Schulte Roth&Zabel LLP

919 Third Avenue
New York, NY 10022
212.756.2000
212.593.5955 fax

www.srz.com

April 12, 2022

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

Re: Rules and Amendments to Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies (File No. S7-04-22)

Dear Ms. Countryman:

We are responding to the request of the Securities and Exchange Commission (the "Commission") for comments to the proposed rules related to cybersecurity risk management for registered investment advisers ("RIAs") as well as amendments to certain rules to require more disclosure regarding cyber risks and incidents (the "Proposed Cyber Rules").[1] We recognize the time and effort invested by the Commission and the Staff of the Division of Investment Management (the "Staff") in formulating the Proposed Cyber Rules and appreciate the opportunity to comment.

Schulte Roth & Zabel LLP is an international law firm with offices in New York, London and Washington, D.C. Our clients include many advisers to private funds that may be affected by the Proposed Cyber Rules as well as institutional investors and limited partners. We regularly advise private fund manager clients with respect to regulatory risks and responses, including with respect to cybersecurity. These comments, while informed by our experience in representing these clients, represent our own views and are not intended to reflect the views of the clients of the firm.

I. Introduction

On February 9, 2022, the Commission issued the Proposed Cyber Rules to, among other things, improve the cybersecurity preparedness of RIAs and to require more disclosure regarding cyber risks and incidents. The Proposed Cyber Rules seek to: (1) require RIAs to adopt and implement written policies and procedures that are reasonably designed to address cybersecurity risks; (2)

[1] *Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies*, Release No. 33-11028 (Feb. 9, 2022) (the "Proposing Release").

require RIAs to report significant cybersecurity incidents to the Commission on Form ADV-C; (3) enhance RIA disclosures related to cybersecurity risks and incidents; and (4) require RIAs to maintain certain cybersecurity-related books and records.[2]

We appreciate the Commission's desire to "enhance cybersecurity preparedness and [. . .] improve investor confidence in the resiliency of advisers and funds against cybersecurity threats and attacks"[3] However, the implications of the Proposed Cyber Rules are significant, potentially representing a shift away from existing cybersecurity standards and frameworks,[4] and we have the following comments and suggestions. In particular, we are concerned that the Proposed Cyber Rules could create new standards that compete with well-established cybersecurity industry standards and impose a uniform set of rules on RIAs regardless of the differing natures of their businesses. Moreover, we are concerned that the Proposed Cyber Rules are too prescriptive and overly broad in certain regards. As such, rather than establish minimum standards for cybersecurity resiliency, they may actually cause RIAs that currently have robust cybersecurity programs to divert resources away from established and effective programs to meet the SEC's requirements. We respectfully suggest that the Proposed Cyber Rules be revised as described herein, with an eye towards flexibility and less prescriptive elements, to better align with cybersecurity industry standards and to stand the test of time in the ever-evolving world of cybersecurity preparedness.

Therefore, we respectfully request that the Commission:

(i) Consider revising the definitions of "adviser information," "adviser information systems" and "cybersecurity incident" to better align with cybersecurity industry standards and allow RIAs to adopt a risk-based approach to prioritize their cybersecurity efforts;

(ii) Consider revisions to the Proposed Cyber Rules to permit RIAs to tailor their policies and procedures to their size and their risks to afford flexibility in the rule, rather than have it become outdated and potentially conflict with industry-accepted, established cybersecurity standards such as the National Institute of Standards and Technology ("NIST") framework;

(iii) Consider narrowing the scope of the types of service providers that RIAs would be required to assess for cybersecurity purposes, taking the risks associated with the types of service providers into account;

(iv) Consider including a review of cybersecurity policies as part of a Rule 206(4)-7 compliance review rather than requiring a separate written report;

---

[2] *Id.* at 1.

[3] Press Release, SEC, *SEC Proposes Cybersecurity Risk Management Rules and Amendments for Registered Investment Advisers and Funds* (Feb. 9, 2022), *available at* https://www.sec.gov/news/press-release/2022-20.

[4] Examples of widely used cybersecurity standards include the ISO/IEC 27000:2018 Family of Standards ("ISO 27000"); the National Institute of Standards and Technology Special Publication 800-53 Rev. 5 ("NIST 80-53") and COBIT 2019 from ISACA.

(v) Consider changing the time to file a Form ADV-C report after having a reasonable basis to conclude that a "significant cybersecurity incident" has occurred or is occurring from 48 hours to a "prompt" filing or, in the alternative, at least 72 hours;

(vi) Consider changing the threshold for filing an amended Form ADV-C from any "new material information" to "new information that causes a material change in how the significant cybersecurity incident is understood to impose risks to the RIA or its investors"; and

(vii) Consider harmonizing reporting of significant cyber events under the proposed amendments to Form PF[5] and the new proposed Form ADV to avoid duplicative reporting.

II. Certain Proposed Definitions

The Proposed Cyber Rules' definitions of "adviser information," "adviser information systems" and "cybersecurity incident," as drafted, are so broad that they render much of the Proposed Cyber Rules difficult to implement and put the Proposed Cyber Rules at odds with industry accepted cybersecurity standards. As a result, compliance with these requirements as proposed could create standards that compete with the NIST framework and other leading industry frameworks and standards and undermine the flexible, risk-based approach that we believe is critical to an effective cybersecurity program.

The Proposing Release acknowledges the leading role that NIST plays in establishing industry standards for cybersecurity resiliency.[6] NIST offers thorough and up-to-date guidance on cybersecurity best practices, including frameworks for assessing and reviewing cybersecurity policies and procedures.[7] Cybersecurity professionals rely on this and other guidance from various cybersecurity associations and organizations in creating and operationalizing cybersecurity procedures. These types of organizations build into their frameworks the ability to adapt and amend as cyber risks evolve and change. We believe that a view towards flexibility is key as it relates to cybersecurity and suggest the Commission work to incorporate this concept as it revises the Proposed Cyber Rules.

NIST has long maintained that effective cybersecurity approaches begin by assessing the risks facing the firm, and the Proposing Release similarly endorses a risk-based approach. However, the proposed definitions of "adviser information" and "adviser information systems" would effectively capture all electronic business communications and all adviser systems, which may undermine the prioritization of safeguarding the systems critical to RIA operations and the information that is most sensitive to RIAs. Cybersecurity professionals often emphasize that a

---

[5] *Amendments to Form PF to Require Current Reporting and Amend Reporting Requirements for Large Private Equity Advisers and Large Liquidity Fund Advisers*, Release No. IA-5950; File No. S7-01-22 (the "Form PF Amendments") at 34.

[6] *See* Proposing Release at 15 n.24, 16 n.25, 72.

[7] *See* Cybersecurity Framework: General Resources, National Institute of Standards and Technology – U.S. Department of Commerce (last updated Dec. 8, 2021), *available at* https://www.nist.gov/cyberframework/general-resources.

broad-brush approach that attempts to protect everything is much more likely to fail to protect the most valuable assets.[8]

Accordingly, we believe that our suggested revisions to the proposed definitions would better align the Proposed Cyber Rules with the definitions adopted by the "established sources" the Commission draws from and enable RIAs to focus on the specific cybersecurity risks they face.[9]

Adviser Information. In the Proposed Cyber Rules, "adviser information" is defined as "any electronic information related to the adviser's business, including personal information, received, maintained, created, or processed by the adviser"[10] and includes electronic business communications whether in the RIA's possession or subsequently stored or transmitted elsewhere.[11] Throughout the Proposed Cyber Rules, all "adviser information" is treated the same, with no consideration of the potential adverse impact of the unauthorized disclosure of such information. As such, the Proposed Cyber Rules could have the unintended consequence of causing RIAs to abandon a risk-based cybersecurity approach to assessing what information warrants protection in seeking to comply with the Proposed Cyber Rules. We suggest that the Commission revise the Proposed Cyber Rules to keep RIAs focused on the risks their cybersecurity assessments identify by rooting the Proposed Cyber Rules in the information that, if compromised, "would be substantially likely to cause material harm to the RIA, its clients or its investors." This approach builds in the concept of data classification, which is a bedrock principle of most cybersecurity programs, and aligns the definition with the reporting obligations in the new Form ADV-C.

Adviser Information Systems. In the Proposed Cyber Rules, "adviser information systems" is defined as "information resources owned or used by the adviser, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of adviser information to maintain or support the adviser's operations" (emphasis added).[12] This definition may cause unintended harm to RIAs' clients and investors by reaching every RIA system, regardless of whether it is internal to the RIA or an external service, and regardless of the role it serves in the RIA's operations. We believe it is important that "adviser information systems" be a concept reserved for the systems that, if compromised, "would be substantially likely to cause material harm to the RIA, its clients or its investors." Revising the definition of "adviser information" as suggested above would address this. This revised definition is most congruent with a risk-based approach and will enable RIAs to provide heightened protections specific to these critical resources.

---

[8] *E.g.*, Asim Rahal, *Developing a risk-based cybersecurity approach*, SECURITY MAGAZINE (Feb. 5, 2021), *available at* https://www.securitymagazine.com/articles/94528-developing-a-risk-based-cybersecurity-approach; Jim Boehm et al., *Enhanced cyberrisk reporting: Opening doors to risk-based cybersecurity* (McKinsey & Co., Jan. 29, 2020), *available at* https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/enhanced-cyberrisk-reporting-opening-doors-to-risk-based-cybersecurity.

[9] Proposing Release at 16 n.25.

[10] *Id.* at 216.

[11] *Id.* at 215.

[12] Proposing Release at 19 n.30.

Cybersecurity Incident. We also suggest that the Commission narrow the definition of "cybersecurity incident," which the Proposed Cyber Rules currently define 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."[13] This definition departs from the common understanding of this term as an event that materially interferes with information systems or adversely affect a business' ability to proceed with normal business. The examples set forth in the Proposing Release illustrate this common understanding.[14] Further, this would align the definition with the concept of "significant cybersecurity incidents" in the reporting requirements in the Proposed Cyber Rules. Otherwise, requiring disclosure of every "unauthorized occurrence" that could be viewed as "jeopardizing" the information systems will result in significant time and attention focused on reporting matters that raise little in the way of risk. Accordingly, we suggest that the Commission revise the Proposed Cyber Rules to clarify that cybersecurity incidents require reporting in the Form ADV Part 2A only when they "have a material impact on the operation of the RIA or its advised funds or pose a significant risk of substantial harm to investors." This revised definition will prove more informative for clients and investors in evaluating RIAs' cybersecurity. Further, this would align the definition with the concept of "significant cybersecurity incidents" that the Form ADV-C reporting requirements in the Proposed Cyber Rules already employ.

III. Cybersecurity Policies and Procedures

The Proposed Cyber Rules would require RIAs to adopt and implement written policies and procedures that are reasonably designed to address relevant cybersecurity risks.[15] Under the Proposed Cyber Rules, RIAs would have the flexibility to tailor their policies and procedures to the individual cybersecurity risks for the business, but at a minimum would need to incorporate the following five elements: (i) risk assessment, (ii) user security and unauthorized access, (iii) information protection, (iv) threat and vulnerability management and (v) incident response and recovery. Although the Commission acknowledges the importance of "the ability [of RIAs] to tailor their cybersecurity policies and procedures based on their individual facts and circumstances,"[16] the prescriptive nature of the required elements risks a rule that ultimately lacks the very flexibility the Commission seeks, resulting in the potential inability to stay relevant in the dynamic cybersecurity space.

Given the dynamic nature of cyber threats and responses, we believe a less prescriptive rule, using the NIST 800-53 cybersecurity framework as a guide, is better suited to achieve the Commission's goal of enhancing cybersecurity preparedness and protecting against cybersecurity incidents for years to come. The NIST 800-53 cybersecurity framework offers a set of guidelines and best practices to help organizations identify, prevent, detect and respond to cybersecurity incidents. While the NIST framework focuses on outcomes, it does not prescribe how an organization must achieve those outcomes. As a result of this allowance for firm-specific flexibility, a small

[13] *Id.* at 219.
[14] *Id.* at 21 ("such unauthorized access or use or failure could disrupt portfolio management, trade execution, or other aspects of its operations"); *id.* at 30 ("significant business disruptions, including losing the ability to communicate or the ability to access accounts or investments. These incidents also can lead to the unauthorized access or use of adviser or fund information".).
[15] *See* Proposing Release.
[16] Proposing Release at 15.

organization with a low cybersecurity budget and a large corporation with a big budget are each able to approach the outcome in a way that is feasible for them, particularly in light of then-current technology and best practices.

The Commission has already adopted this approach in Section 204A of the Advisers Act, which requires RIAs to have policies and procedures in place to prevent the misuse of material nonpublic information ("MNPI") but does not prescribe how such policies and procedures should be written. This approach has allowed the requirement to stay relevant and flexible to, among other things, keep pace with the increasingly complex nature of research and other relationships that can introduce MNPI without a need to constantly revisit the rule. Cybersecurity, like the world of insider trading, is constantly shifting and warrants a flexible approach to rulemaking.

Accordingly, while we support the adoption of written policies and procedures that are reasonably designed to address relevant cybersecurity risks, we suggest that the rule requiring such policies not enumerate specific elements that must be included in the policies. The expectations as to what should be specified in these policies and procedures will vary among different RIAs and can be expected to develop over time, which supports a more flexible approach.

IV. Cybersecurity Risk Assessment and Service Provider Diligence

The Proposed Cyber Rules would require RIAs to conduct and document periodic assessments to (i) identify, categorize and prioritize "cybersecurity risks"[17] based on an inventory of the components of their adviser information systems and adviser information and the potential effect of a cybersecurity incident, and (ii) identify and assess cybersecurity risks associated with using service providers that either receive, maintain or process adviser information or have access to adviser information systems.

We agree that periodic risk assessments are often an important part of a cybersecurity program, but we are concerned that the prescriptiveness of this requirement in the Proposed Cyber Rules may result in conflict with already-established cybersecurity guidelines. A significant number of cybersecurity assessments are already performed in accordance with industry-accepted, established cybersecurity standards, such as the ISO 27000 series, NIST Framework and SANS Institute Top 25 standards. Rather than introducing a new and potentially competing standard for a risk assessment in the Proposed Cybersecurity Rules, we believe a rule with flexibility will allow the most appropriate standards for such an assessment based on the circumstances applicable to the RIA.

In addition, we believe a more flexible approach to service provider diligence would strike the right balance. We believe that service provider diligence for those service providers that hold sensitive adviser information, have access to sensitive adviser systems or are critical service providers such that their cyber vulnerabilities could materially impact the operations of the RIA (the "Relevant Service Providers") would already be covered in the requirement that RIAs have policies and procedures reasonably designed to address cybersecurity risks, similar to the way that diligence of research providers that have the potential to introduce MNPI risks is encompassed as

[17] The Proposed Cyber Rules (*i.e.,* 206(4)-9(b) and Rule 38a-2(f)) define "cybersecurity risk" as "financial, operational, legal, reputational and other adverse consequences that could result from cybersecurity incidents, threats and vulnerabilities" respectively.

part of the obligations of Section 204A. If the Commission nonetheless determines to explicitly address service provider diligence as part of the final cyber rules, we suggest that the Commission limit such diligence to Relevant Service Providers, which is consistent with a flexible, risk-based approach.

V. Annual Cybersecurity Review

The Proposed Cyber Rules would require RIAs to review their cybersecurity policies and procedures no less than annually.[18] The review would focus on the design and effectiveness of the cybersecurity policies and procedures and include an analysis of whether those policies and procedures reflect changes in cybersecurity risk over the time period covered by the review. It would also require the preparation of a written report that (i) describes the review, assessment and control tests performed, (ii) explains results of a control test, (iii) documents any cybersecurity incident that occurred since the date of the last report and (iv) discusses any material changes to cybersecurity policies and procedures since the date of the last report. [19]

We recommend that a less prescriptive version of this requirement be included in the Proposed Private Fund Rules requiring that a RIA's annual compliance review under Rule 206(4)-7 be documented in writing[20] (in lieu of including the requirement in the Proposed Cyber Rules) so that there is a single annual compliance review requirement. We suggest that the Commission keep the requirements of any such rule flexible, using NIST's approach as a guide, so that RIAs can continue to be guided by cyber industry standards in conducting their annual reviews and testing.

VI. Reporting of Significant Cybersecurity Incidents under Proposed Form ADV-C

The Proposed Cyber Rules would require RIAs to report a "significant cybersecurity incident"[21] within 48 hours after having a reasonable basis to conclude that such an incident has occurred or is occurring.[22] RIAs would be required to file qualifying incident reports on a proposed new confidential Form ADV-C and submit an amended Form ADV-C in the event the RIA discovers "new material information about a previously reported incident" discovers that information previously reported on Form ADV-C has become "materially inaccurate" or resolves or closes an investigation of a previously reported incident.[23]

We appreciate the Commission's desire to have confidential regulatory reporting of certain significant cybersecurity incidents. The Proposed Cyber Rules in this regard, however (i) do not

---

[18] Proposed Cyber Rules 204(4)-9(b) and 38a-2(b).
[19] *See* Proposing Release at 35.
[20] Proposed Private Fund Rules at 321.
[21] As proposed, Rule 204-6 defines a "significant cybersecurity incident" as

> a cybersecurity incident, or a group of related 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: (1) substantial harm to the adviser, or (2) substantial harm to a client, or an investor in a private fund, whose information was accessed.

Proposing Release at 212-13.
[22] *See id.* at 212.
[23] *See id.* at 42.

allow for an adaptable timeframe for reporting that can meet the circumstances of the incident; (ii) may detract from an RIA's ability to immediately address qualifying incidents because the very personnel who are equipped to address such incidents are required to prepare and file Form ADV-C reports first; (iii) creates some ambiguity as to what constitutes "substantial harm" for purposes of determining whether a cybersecurity incident qualifies as a "significant cybersecurity incident" and (iv) require RIAs to regularly amend their Form ADV-C reports any time they discover new information about an incident.

A. 48-Hour Reporting Requirement

The 48-hour reporting requirement in the Proposed Cyber Rules places an undue burden on RIAs while they are in the early stages of assessing and responding to the incident and is inconsistent with state and federal reporting obligations regarding cyber incidents. To rectify the burden and the inconsistency, we suggest that the Commission consider adopting a "prompt" reporting standard.

A "prompt" reporting standard, which is flexible and adaptable to the particular circumstances of the incident, would allow the Staff over time to develop standards for what "prompt" means in different contexts. For example, "prompt" in the context of an RIA experiencing a denial of service to some or all of its systems would likely be a different reporting standard than "prompt" in the context of an RIA learning of unauthorized access to a single email account that theoretically could include confidential investor information, but exactly what was accessed has not yet been determined. A "prompt" reporting standard for the proposed new Form ADV-C is also consistent with the standard for filing other-than-annual amendments to Form ADV.[24] We further note that such an approach is consistent with most state cyber breach reporting obligations, which provide flexible timing requirements such as "without unreasonable delay" or "as soon as possible."[25]

However, if the Commission believes that this reporting should be subject to a more specific, short reporting window, we suggest that 72 hours is more appropriate than 48 hours to, among other things, bring the requirements in line with other federal incident reporting requirements. For example, the recently enacted Cyber Incident Reporting for Critical Infrastructure Act of 2022, which President Biden signed into law on March 15, 2022, requires reporting of a "covered cyber incident" within 72 hours of forming a reasonable belief that such incident occurred.[26]

---

[24] The "prompt" reporting standard is also used for Form 13H, which requires large traders to file initial filings promptly after effecting transactions that reach the identifying activity level and to file amendments promptly following the end of a calendar quarter if any information becomes inaccurate for any reason.

[25] *See, e.g.*, N.Y. GEN. BUS. § 899-aa(2) ("in the most expedient time possible and without unreasonable delay"); CAL. CIV. CODE § 1798.82(a) ("in the most expedient time possible and without unreasonable delay"); NEB. REV. STAT. § 87-803(1) ("as soon as possible and without unreasonable delay"). Indeed, a handful of states that require reporting within a specified timeframe require such notification within 30, 45, or even 60 days. *See, e.g.*, COLO. REV. STAT. § 6-1-716(2) ("but not later than thirty days after the date of determination that a security breach occurred"); MD. CODE COM. LAW § 14-3504(b)(3) ("but not later than 45 days after the business concludes the investigation required . . . ."); CONN. GEN. STAT. § 36a-701b(b)(1) ("but not later than sixty days after the discovery of such breach, unless a shorter time is required under federal law").

[26] Cyber Incident Reporting for Critical Infrastructure Act of 2022, Pub. L. No. 117-103, 136 Stat. 1038 (2022).

B. Reciprocal Exceptions for Form ADV-C and Form PF Filings

The Commission has requested comments as to whether it should provide an exception to the proposed Form ADV-C filing requirement for RIAs that have reported a qualifying cybersecurity incident on Form PF, and vice versa for RIAs that have reported a reporting event on Form ADV-C.[27] We believe the Commission should harmonize the two proposals to avoid duplicative reporting.

* * *

We would be pleased to respond to any inquiries you may have regarding our letter or our views on the Proposed Cyber Rules more generally. Please feel free to direct any inquiries to Marc Elovitz, Kelly Koscuiszka or Alexander Kim at (212) 756-2000.

Respectfully submitted,

SCHULTE ROTH & ZABEL LLP

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

[27] *See* Proposing Release.