April 8, 2022

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

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

Dear Ms. Countryman:

The American Securities Association (ASA)[1] submits these comments in response to the Securities and Exchange Commission's (SEC) proposed rules regarding cybersecurity risk management for registered investment advisers (RIA) and registered investment companies (Proposal).

While the ASA appreciates the SEC's focus on ensuring sound cybersecurity practices for investment advisers and funds, we believe that several revisions to the Proposal are necessary. Without such revisions it will not have its intended effect without creating unnecessary and costly compliance burdens on registered entities.

While many of the recommendations in this comment letter are specific in nature, we would also like to make a broader comment that RIAs should not have any regulatory advantage over registered broker-dealers in this area because consistent cyber regulation matters a great deal.

Accordingly, the ASA makes the following recommendations:

I. Investment advisers should be permitted 72 hours to report significant cybersecurity incidents.

The Proposal currently requires that RIAs would be required to submit proposed Form ADV-C to the Commission within forty-eight (48) hours of a significant cybersecurity event taking place.

[1] The ASA is a trade association that represents the retail and institutional capital markets interests of regional financial services firms who provide Main Street businesses with access to capital and advise hardworking Americans how to create and preserve wealth. The ASA's mission is to promote trust and confidence among investors, facilitate capital formation, and support efficient and competitively balanced capital markets. This mission advances financial independence, stimulates job creation, and increases prosperity. The ASA has a geographically diverse membership of almost one hundred members that spans the Heartland, Southwest, Southeast, Atlantic, and Pacific Northwest regions of the United States.

While it is reasonable for the SEC to establish a timeline for the reporting of such events, we believe the proposed timeframe is unreasonable.

Investment advisers and businesses must divert an enormous amount of resources and employee time towards investigating the source of and consequences associated with a cyberattack. In most cases, the first forty-eight (48) hours after a major cyberattack are the most critical in determining the extent of any harm done and/or learning about any data that may have been breached. During that period, firms also work diligently to take steps to protect any data and/or sensitive information that may still be vulnerable as a result of the attack.

Firms may not have a clear idea of what to report to the SEC (or any other government body) within forty-eight (48) hours and thus, could end up having to file multiple revisions to Form ADV-C as additional material information comes to light. Further incidents or discoveries could render a previous report "materially inaccurate." Accordingly, we believe that the reporting period should, at a minimum, be extended to seventy-two (72) hours.

II. RIAs should not be required to disclose cyberattacks in the ADV brochure.

The Proposal's requirement that significant cybersecurity incidents be disclosed in the ADV brochure is misguided and could cause unnecessary alarm for customers of an RIA. It is an inherent challenge to inform potentially hundreds of thousands of advisory clients when amendments have been made to Form ADV, and the very purpose of the form is to discuss fees, services, and conflicts of interest.

Additionally, the public disclosure of an incident and cybersecurity policy information could benefit bad actors by telegraphing potential vulnerabilities of certain RIAs.

RIAs should not be required to disclose such information, which is not required of any other regulated entity.

III. The SEC should not require individual branch offices to have their own cybersecurity policies and procedures.

As currently drafted, the Proposal would require each individual branch office of an RIA to have its own policies and procedures regarding cybersecurity. We believe this approach is ill-advised as most branch offices do not have the level of expertise or experience to deal with cybersecurity.

We believe any requirement here should apply to a RIAs home office, which has the responsibility to establish policies and procedures that apply to all branch offices.

IV. The SEC should coordinate efforts with the Cybersecurity & Infrastructure Security Agency (CISA).

If this proposal and related SEC proposal regarding public company disclosure were finalized, a publicly-traded financial services firm would potentially have three proposed reporting requirements from one incident: (1) a CISA reporting requirement; (2) a reporting requirement under the Proposal; and (3) a reporting requirement under the SEC's recently proposed rule for public company cybersecurity disclosure.

The SEC should work closely with CISA to ensure that any new obligations are standardized, and that RIAs, or public companies, are not required to report different information to different federal agencies. This outcome would costly, unnecessary, and burdensome with little regulatory benefit.

To strengthen the Proposal, the SEC should consider providing a safe harbor to firms to comply with SEC rules, if such firms follow CISA's reporting mechanisms and standards.

V. The data "inventorying" requirement included in the Proposal would be cost-prohibitive and not enhance cybersecurity practices.

The Proposal requires a risk assessment and categorization/prioritization of risks based on an inventory of the components of a firm's information systems.

The costs for completing a data inventory would be significant and particularly burdensome on small RIAs. It is also not clear how such a requirement would improve the ability of an RIA or other regulated firm to address cybersecurity risks. In this case, the costs do not outweigh the benefits and we urge the SEC to drop this requirement prior to proceeding with a final rule.

VI. Conclusion

While we appreciate the SEC's prioritization of enhancing cybersecurity for RIAs and investment companies, we believe the changes outlined in this letter are necessary prior to the adoption of any final rule. We look forward to working with SEC commissioners and staff on this initiative as it is considered further.

Sincerely,

Christopher A. Iacovella

Christopher A. Iacovella
Chief Executive Officer
American Securities Association