Managed Funds Association
The Voice of the Global Alternative Investment Industry
Washington, D.C. | New York | Brussels | London

June 22, 2023

Via Electronic Mail: rule-comments@sec.gov

Vanessa A. Countryman
Securities and Exchange Commission
100 F Street, NE
Washington, D.C. 20549-1090

Re: Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies; Reopening of Comment Period; File No. S7-04-22

Dear Ms. Countryman,

Managed Funds Association[1] ("**MFA**") welcomes the opportunity to further comment[2] on the proposed rule release from the Securities and Exchange Commission (the "**Commission**"), "Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies" (the "**Proposed Rules**").[3] These comments supplement our comment letters dated May 22, 2023 ("**May 2023 Comment Letter**")[4] and April 11, 2022 ("**April 2022 Comment Letter**")[5] on the Proposed Rules, and are in furtherance of meetings that we and our members have had with Commissioners and staff of the Commission.

[1] Managed Funds Association ("**MFA**"), based in Washington, D.C., New York, Brussels, and London, represents the global alternative asset management industry. MFA's mission is to advance the ability of alternative asset managers to raise capital, invest, and generate returns for their beneficiaries. MFA advocates on behalf of its membership and convenes stakeholders to address global regulatory, operational, and business issues. MFA has more than 170 member firms, including traditional hedge funds, credit funds, and crossover funds, that collectively manage nearly $2.2 trillion across a diverse group of investment strategies. Member firms help pension plans, university endowments, charitable foundations, and other institutional investors to diversify their investments, manage risk, and generate attractive returns over time.

[2] *See* Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies; Reopening of Comment Period, 88 Fed. Reg. 16921 (March 21, 2023), available at https://www.govinfo.gov/content/pkg/FR-2023-03-21/pdf/2023-05766.pdf.

[3] Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, 87 Fed. Reg. 13524 (Mar. 9, 2022), available at https://www.govinfo.gov/content/pkg/FR-2022-03-09/pdf/2022-03145.pdf.

[4] Managed Funds Association, Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies; Reopening of Comment Period; File No. S7-04-22 (May 22, 2023), https://www.sec.gov/comments/s7-04-22/s70422-192519-383102.pdf.

[5] Managed Funds Association, Comment Letter re Cybersecurity Risk Management, File number S7-04-22 (April 11, 2022), https://www.sec.gov/comments/s7-04-22/s70422-20123280-279547.pdf.

We support the Commission's objective of promoting cybersecurity risk management by investment advisers, but we are concerned that the breadth of certain aspects of the Proposed Rules would in fact result in a *decrease* in overall cybersecurity for the industry.[6] We believe the Commission's goal in this area would best be achieved by narrowing the focus of information covered by the Proposed Rules to the set of adviser information that is likely to cause actual harm in the event of a cybersecurity incident. In addition, as highlighted in the April 2022 Comment Letter, we believe that the burdensome and overly prescriptive reporting requirements that the Proposed Rules would impose on advisers that have been the victim of a cyberattack would have the unintended consequence of diverting advisers' resources during a critical window following discovery of an attack, when advisers would likely need to work with law enforcement officials and communicate with a range of other external parties.

In the Annex to this letter, we offer suggested changes to the Proposed Rules that are intended to offer the Commission alternative approaches to address the relevant policy concerns, as we understand them, while mitigating, at least in part, some of the negative unintended consequences of certain aspects of the Proposed Rules. We have not offered suggested changes to every aspect of the Proposed Rules discussed in our May 2023 Comment Letter and/or April 2022 Comment Letter. Accordingly, the Commission should not read this letter as expressing support for aspects of the Proposed Rules not addressed in the Annex to this letter (*e.g.*, we continue to advocate for amendments to Proposed Rule 204-3(b) that would provide investment advisers a thirty-day timeline to disclose significant cybersecurity incidents to investors, to begin upon the resolution of the significant cybersecurity incident); rather, we continue to encourage the Commission to refer to our previous comment letters and the recommendations therein. Finally, please note that our suggested changes do not include considerations that we believe the Proposed Rules must take into account if the Commission were to proceed, as already described in the record (*e.g.*, coordination with other federal, state and local, and foreign authorities, consistent with the principles announced by the Biden-Harris Administration and Financial Stability Board).[7]

* * *

We appreciate the opportunity to provide additional comments to the Commission on the Proposed Rules, and we would be pleased to meet with the Commission or its staff to discuss our comments. If the staff has questions or comments, please do not hesitate to contact Rachel Grand, Vice President and Senior Counsel, or the undersigned at [redacted].

[6] *See id.*

[7] *See* Recommendations to Achieve Greater Convergence in Cyber Incident Reporting: Final Report, Financial Stability Board (April 13, 2023), available at https://www.fsb.org/wp-content/uploads/P130423-1.pdf; National Cybersecurity Strategy, The White House (March 2023), available at https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

Respectfully submitted,

/s/ Jennifer W. Han

Jennifer W. Han
Executive Vice President
Chief Counsel & Head of Global Regulatory Affairs
Managed Funds Association

cc: The Hon. Gary Gensler, Chairman, Securities and Exchange Commission
The Hon. Hester M. Peirce, Commissioner, Securities and Exchange Commission
The Hon. Caroline A. Crenshaw, Commissioner, Securities and Exchange Commission
The Hon. Mark T. Uyeda, Commissioner, Securities and Exchange Commission
The Hon. Jaime Lizárraga, Commissioner, Securities and Exchange Commission
William Birdthistle, Director, Division of Investment Management, Securities and Exchange Commission

Annex

Subject to the discussion and qualifications in the letter that accompanies this Annex, MFA provides the following suggested textual changes to the Proposed Rules. These suggested changes are intended to offer the Commission alternative approaches to address its policy concerns, as we understand them, while mitigating, at least in part, some of the negative, unintended consequences of some of the more problematic aspects of the proposed Rules. The notes accompanying these suggested changes are intended to highlight certain reasons for the changes but should be read in conjunction with our May 2023 Comment Letter and April 2022 Comment Letter, which provide a fuller explanation of our concerns with the Proposed Rules.

* * *

Please note that rule text edits are marked as follows:
Additions ~~Deletions~~ Transpositions

21. Section 275.204-6 is added to read as follows:

§ 275.204-6 Cybersecurity incident reporting.

a) Every investment adviser registered or required to be registered under section 203 of the Act (15 U.S.C. 80b-3) shall~~:~~

~~(1)~~ ~~R~~report to the Commission any significant adviser cybersecurity incident or significant fund cybersecurity incident, ~~promptly~~ as soon as practicable, but in no event more than ~~48~~ 72 hours, after having a reasonable basis to conclude that any such incident has occurred or is occurring by filing Form ADV-C electronically on the Investment Adviser Registration Depository (IARD); provided, that if such investment adviser has separately notified the Commission of such cybersecurity incident pursuant to another Commission rule, then separate reporting under this paragraph 204-6(a) is not required.

~~(2) Amend any previously filed Form ADV-C promptly, but in no event more than 48 hours after:~~

~~(i) Any information previously reported to the Commission on Form ADV-C pertaining to a significant adviser cybersecurity incident or a significant fund cybersecurity becoming materially inaccurate;~~

~~(ii) Any new material information pertaining to a significant adviser cybersecurity incident or a significant fund cybersecurity incident previously reported to the Commission on Form ADV-C being discovered; or~~

~~(iii)Any significant adviser cybersecurity incident or significant fund cybersecurity incident being resolved or any internal investigation pertaining to such an incident being closed.~~

Notes:

- ***Requiring an adviser to file a report within 48 hours after discovery of a cybersecurity incident would have the negative unintended consequence of diverting adviser resources away from responding to the incident itself and communicating with law enforcement and/or other stakeholders during a critical window.***

- ***Similarly, if an adviser has already notified the Commission of the event, then the resources that would be required to file an additional notification should be conserved so that the adviser may focus on incident response.***
- ***Moreover, a 72-hour reporting window would harmonize with other regulatory requirements to which advisers may be subject, such as the New York Department of Financial Services' Cybersecurity Regulation and the EU General Data Protection Regulation, as well as with "current report" reporting requirements under Form PF. Among other benefits, harmonization of reporting windows would ensure that advisers are filing based on the same information available to the adviser at the applicable point in time, thereby mitigating the risk of investor confusion due to inconsistent reported information.***
- ***As noted in our May 2023 Comment Letter and April 2022 Comment Letter, the Commission should eliminate the proposed requirement to amend initial notices; this would alleviate some of the burden on advisers that are already subject to multiple notification requirements to the Commission (and likely to other agencies) when such advisers are in the process of responding to a cybersecurity incident.***

b) For the purposes of this section:

Adviser information, ~~and~~ *cybersecurity incident*, and *sensitive adviser information* have the same meanings as in §275.206(4)-9 (Rule 206(4)-9 under the Investment Advisers Act of 1940).

Significant adviser cybersecurity incident means a cybersecurity incident, or a group of related cybersecurity 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 sensitive adviser information~~, where the unauthorized access or use of such information results in:~~

~~(i) Substantial harm to the adviser; or~~

~~(ii) Substantial harm to a client, or an investor in a private fund, whose information was accessed~~.

Significant fund cybersecurity incident has the same meaning as in § 270.38a-2 of this chapter (Rule 38a-2 under the Investment Company Act of 1940).

Notes:

- ***A significant adviser cybersecurity incident should refer to an incident (or group of related incidents) that affect the adviser itself. Such an incident may in some cases also affect one or more private fund clients of the adviser, but in other cases, a private fund that is a client of an adviser may be managed by a wholly different entity that has engaged the adviser to provide advisory services to the fund; in the latter circumstance, an incident affecting the fund but not the adviser should not be considered a "significant adviser cybersecurity incident." (Instead, applicable events affecting a fund would fall under the definition of "significant fund cybersecurity incident.")***
- ***Streamlining the definition of "significant adviser cybersecurity incident" as shown above would help to harmonize the reporting requirement threshold with that of other proposed rules (such as those for registered broker-dealers); it would also avoid the outcome of requiring advisers to report an incident that impacts the information of even a single investor, thereby increasing the likelihood that the Commission receives reports regarding incidents that truly have the potential to cause widespread or systemic harm.***
- ***Note that the "substantial harm" elements previously appearing as clauses (i) and (ii) in this definition are not deleted altogether; rather, we have proposed including versions of these elements in the definition of "sensitive adviser information" in Section 275.206(4)-9(c) below. The intent remains that only unauthorized access or use of information that causes substantial harm will comprise a significant cybersecurity incident (as will a significant disruption or degradation of the adviser's ability to maintain critical operations, as set forth in the rule text above).***

22. Section 275.206(4)-9 is added to read as follows:

§ 275.206(4)-9 Cybersecurity policies and procedures of investment advisers.

(a) *Cybersecurity policies and procedures*. As a means reasonably designed to prevent fraudulent, deceptive, or manipulative acts, practices, or courses of business within the meaning of section 206(4) of the Act (15 U.S.C. 80b6(4)), it is unlawful for any investment adviser registered or required to be registered under section 203 of the Investment Advisers Act of 1940 (15 U.S.C. 80b-3) to provide investment advice to clients unless the adviser adopts and implements written policies and procedures that are reasonably designed to address the adviser's cybersecurity risks, including policies and procedures that:

(1) *Risk assessment*.

(i) Require periodic assessments of cybersecurity risks associated with ~~adviser information systems and adviser information residing therein~~ the adviser's investment advisory business, including requiring the adviser to:

(A) ~~Categorize and prioritize cybersecurity risks based on~~ Create an inventory of ~~the components of the~~ systems containing sensitive adviser information ~~systems~~ and the sensitive adviser information residing therein ~~and the potential effect of a cybersecurity incident on the adviser~~; and

(B) Identify the adviser's service providers that receive, maintain, or process sensitive adviser information, or are otherwise permitted to access adviser information systems ~~and any~~ known to contain sensitive adviser information ~~residing therein~~, and assess the cybersecurity risks associated with the adviser's use of these service providers.

(ii) Require written documentation of any risk assessments.

Note:

- ***Focusing advisers' risk assessment undertakings on systems and service providers that handle and process sensitive information, as opposed to any adviser information regardless of the expected impact of unauthorized use, would allow advisers to engage in tailored, informed, and therefore more effective risk mitigation.***

(2) *User security and access*. Require controls designed to minimize user-related risks and prevent unauthorized access to adviser information systems ~~and~~ containing sensitive adviser information and to the sensitive adviser information residing therein, including:

(i) Requiring standards of behavior for individuals authorized to access such adviser information systems and ~~any~~ sensitive adviser information residing therein, such as an acceptable use policy;

(ii) Identifying and authenticating individual users, including implementing authentication measures that require users to present a combination of two or more credentials for access verification;

~~(iii)Establishing procedures for the timely distribution, replacement, and revocation of passwords or methods of authentication;~~

(~~iv~~ iii) Restricting access to ~~specific~~ such adviser information systems or components thereof and sensitive adviser information residing therein ~~solely~~ to groups of individuals requiring access to such systems and information ~~as is necessary for them to~~ for purposes of performing their responsibilities and functions on behalf of the adviser; and ~~(v) Securing remote access technologies.~~

(iv) Securing remote access technologies (for example, through the use of multifactor authentication).

(3) *Information protection*.

(i) Require measures designed to monitor adviser information systems containing sensitive adviser information and protect sensitive adviser information from unauthorized access or use, based on a periodic assessment of the adviser information systems containing sensitive adviser information and the sensitive adviser information that resides on ~~the~~ such systems that takes into account:

(A) The sensitivity level and importance of such sensitive adviser information to its business operations;

(B) Whether ~~any~~ sensitive adviser information is personal information;

(C) Where and how sensitive adviser information is accessed, stored and transmitted, including the monitoring of sensitive adviser information in transmission;

(D) ~~Adviser information systems~~ The access controls and malware protection in place with respect to such adviser information systems; and

(E) The potential effect a cybersecurity incident involving such sensitive adviser information could have on the adviser and its clients, including the ability ~~for~~ of the adviser to continue to provide investment advice.

(ii) Require oversight of service providers that receive, maintain, or process sensitive adviser information, or are otherwise permitted to access adviser information systems ~~and~~ known to contain ~~any~~ sensitive adviser information ~~residing therein~~, and ~~through that~~ as part of such oversight ~~document~~, take measures to confirm

that such service providers~~, pursuant to a written contract between the adviser and any such service provider, are required to~~ implement and maintain appropriate measures that are designed to protect sensitive adviser information and adviser information systems, ~~including~~ which measures should be comparable to, but need not be identical to, the practices described in paragraphs (a)(1), (2), (3)(i), (4), and (5) of this section~~, that are designed to protect adviser information and adviser information systems~~.

(4) *Cybersecurity ~~threat~~*risk *and vulnerability management*.

(i) Require measures intended to detect, mitigate, and remediate ~~any~~ cybersecurity threats and vulnerabilities with respect to ~~adviser information systems and the~~ sensitive adviser information residing ~~therein~~ in adviser information systems, where the nature and extent of such measures is commercially reasonable based on the adviser's risk assessments; and

(ii) Require security training for personnel to address cybersecurity risks identified during periodic assessments of cybersecurity risks associated with sensitive adviser information.

Notes:

- ***Removing the requirement that advisers contract with service providers around the Proposed Rules reflects the reality that many service providers are not subject to Commission oversight and are generally unwilling to agree to be governed by standards set by a regulator that does not regulate them. Many advisers have been pushing unsuccessfully for these terms with vendors for years and, because advisers are a relatively small part of the customer base for many service providers, it is unlikely that adoption of the Proposed Rules will change that outcome. Accordingly, we have proposed that advisers be required to conduct reasonable due diligence when selecting critical service providers and engage in ongoing monitoring of those service providers.***
- ***We support the Commission's objective of mandating adviser policies and procedures related to cybersecurity threats and vulnerabilities. Accordingly, we have proposed additional measures such as training. Advisers will be best situated to determine what measures are warranted for their specific businesses, which may vary across advisers in light of number of employees, number and type of service providers engaged, strategy reliance on information systems, etc.***
- ***Multifactor authentication is likely to be an important component of an adviser's user security and access controls and, accordingly, we have proposed that the use of such technology is one means of satisfying an adviser's obligation in respect of securing remote access technologies. We further encourage the Commission to provide guidance regarding multifactor authentication, including that an adviser may take into account any or all of the circumstances outlined in our April 2022 Comment Letter. Advisers also should have the ability to determine appropriate reasonably equivalent compensating or mitigating controls that may be implemented instead of multifactor***

authentication, similar to what is permitted by the New York Department of Financial Services.[8]

(5) *Cybersecurity incident response and recovery*.

(i) Require measures to detect, respond to, and recover from a cybersecurity incident, including policies and procedures that are reasonably designed to ensure:

(A) Continued material operations of the adviser;

(B) The protection of sensitive adviser information systems ~~and the adviser information residing therein~~;

(C) External and internal cybersecurity incident information sharing and communications; and

(D) Reporting of significant cybersecurity incidents where required under § 275.204-6 (Rule 204-6).

(ii) Require written documentation of any significant cybersecurity incident, including the adviser's response to and recovery from such an incident.

(b) *Annual review*. An adviser must, at least annually:

(1) Review and assess the design and effectiveness of the cybersecurity policies and procedures required by paragraph (a) of this section, including whether they reflect changes in cybersecurity risk over the time period covered by the review; and

(2) ~~Prepare a written report that, at a minimum, describes the review, the assessment, and any control tests performed, explains their results, documents any cybersecurity incident that occurred since the date of the last report, and discusses any material changes to the policies and procedures~~ Maintain a record indicating that the assessment has been performed and noting material changes to risks or controls since the date of the last report.

Notes:

- ***With the proposed revisions to (b)(2), the goal is to require advisers to establish and maintain documentation while also allowing advisers to exercise discretion in determining what details are most meaningful and therefore important to record, as well as to develop a format that is tailored to their particular business and structure.***

[8] *See* Guidance on Multi-Factor Authentication (Dec 7, 2021), available at: https://www.dfs.ny.gov/industry_guidance/industry_letters/il20211207_mfa_guidance.

(c) *Definitions*. For purposes of this section:

Adviser information means ~~any~~ electronic information related to the adviser's investment advisory business, including personal information, received, maintained, created, or processed by the adviser.

Adviser information systems means the 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.

Cybersecurity incident means 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.

Cybersecurity risk means the risk of financial, operational, legal, reputational, and other consequences ~~that could~~ resulting from cybersecurity incidents~~, threats, and vulnerabilities~~.

~~*Cybersecurity threat* means any potential occurrence that may result in an unauthorized effort to adversely affect the confidentiality, integrity, or availability of an adviser's information systems or any adviser information residing therein.~~

Cybersecurity vulnerability means a vulnerability in an adviser's information systems, information system security procedures, or internal controls, including vulnerabilities in their design, configuration, maintenance, or implementation that, if exploited, could reasonably be expected to result in a cybersecurity incident.

Personal information means:

(i) ~~Any i~~Information that can be used, alone or in conjunction with ~~any~~ other information, to identify an individual, such as name, date of birth, place of birth, telephone number, street address, mother's maiden name, Social Security number, driver's license number, electronic mail address, account number, account password, biometric records or other nonpublic authentication information; or

(ii) ~~Any o~~Other non-public information regarding a client's account.

Sensitive adviser information means adviser information, the unauthorized access or use of which (a) would be likely, as determined by the adviser, to result in or (b) in the event of a cybersecurity incident, actually results in:

(i) Substantial harm to the adviser; or

(ii) Substantial harm to a client~~, or an investor in a private fund,~~ whose information was accessed or used in an unauthorized manner.

For purposes of the definition of *significant adviser cybersecurity incident* provided by § 275.204-6(b) of this chapter, only clause (b) of the definition of *sensitive adviser information* in this paragraph (c) would apply.

Notes:

- ***We have proposed retaining the defined terms "cybersecurity incident," "cybersecurity risk," and "cybersecurity vulnerability" (with the edits reflected above) but deleting the term "cybersecurity threat," in order to avoid confusion given the similarities between the definitions of "cybersecurity threat" and "cybersecurity incident." We believe that the notion of a cybersecurity threat is covered by the "risk" and "vulnerability" terms.***
- ***Separately, as noted above, narrowing the scope of the type of information covered by various provisions of the proposed rules to "sensitive adviser information" will increase the likelihood that the Commission receives reports regarding incidents that truly have the potential to cause widespread or systemic harm.***
- ***It will also allow advisers to focus their preventative and mitigation measures on areas that are most vulnerable to meaningful cybersecurity threats.***
- ***Our aim in adding the new sentence at the end of the definition of "sensitive adviser information" indicating that, for purposes of the definitions set forth in § 275.204-6(b), only clause (b) would apply, is to clarify that at least one of the two elements listed in the rule text above – substantial harm to the adviser or substantial harm to a client – would need to have actually occurred in order for the event to be considered a "significant adviser cybersecurity incident" as defined in § 275.204-6(b).***
- ***Tying the definition of "sensitive adviser information" to a standard of actual harm in the event a cybersecurity incident has occurred is consistent with recently adopted rules from the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation.[9]***

(d) *Safe Harbor*. Any adviser registered or required to be registered under section 203 of the Investment Advisers Act of 1940 (15 U.S.C. 80b-3) that meets any of the following criteria will be considered to have reasonably designed its policies and procedures to address the adviser's cybersecurity risks in the manner required by § 275.204-9 (Rule 204-9):

1) The adviser's policies and procedures for the protection of sensitive adviser information are reasonably consistent with one or more industry-recognized cybersecurity frameworks, including (but not limited to) the current version of or any combination of the current versions of:

a) The National Institute of Standards and Technology's Cybersecurity Framework, as may be amended or updated from time to time;

b) The "ISO/IEC 27000-series" information security standards published by the International Organization for Standardization and the International Electrotechnical Commission; and/or

[9] Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 86 Fed. Reg. 66424 (Nov. 23, 2021).

c) The National Futures Association's Information Systems Security Programs, as may be amended or updated from time to time.

Notes:

- ***Establishing a safe harbor for advisers who adopt and utilize programs that align with one or more of the recognized frameworks listed above will promote and encourage the use of such frameworks, allowing advisers and their investors to benefit from the considerable industry expertise and ongoing refinement reflected in each such framework.***
- ***Moreover, advisers who opt to adopt and utilize such programs should not be second-guessed with the benefit of hindsight as to the suitability of their related policies and procedures.***