1100 15th Street NW, Washington, DC 20005
+1 202 919 4940
info@aima.org

aima.org

Vanessa Countryman
Secretary
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-0609

May 9, 2024

Dear Ms. Countryman,

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

The Alternative Investment Management Association ("AIMA")[1] would like to take the opportunity to provide further comment to the U.S. Securities and Exchange Commission ("SEC") on its proposed rule to require registered investment advisers ("advisers") and registered investment companies, including business development companies (collectively, "funds"), to adopt and implement cybersecurity policies and procedures to address cybersecurity risks (the "Proposing Release").[2]

---

1 The Alternative Investment Management Association (AIMA) is the global representative of the alternative investment industry, with around 2,100 corporate members in over 60 countries. AIMA's fund manager members collectively manage more than $3 trillion in hedge fund and private credit assets. AIMA draws upon the expertise and diversity of its membership to provide leadership in industry initiatives such as advocacy, policy and regulatory engagement, educational programs and sound practice guides. AIMA works to raise media and public awareness of the value of the industry. AIMA set up the Alternative Credit Council (ACC) to help firms focused in the private credit and direct lending space. The ACC currently represents over 250 members that manage over $1 trillion of private credit assets globally. AIMA is committed to developing skills and education standards and is a co-founder of the Chartered Alternative Investment Analyst designation (CAIA) – the first and only specialised educational standard for alternative investment specialists. AIMA is governed by its Council (Board of Directors). For further information, please visit www.aima.org.

2 SEC, Proposing Release, "Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies", 87 FR 13524 (March 9, 2022).

We initially submitted comments to the proposed requirements on April 11, 2022.[3] In our prior comment letter, we raise a number of concerns which our members have with the proposed requirements, stating that:

- The 48-hour notification period does not provide sufficient time to conduct a thorough investigation into a potentially significant cyber incident;
- Greater flexibility is needed on the proposed public disclosure requirements;
- A narrowing of the scope of the service providers included in the proposed requirements could reduce costs for advisers and funds and investors without significantly diminishing the positive effects of the new rule;
- A more proportionate and appropriate approach is required in a number of areas as there is a real risk that some of the proposed requirements could cause some advisers and funds to do a disproportionate amount of work for little or no benefit;
- A realistic and reasonable timeframe is required for advisers and funds to implement the new requirements; and
- Despite reasonable efforts, advisers could be penalized as a result of the SEC using its anti-fraud authority for the new rule.

In addition to those abovementioned points, we would like to expand on our stated concern in our initial comments on the requirements for advisers to report significant cybersecurity incidents to the SEC within 48 hours.

If Rule 204-6 under the Investment Advisers Act of 1940, as amended ("Advisers Act"), were adopted as proposed, advisers would be required to report "significant cybersecurity incidents" to the SEC on new Form ADV-C, including on behalf of any registered funds and private funds that experience such incidents. The reports would have to be made **promptly but in no event later than 48 hours after** having a reasonable basis to conclude that a "significant adviser cybersecurity incident" or "significant fund cybersecurity incident" has occurred or is occurring. We understand that Form ADV-C would include both general and specific questions related to the cybersecurity incident, for example, the nature and scope of the incident.

We note, however, that under the adopted amendments to Form PF,[4] the confidential reporting form for certain SEC-registered investment advisers to private funds, large advisers must file reports relating to,

[3] *See* AIMA comment letter, "Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies", File No. S7-04-22 (April 11, 2022), https://www.sec.gov/comments/s7-04-22/s70422-20123067-279404.pdf.

[4] *See* https://www.sec.gov/files/rules/final/2023/ia-6297.pdf.

for example, operations events such a significant cybersecurity incident **no later than 72 hours from the occurrence of the relevant event**.

We believe it would be appropriate therefore for these timelines to be aligned in that advisers would be required to report "significant cybersecurity incidents" to the SEC on new Form ADV-C, within 72 hours instead of 48 hours, as proposed. Unaligned timeframes for submitting reports on cybersecurity incidents would impose a significant incremental burden on advisers, potentially leading to confusion and inconsistencies in the information submitted due to the varying durations allowed for gathering and verifying data. We strongly believe that simplifying and rationalizing the reporting requirements, and thereby reducing administrative burdens, is crucial to maintaining the competitiveness of the U.S. asset management industry.

We would be happy to elaborate further on any of the points raised in this response. For further information, please contact James Delaney, Managing Director, Asset Management Regulation (jdelaney@aima.org).

Yours sincerely,

Jenf Wood

Jennifer Wood
Managing Director, Global Head of Asset Management Regulation & Sound Practices