ADISA
ALTERNATIVE & DIRECT INVESTMENT SECURITIES ASSOCIATION
Education ▲ Networking ▲ Advocacy

450 E. 96th Street
Suite 185
Indianapolis, IN 46240

317-663-4180 *main*
www.adisa.org

May 22, 2023

VIA email: rule-comments@sec.gov
Subject: File No. S7-04-22

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

Re: ***SEC Notice of Proposed Rulemaking titled "Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies."***

File No. S7-04-22, 87 FR 13524, RIN 3235-AN08, (SEC Release No. IA-5956 (March 9, 2022)

Dear Secretary Countryman:

The Alternative and Direct Investment Securities Association ("ADISA")[1] appreciates the opportunity to provide comments on the Securities and Exchange Commission ("SEC") notice of proposed rulemaking titled "**Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies**" and published in the *Federal Register* of March 9, 2022, subsequently reopened on March 15, 2023.

ADISA represents the retail direct investment industry, and as such, seeks to act for both large and small investment firms throughout the United States. As an association, we wholeheartedly support the SEC's efforts to strengthen our nation's posture with respect to financial-sector cybersecurity. Moreover, our member companies overwhelmingly support the move toward greater cybersecurity transparency, as we have always held transparency across all industry

[1] ADISA (Alternative & Direct Investment Securities Association), is the nation's largest trade association for the non-traded alternative investment space (i.e., retail vs. institutional). Through its 4,500 financial industry members (close to 900 firms), ADISA reaches over 220,000 finance professionals, with sponsor members raising in excess of $200 billion in 2021-2 alone, serving more than 1 million investors. ADISA is a non-profit organization (501c6), registered to lobby, and also hosts a related 501c3 charitable non-profit (ADISA Foundation) assisting with scholarships and educational efforts.

sectors as a core value. This is part of our member companies' longstanding efforts to self-police our industry and never shy away from our duties to ensure the highest levels of professional ethics.

However, the proposed rule as written likely would undermine the SEC's objective to address "the effectiveness of disclosures to advisory clients and fund shareholders concerning cybersecurity risks and incidents."[2] Our recommendations to address industry concerns are as follows:

1. ***The SEC Should Focus on Mitigation and Management of Any Cybersecurity Breach in the First 48 Hours to Minimize Harm to Investors.***

   ADISA agrees that a timeline must be in place to ensure companies and firms follow through on all reporting requirements. Firms should share information in a timely manner, but information that is complete and accurate. The proposed 48-hour requirement would be counter-productive for multiple reasons:

   a. The first 48 hours following a cyber-attack are critical, and firms should be focused on mitigating any intrusion, understanding the scope of the attack, protecting and recovering data, and locking out intruders. The SEC should encourage firms to use this limited time and corresponding resources investigating and, subsequently, managing an incident to protect investors from any potential additional harm.

   b. Focusing resources on reporting during the first 48 hours impedes firms' response times and hampers mitigation of an event, negatively impacting investors. Every organization, whether in financial services or any other industry, requires time to investigate and understand cyber intrusions before determining the nature and scope of the incident.

2. ***The SEC Should Create Response Times Appropriate for the Circumstances.***

   Most firms appropriately utilize third-party service providers for various operational and administrative functions, including technology and data storage. A cybersecurity breach may or may not involve more than one firm or be focused on a single vendor, rather than a reporting firm, adding complexity to any investigation. Incidents – and access to information – can occur outside a firm's control, which makes a 48-hour reporting requirement impractical and potentially unachievable, especially if the incident requires the outside vendor to investigate its own systems during that same 48-hour window while also responding to calls from dozens, if not hundreds, of clients separate from the reporting firm.

   Moreover, smaller firms – necessarily with fewer staff – must be particularly judicious with their time in the first few days after a cybersecurity breach. Protecting investors remains paramount. Peeling off human resources that should be, initially, focused on assessment, containment, and working with third-party vendors that manage data should

[2] 87 Fed. Reg. 13525 col. 3

be supported through SEC policies, not unintentionally undermined. Thus, we believe a period of at least five business days is a more appropriate window for enforcing this reporting requirement.

3. ***Alternatively, the SEC Should Implement A Two-Part Notification and Reporting Regime.***

   ADISA supports the overall goal of advisers having cybersecurity incident response and recovery policies and procedures, but it is imperative that any policies are flexible, provide meaningful information to investors and other stakeholders, and yet not so detailed as to unwittingly provide a roadmap for futher, future attacks by bad actors. Thus, we propose an alternative Two-Part Notification and Reporting Regime that ensures timely but also accurate information. Under this proposal, advisers would provide an initial, brief notification that a significant cyber incident had occurred, followed by a more detailed version through Form ADV-C after the incident was contained and remediation efforts completed. Every report would exclude certain sensitive data, such as the remedy itself, disclosure, and cyber-insurance information, because this information is 'fuel' for bad actors and the information is not necessary for the Commission to carry out its expressed objectives.

   ADISA shares the view of other associations that the Commission should not require the filing of any amendments to ADV-C. Our primary concern is this emphasis on numerous forms at the expense of good faith efforts to mitigate a cyber event and report in a timely but meaningful manner. Cybersecurity incidents occur in rapid time, and surrounding facts and circumstances are rarely fully known – if at all – in the first several days. Information changes rapidly as well, such that numerous ADV-C amendments would be required under the Commission's proposal. Such is not consistent with the intent and purpose of reporting a cybersecurity rbeach in the first place.

   In addition, from an administrative perspective ADV-C reporting is serious and must be accurate: multiple filings take time to analyze, draft, and review by responsible parties including risk and legal personnel, outside counsel, operations personnel, compliance officers, etc., approvals from which all would be required.

4. ***The SEC Should Coordinate Efforts with the Cybersecurity & Infrastructure Security Agency (CISA).***

   The SEC should coordinate with other federal regulators to adopt a holistic, uniform federal requirement for reporting cybersecurity and data breach incidents. The SEC is particularly well-positioned to enhance cybersecurity efforts by working within a cohesive and efficient reporting framework through robust information sharing in full coordination with CISA and other agencies and relevant organizations gathering cybersecurity information. Indeed, as we have seen, the impact of bad actors is felt across all industries and sectors; working in unison to thwart cyber-crime has, as its ultimate benefit, all investors.

5. ***The SEC Should Avoid Requiring Disclosure of Breach Details in Brochures.***

   ADISA is concerned by the proposed disclosure requirement forcing firms to publish information about cyber incidents in their brochures. Specifically, we are worried this will potentially cause firms to be viewed as particularly vulnerable to attack and breach; this may unduly create the impression that smaller firms are even more vulnerable. In order to achieve robust cooperation from industry, the SEC should weigh the type of information required to be disclosed against the unwarranted potential damage to a firm's business and reputation.

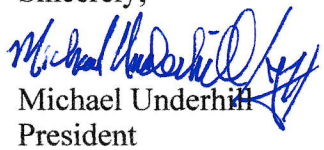
6. ***The SEC Should Not Prescribe Specific Controls Such as Multi-Factor Authentication.***

   As noted by other groups, the requirement by the SEC for specific protocols such as multi-factor authentication is not prudent because technology often becomes outdated well in advance of Rule updates, quickly rendering agency actions moot and, worse, hampering firms and investors alike with antiquated practices and protections. Rather, recognizing the need to embrace the rapidity of technology advancements, ADISA suggests that the SEC promulgate a set of best practices and procedures that firms can choose to adopt based on specific circumstances. This ensures that mandates from the SEC remain applicable and timely, rather than quickly becoming obsolete.

In conclusion, ADISA appreciates the opportunity to provide our comments to the Commission regarding the proposals set forth in the Release. . We enthusiastically support the SEC codifying cybersecurity guidelines for our industry sector. However, we believe our subtle and nuanced adjustments will increase support from the private-sector while also lessening the burden on small firms. We stand ready to discuss our comments at your convenience.

As always, ADISA stands ready to offer objective recommendations and analysis from our unique position within the American economy.

Sincerely,



Michael Underhill
President

cc: Drafting committee--ADISA's Legislative & Regulatory Committee