefit analysis in this respect appears to be theoretical. "In principle, the proposed disclosure requirements would help alleviate this information asymmetry, and in so doing enable clients and investors to better assess the effectiveness of advisers' and funds' cybersecurity preparations and the cybersecurity risks of different advisers and funds."[94] We do not believe that these assumptions provide enough of a basis to justify the burdens that the broad disclosure requirements, as proposed, would place on advisers.

B. The Proposal will be particularly burdensome for smaller advisers.

These costs are especially burdensome for smaller and mid-sized advisers that may not have in-house technical expertise or dedicated in-house IT personnel. As we have noted in the past, smaller advisory firms face unique challenges. The vast majority of investment advisers are small businesses by any logical measure and they should be treated accordingly.[95] Smaller advisers have been significantly burdened by one-size-fits-all regulations – both in isolation and cumulatively – that effectively require substantial fixed investments in infrastructure, personnel, technology more broadly, and systems relating to documentation, monitoring, operations, custody, business continuity planning, and more. According to the Commission's Asset Management Advisory Committee (**AMAC**), "There is a widening gap between regulatory expectations on deployment of cybersecurity measures relative to the resources available for small firms/funds." AMAC also found that "the impact [of cybersecurity costs] is outsized for

[93] *See* Proposal at 13526-13627, 13547, and 13581.

[94] Proposal at 13552.

[95] *See* Industry Snapshot.

small firms, as both a percentage of operating expenses and a percentage of revenues."[96] We are concerned that these stressors and barriers will impact smaller advisers' business models and lead to industry consolidation.

The IAA recommends that the Commission carefully consider the specific impact all elements of the Proposal (and, indeed, the many other regulatory proposals currently under consideration) would have on smaller advisory firms, and conduct a more realistic assessment of the additional cumulative impact the Proposal would have on smaller advisers. Unfortunately, under current federal regulations, the Commission is not required to conduct a realistic analysis of the impact the Proposal would have on smaller advisers, and we believe that the Proposal thus severely underestimates the costs and burdens that would be imposed on smaller firms.

As a practical matter, the Commission is not required to analyze the economic impact of its regulations on small advisers because, inexplicably, its definition of "small business" includes only advisory firms with less than $25 million in AUM, while with rare exceptions an advisory firm must have a minimum of $100 million AUM to fall under SEC jurisdiction. We have long urged the Commission to reexamine this definition, and, for example, consider other factors in addition to a more meaningful AUM (*e.g.*, number of employees), to make a more realistic assessment of the impact of rules on smaller advisers that by their nature have limited staffing. In our view, this definition makes the Commission's economic impact analysis of the Proposal on smaller advisers virtually meaningless. Moreover, because cybersecurity preparedness and resiliency depend largely on financial and human resources, using an AUM-based test as the only measure risks missing the true burdens on smaller advisers.

We recommend that the Commission utilize the ever-increasing amount of data at its disposal to make a more realistic assessment of the impact the Proposal would have on smaller advisers, including various alternatives suggested by commenters.[97] We also urge the Commission to consider the other contexts in which the agency has tailored regulations more appropriately for smaller advisers.

C. The Commission should provide an exemption to reduce overlapping regulatory requirements.

The Commission should exempt from the proposed cybersecurity risk management rules advisers that are already required to implement specific cybersecurity-related policies and procedures (directly or indirectly through, for example, a parent company) and notify regulators of cybersecurity incidents under other regulatory regimes (*e.g.*, advisers that are affiliated with

---

[96] *See Final Report and Recommendations for Small Advisers and Funds*, AMAC (Nov. 3, 2021), available at https://www.sec.gov/files/final-recommendations-amac-sec-small-advisers-and-funds-110321.pdf.

[97] We are concerned with the statement in the Proposal that "As we do not currently have reliable data on the extent to which registrants' existing policies and procedures follow industry best practices, address cybersecurity risks, their 'reasonableness,' or the frequency at which they are reviewed, it is not possible for us to quantify the scale of the benefits arising from the proposed requirements." Proposal at 13551. We would expect the Commission to have access to this information via its examination program, especially in light of its many cybersecurity sweeps, and we believe that the Commission should look to this data to offer quantifiable costs and benefits as part of the Proposal.

banks and are already subject to notification requirements under banking regulations and can have multiple registered advisers). Otherwise, large, complex organizations – or even smaller affiliated entities subject to the jurisdiction of other regulators – may have to make multiple Form ADV-C or other regulatory filings to report the same incident. Providing this requested exemption would help reduce overlapping regulatory requirements with respect to cybersecurity.

D. An adviser's cybersecurity spending should be evaluated based on a reasonableness standard and not a targeted amount.

The Commission states that the financial services sector is one of the biggest spenders on cybersecurity measures, referencing a survey finding that non-bank financial firms spend an average of approximately 0.5 percent of revenues on cybersecurity.[98] We do not believe it makes sense to target a particular number for firms to spend. Regardless, the amount that an adviser spends on cybersecurity should be evaluated based on a reasonableness standard (*i.e.*, based on the particular circumstances and risks of a specific adviser) rather than some apparent expectation of how much advisers should spend to achieve the most "optimal" cybersecurity program.

VI. The Commission should provide a compliance period of at least 18 months.

Given the scope of work that will be necessary for advisers to implement the Proposal, as described throughout this letter, we recommend that the Commission provide a compliance period of at least 18 months following the effective date of the rules.[99] Although the proposed cybersecurity policies and procedures generally reflect what firms are already required to have in place under the Compliance Program Rule, it would still take significant time for many advisers to align current practices with prescriptive regulatory requirements under the Advisers Act. The details will differ, especially as between larger and smaller firms and different types of firms, but preparing to comply with the new rules would entail considerable resources for advisers of all sizes to holistically reassess their cybersecurity risk, prepare for brand new reporting, draft, update, and implement policies and procedures to reflect new SEC requirements, and update Form ADV Part 2.

These challenges will be severely exacerbated by the many other anticipated Commission rulemakings that will involve increased compliance by advisers.[100] In addition, advisers are already busy implementing sweeping new SEC rules (*e.g.*, Investment Adviser Marketing Rule

---

[98] *See* Proposal at 13545.

[99] This would be consistent with other recent major rulemakings. *See, e.g.*, Marketing Rule Release (providing an 18-month transition period between the effective date of the rule and the compliance date). We expect implementation of the cybersecurity rules to take more time than implementation of the Marketing Rule.

Alternatively, the Commission could consider a tiered implementation approach, in which certain elements (*e.g.*, risk assessments) are given a shorter compliance date while others (*e.g.*, preparation for continuity of operations) are given a longer compliance date. The Commission could also tier implementation based on an adviser's size or nature of business (*see, e.g.*, investment company Liquidity Rule).

[100] *See supra* n.92.

206(4)-1 and proxy voting rules and guidance). It is imperative for the Commission to consider the cumulative effect of all of these regulations on advisers' operational limitations in determining the compliance date of cybersecurity rules for investment advisers.

* * * *

We appreciate the Commission's consideration of our comments on the cybersecurity risk management proposal for investment advisers and would be happy to provide any additional information that may be helpful. Please contact the undersigned or Associate General Counsel Laura Grossman at [redacted] if we can be of further assistance.

Respectfully,

/s/ Gail C. Bernstein

Gail C. Bernstein
General Counsel

cc: The Honorable Gary Gensler, Chair
The Honorable Hester M. Peirce, Commissioner
The Honorable Allison Herren Lee, Commissioner
The Honorable Caroline A. Crenshaw, Commissioner
William A. Birdthistle, Director, Division of Investment Management