NORTH AMERICAN SECURITIES ADMINISTRATORS ASSOCIATION, INC.
750 First Street, NE, Suite 1140
Washington, DC 20002
202/737-0900
www.nasaa.org

April 11, 2022

Submitted by Webform (https://www.sec.gov/cgi-bin/ruling-comments)

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

RE: File No. S7-04-22: Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies

Dear Ms. Countryman:

On behalf of the North American Securities Administrators Association, Inc. ("NASAA"),[1] I am writing in response to U.S. Securities and Exchange Commission ("SEC" or the "Commission") Release No. 33-11028, *Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies* (the "Proposal"),[2] in which the SEC proposes to require SEC-registered investment advisers and funds to adopt and implement written cybersecurity policies and procedures, report significant cybersecurity incidents to the SEC on Form ADV-C, disclose cybersecurity risks and incidents on Form ADV Part 2A, and maintain records related to cybersecurity incidents and program maintenance.

The Proposal describes the important role investment advisers and funds play in our financial markets and the numerous cybersecurity risks that can cause, or be exacerbated by, critical system or process failures.[3] As offered, the Proposal would improve investor protection and confidence by requiring investment advisers and funds to consider, document, and report cybersecurity risks, vulnerabilities, and events. NASAA appreciates the proposed flexibility to allow an adviser or fund to tailor its cybersecurity policies and procedures to address its specific

[1] Organized in 1919, NASAA is the oldest international organization devoted to investor protection. NASAA's membership consists of the securities administrators in the 50 states, the District of Columbia, Canada, Mexico, Puerto Rico, and the U.S. Virgin Islands. NASAA is the voice of securities agencies responsible for grass-roots investor protection and efficient capital formation.

[2] The Proposal is available at https://www.sec.gov/rules/proposed/2022/33-11028.pdf.

[3] Proposal at 6.

President: Melanie Senter Lubin (Maryland)
President-Elect: Andrew Hartnett (Iowa)
Past-President: Lisa Hopkins (West Virginia)
Executive Director: Joseph Brady
Secretary: Kevin Hoyt (New Brunswick)
Treasurer: Claire McHenry (Nebraska)
Directors: William Beatty (Washington)
Marni Gibson (Kentucky)
Leslie Van Buskirk (Wisconsin)
Diane Young-Spitzer (Massachusetts)

"business operations, including its complexity, and the attendant cybersecurity risks."[4] The same policies guided NASAA's adoption of its model *Investment Adviser Information Security and Privacy Rule*[5] and the *NASAA Model Rule for Investment Adviser Written Policies and Procedures under the Uniform Securities Acts of 1956 and 2002*.[6] While there are several differences between the Proposal and NASAA's model rules, we note and appreciate the similarities in the overall regulatory and investor protection goals.

While NASAA supports the Proposal generally and encourages its adoption, we offer several considerations and areas for potential revision below. We agree that requiring the adoption of written cybersecurity policies and procedures will protect investors, though we believe a "phased in" approach that takes into account an investment adviser's assets under management, limited firm operations, and staffing should be applied. We also agree with the proposed disclosure requirements of Form ADV-C and the requirement to provide updates, through the Investment Adviser Registration Depository ("IARD"), until an incident is resolved. NASAA supports the proposed 48-hour reporting period, though we advise the Commission to consider whether changes are required to accord with recent federal legislation.[7] Additionally, the proposed disclosures should be provided to other relevant regulators to assist in regulatory coordination in responding to a cybersecurity incident. Finally, we believe that "inconvenience" rather than "substantial harm" should be the appropriate threshold to trigger reporting when investor information has been accessed because it will urge advisers and funds to inform affected parties earlier, which in turn will allow them to make better informed investment decisions and take earlier precautions to protect their personal information and investments.[8]

---

4 Proposal at 12.

5 NASAA, *Investment Adviser Information Security and Privacy Rule* (May 19, 2019), *available at* https://www.nasaa.org/wp-content/uploads/2019/05/NASAA-IA-Information-Security-and-Data-Privacy-Model-Rule.pdf.

6 NASAA, *NASAA Model Rule for Investment Adviser Written Policies And Procedures Under the Uniform Securities Acts of 1956 And 2002*, (Nov. 24, 2020), *available at* https://www.nasaa.org/wp-content/uploads/2020/07/NASAA-IA-PandP-Model-Rule-and-Sample-Compliance-Grid.pdf.

7 *See* Cyber Incident Reporting for Critical Infrastructure Act of 2022, *available at* https://www.congress.gov/bill/117th-congress/house-bill/2471/text. The new legislation requires the Cybersecurity and Infrastructure Security Agency ("CISA") of the Department of Homeland Security ("DHS") to promulgate a set of rules and guidelines with 24 months of signing on March 15, 2022, and requires covered entities to report cybersecurity incidents to DHS and CISA within 72 hours of discovery and ransomware payments within 24 hours. The legislation also includes a deconflict and harmonization clause seeking to align federal cybersecurity reporting requirements. Accordingly, the Commission may best serve advisers, funds and investors impacted by cybersecurity incidents by coordinating the terms of the Proposal with other federal requirements.

I. Investment Adviser Cybersecurity Risk Management Policies and Procedures

In NASAA's view, the Proposal strikes an appropriate regulatory balance by allowing firms to tailor their cybersecurity policies and procedures to their risks and vulnerabilities. The required considerations retain flexibility in designing appropriate procedures while drawing heavily from respected cybersecurity concepts and standards, such as the confidentiality, integrity and availability triad, and the five-function National Institute of Standards and Technology ("NIST") cybersecurity framework.[9] If the Proposal is adopted, the Commission should assist its registrants by periodically issuing guidance on appropriate and relevant cybersecurity standards as they evolve.[10] This would help advisers and funds remain current in their cybersecurity practices while allowing the Commission to update the information as needed. Advisers and funds undergoing periodic risk assessments, as proposed, could use this guidance to review and modify their policies, thereby protecting themselves and their clients.

We appreciate the significance of cybersecurity threats facing the financial services industry and the need for firms to dedicate resources to address those threats. However, NASAA believes that a staged cybersecurity model would be appropriate for small advisers.[11] The concern is that creating a one-size-fits-all cybersecurity rule that is ill-suited for certain firms could impose extraordinary burdens on small advisers, which in turn could either be passed on to investors in the form of higher fees or lead to compliance lapses. A balance should be drawn between risks and compliance burdens on these entities by modifying the requirements.[12] The proposed flexibility afforded to firms in designing their specific program alleviates some of our concerns; however, small advisers may need more flexibility in order to comply with the new rule.[13]

---

[9] NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (Apr. 16, 2018), *available at* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[10] By way of example, we remind the Commission of its 2020 cybersecurity resiliency guidance and 2015 National Exam Program Risk Alerts regarding cybersecurity initiatives in which the Office of Compliance Inspections and Examinations refers to NIST standards. Updated guidance to covered entities would further cyber resiliency and preparedness. *See, e.g.*, SEC, *OCIE Cybersecurity and Resiliency Observations* (Jan. 27, 2020), *available at* https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf; SEC, *Risk Alert, OCIE Launching Cybersecurity Preparedness Initiative* (Apr. 15, 2014), *available at* https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf.

[11] The monetary threshold and impact to small advisers is discussed at length in the Proposal at 158-69. Impacts on mid-size advisers ($25 million to $100 million AUM) is not discussed.

[12] *See* Proposal at 15, Question 2 (*"Should we scale the proposed requirements based on the size of the adviser or fund?... Would using different thresholds based on assets under management, such as $150 million or $200 million, be appropriate? Would another threshold be more suitable, such as one based on an adviser's or fund's limited operations, staffing, revenues or management?"*). The rule should take into account the totality of circumstances for small advisers, including assets under management, staffing and operations, and management structure. A graduated structure would also ease the transition for firms moving from state to federal regulation as they grow in size and assets under management.

[13] For example, small advisers could be allowed to have longer periods between risk assessments of their programs, and could have longer post-cybersecurity incident update intervals for reporting non-material information.

Small to mid-size advisers and funds often rely on vendors to carry out various business functions and may also outsource their cybersecurity compliance programs. The use of outside experts in designing and maintaining cybersecurity programs is certainly appropriate as long as the adviser's management, firm personnel, or fund managers understand and assume responsibility for implementing any such program. Further, periodic examinations by regulators and required regular firm review are essential to ensure that advisers have implemented written policies and procedures *and* are following or employing those policies and procedures. This extends, as written in the Proposal, to any third-party cybersecurity consultant as well as any sub-adviser or service provider with access to adviser or client information. Advisers and funds should be prepared to demonstrate that any service provider with whom they share data has robust measures in place to protect sensitive information and can comply with the adviser's written policies and procedures.[14]

II. Cybersecurity Incident Reporting

The Proposal would require advisers to report significant cybersecurity incidents to the Commission within 48 hours of forming a "reasonable basis" to conclude that a significant cybersecurity incident has occurred.[15] NASAA generally agrees that 48 hours is sufficient to reach such a conclusion. However, the Commission should consider regulatory harmony with recently enacted legislation in order to determine whether it is appropriate to extend the initial reporting period to 72 hours.[16] We also urge the Commission to provide a process by which such disclosures could also be provided, at a minimum, to the state securities administrators for the jurisdiction where the incident took place and the adviser's home state.[17]

The rule should also require a firm to identify the person or team that is responsible for forming the reasonable basis to believe that a cybersecurity event has occurred as part of its cybersecurity policies and procedures, which should vary based on the firm's specific

---

[14] The staged approach should apply the cybersecurity risk management rule to large firms first, with a longer implementation period for mid-size and small advisers. Larger firms have more leverage to amend contracts and update requirements whereas mid-size and small firms may be locked in until expiration or renewal.

[15] Proposal at 42.

[16] *See supra* note 7.

[17] Federally covered advisers are required to notice file with the jurisdiction where they hold their primary place of business and, generally, jurisdictions where they have six or more clients. By reporting to the home jurisdiction or the jurisdiction where the cybersecurity incident took place, the SEC and state regulators can coordinate investor protection efforts and regulatory responses. Also, such information could potentially be beneficial to state regulators for purposes of examinations of broker-dealers and investment advisers, as well as licensing and registration decisions for individual broker dealer agents or investment adviser representatives. Access to this information would better enable state regulators to protect investors by exercising their antifraud authorities and being able to respond quickly. Finally, investment advisers and funds should be mindful that, regardless of their obligations to federal and state securities regulators, they are also in many instances subject to state data breach notification requirements. Periodic Commission guidance could help firms meet those obligations by reminding them of such requirements. *See infra* note 21.

vulnerabilities, risks, and cybersecurity policies and procedures. The Commission should also provide guidance on what constitutes a "reasonable basis" with an emphasis on over reporting from advisers. Overreporting and receiving a false positive for cybersecurity incidents is a preferable outcome to underreporting and waiting until actual, significant harm has occurred. Time is of the essence during and after a cybersecurity event. The earlier regulators are notified of a potential incident the better the outcome for deterring bad actors, mitigating damage, or recovering assets.[18]

In many cases, a significant cybersecurity event will involve days or weeks of intrusions before being discovered, and the recovery from any such incident will be an extended process. To that end, in addition to the initial reporting requirement, advisers should be required to provide periodic reports to the Commission at weekly intervals. Material changes or updates to the initial report should be provided promptly through amended Forms ADV-C, but investigative updates and non-material changes should be provided, again through amended Forms ADV-C, within seven days from the last report.[19] This ongoing reporting requirement would reveal whether the firm is implementing and following its written cybersecurity policies and procedures. The reporting would also provide the Commission, and potentially other regulators, with appropriate oversight of the cybersecurity incident and response.

As drafted, the Proposal seeks to increase investor protection by mandating incident disclosure to the Commission. As noted above, we urge the Commission to extend mandated reporting to the state securities administrators for the jurisdiction where the cybersecurity incident occurred, as well as the adviser's home jurisdiction. Cybersecurity incidents are an industry-wide concern and state and federal regulators working together can seek to minimize the damage caused by these events. More importantly, state and federal partnerships promote increased awareness among regulators and help identify dangerous activities and potentially systemic risks arising among regulated entities. Information sharing in this context is a net benefit for state securities administrators and the Commission and would easily be facilitated by utilizing the shared IARD system for Form ADV-C filings.[20]

---

[18] Any SEC issued guidance should stress the importance of reporting as soon as possible.

[19] *See* Proposal at 49, Question 44 (*"Should advisers be required to provide the Commission with ongoing reporting about significant cybersecurity incidents? If so, are the proposed requirements to amend Form ADV-C promptly, but in no event more than within 48 hours, sufficient for such reporting? Is this timeframe appropriate? Should we require a shorter or longer timeframe? …."*). The Proposal contemplates amended ADV-C timeframes from every 48 hours up to 30 days from the incident. NASAA feels that seven-day intervals would provide sufficient time to assess, investigate, and begin or further the development of a response plan to a cybersecurity incident while informing the Commission of updates or immaterial changes.

[20] *See* Proposal at 50-51 suggesting the use of IARD for this purpose. State regulators and the SEC utilize IARD for Form ADV submissions, and the site is funded through adviser filing fees. In our view, the IARD system would be a better choice, as a purpose-built solution for disseminating this information to the relevant regulators, rather than using EDGAR for this purpose. If the Commission accepts our recommendations to the Proposal for greater regulatory coordination and information sharing among state and federal securities agencies, IARD would provide a seamless solution.

III. Reporting Threshold for Breaches that Access Investor Information

Cybersecurity breaches in which investor information has been accessed can potentially harm the affected parties beyond the incident at issue. Advisers and funds should not make subjective judgments about the wider risks to investors whose information has been exposed. Accordingly, the appropriate threshold to report an incident in which investor or client information has been accessed should be "inconvenience" rather than "substantial harm".[21] As written, a cybersecurity incident may occur for an adviser or fund but until harm "such as monetary loss or theft of personally identifiable or proprietary information[22]" actually results to the client, it would not be considered a significant adviser or fund cybersecurity incident triggering reporting and disclosure. That threshold entails too much risk. Unauthorized access to an adviser or fund's systems, and an investor's personally identifiable information, should alone trigger a reporting event. A reasonable investor would want to know that his or her information has been accessed, even if the adviser or fund believes it was not stolen or otherwise misappropriated, in order to take identity theft protection or similar measures to mitigate harm before it happens. Requiring Commission reporting of such breaches on the basis of "inconvenience" rather than "substantial harm" will urge reporting entities to provide such information to investors more quickly. Waiting until the harm results would frustrate the investor protection purpose of the Proposal.

The Proposal requires "prompt" disclosure and delivery of brochure amendments to clients reporting any added cybersecurity incident.[23] Prompt is not a defined term in the Proposal, and it is unclear whether the prompt reporting requirement applies to the date of the cybersecurity incident or the date the incident is resolved and the adviser files a final amended report for a significant cybersecurity incident.[24]

---

[21] *See* Proposal at 48, Question 40 (*"Is the proposed 'substantial harm' threshold under the definition of significant adviser and fund cybersecurity incident appropriate? Should we also include 'inconvenience' as a threshold with respect to shareholders, clients and investors? …."*). Further, while the Proposal sets out guidelines for advisers and funds, these entities will likely be aware – or will be advised by counsel – that state data breach notification rules and requirements apply in many of the jurisdiction(s) where impacted investors are located. Those requirements will in many cases compel disclosure to investors well before evidence of substantial harm has surfaced. *See* International Association of Privacy Professionals, *State Data Breach Notification Chart*, March 2021, *available at* https://iapp.org/resources/article/state-data-breach-notification-chart/.

[22] Proposal at 44.

[23] *Id.* at 56. The Proposal also requires a two-year lookback provision for cybersecurity incidents on Form ADV Part 2A. NASAA supports this provision and the associated record keeping requirements.

[24] Proposal at 220, Form ADV-C.

IV. Conclusion

For the reasons expressed above, NASAA supports the Proposal and encourages its adoption with certain revisions. The Proposal increases investor protection by implementing flexible cybersecurity policies and procedures that inure to the benefit of investors and the market. If you have any questions or would like additional information, please do not hesitate to contact the undersigned or NASAA's General Counsel, Vince Martinez, at [redacted].

Sincerely,

Melanie Senter Lubin
NASAA President
Maryland Securities Commissioner