Federated Hermes, Inc.
1001 Liberty Avenue
Pittsburgh, PA 15222-3779

April 11, 2022

VIA E-MAIL TO RULE-COMMENTS@SEC.GOV

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

Re: Comment Letter of Federated Hermes, Inc. on the Securities and Exchange Commission's Proposed Cybersecurity Rules for Investment Advisers, Registered Investment Companies and Business Development Companies (File No. S7-04-22)

Dear Ms. Countryman:

Federated Hermes, Inc. and its subsidiaries ("**Federated Hermes**") respectfully submit this comment letter to the U.S. Securities and Exchange Commission (the "**Commission**" or the "**SEC**") with respect to the Commission's request for comment on the Commission's proposed new cybersecurity rules and amendments under the Investment Advisers Act of 1940 ("**Advisers Act**") and the Investment Company Act of 1940 ("**Investment Company Act**") (the "**Proposal**")[1]. We appreciate the opportunity to provide comments on the Proposal.

The Commission has proposed, among other things:

- Requiring registered investment advisers ("**advisers**") and investment companies ("**funds**") to adopt and implement written cybersecurity policies and procedures reasonably designed to address cybersecurity risks;
- A new rule and form under the Advisers Act to require advisers to report significant cybersecurity incidents affecting the adviser, or its funds or other clients, to the Commission;
- Amendments to various forms regarding the disclosure related to significant cybersecurity risks and cybersecurity incidents that affect advisers and funds and their clients and shareholders; and
- New recordkeeping requirements under the Advisers Act and Investment Company Act related to proposed cybersecurity management rules and the occurrence of cybersecurity incidents.

We support the Commission's overall objective of protecting investors, other market participants and the financial market in connection with cybersecurity incidents.

[1] Release IC-34497, Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies (February 9, 2022) at https://www.sec.gov/rules/proposed/2022/33-11028.pdf ("Proposing Release").

We support most of the comments and positions of the Securities Industry and Financial Markets Association ("**SIFMA**") as set forth in its letter dated April 11, 2022 (the "**SIFMA Letter**"). Specifically, we agree with the following points raised in the SIFMA Letter:

i. The notification of a cybersecurity incident requirement, including its method of reporting, should be flexible to be efficient;

ii. Incident reporting must be confidential, and the Commission should provide clarity on how it will protect such confidential information from being leaked (to threat actors, the public, etc.);

iii. Cybersecurity issues should be noted in a fund's annual report, not in its prospectus;

iv. Advisers should not be required to continuously update or revise cybersecurity disclosures;

v. Disclosed cybersecurity incidents should not include mention of any vulnerabilities that could be exploited by threat actors; and

vi. While the Commission should continue to recommend risk-management best practices, it should not mandate the implementation of specific security measures or controls to address cybersecurity concerns.

In addition, we provide further comments on the Proposal.

I. Cybersecurity Risk Management Rule

The Commission proposes that advisers and funds adopt and implement written cybersecurity policies and procedures (collectively, the "**program**") that are reasonably designed to address cybersecurity risks that could harm advisory clients and fund investors. The Proposal is not prescriptive in terms of structuring the program, but notes that the program should address several elements including implementation responsibility, risk assessments, user security and access, information protection, threat and vulnerability management, incident response and recovery. Additionally, the Proposal requires an annual review of the program to determine effectiveness.

The Proposal would require advisers and funds, as part of their cybersecurity programs, to address user access controls to restrict system and data access to authorized users.[2] We understand the Commission's goal of reducing "registrants' – and hence their clients' and investors' – exposure to cybersecurity incidents, as well as reduce the costs incurred by registrants (and their clients and investors) in dealing with such incidents."[3] The Proposal, however, lists examples of authentication and authorization methods, including multi-factor authentication ("**MFA**"), as a way to minimize or prevent unauthorized access to information and systems. We have concerns on implementing the general use of authentication and authorization methods, like MFA, when confidential information (e.g., personally identifiable information (**"PII"**) and business identifiable information (**"BII"**)) is not being accessed as such methods can be extremely costly (and time consuming) to implement, regardless of firm size. Therefore, we believe that authentication and authorization methods are necessary only when high-value data (e.g., confidential information) may be accessed. In that instance, in order to protect high-value data, it makes sense to require procedures reasonably designed to seek to limit access permissions to only those individuals with a need to access such data in order to perform his/her job. If high-value data is not being accessed, then authentication and

[2] *Id*. at 23.
[3] *Id*. at 85

authorization methods like MFA are not necessary. Further, we recommend that the Commission not require any specific authentication and authorization method. Instead, the method utilized by a firm should be determined by such firm based on the type of data being accessed and level of impact, if any, should such data be subject to unauthorized access.

We assume that the Proposal requires that the program must be maintained is at firm-wide (i.e., enterprise) level. Accordingly, we request that the Commission confirm in any adopted rules that for organizations that are structured in such a way as to have multiple funds and advisory entities, it is acceptable to establish an appropriate cybersecurity program at the enterprise level, and that the program need not be separately maintained at an individual fund or adviser level. This avoids having multiple iterations of same program implemented throughout the firm.

II. Reporting of Significant Cybersecurity Incidents

The Proposal requires advisers to report to the Commission, on a confidential basis, "significant cybersecurity incidents"[4] affecting the adviser on a new form, Form ADV-C, no more than 48 hours after having a "reasonable basis to conclude that a significant adviser cybersecurity incident or a significant fund cybersecurity incident had occurred or is occurring."[5] Such reporting would cover cybersecurity incidents affecting the adviser, or its fund or private fund clients. Advisers would be required to amend any previously filed Form ADV-C "promptly, but in no event more than 48 hours after, information reported on the form becomes materially inaccurate; if new material information about a previously reported incident is discovered; and after resolving a previously reported incident or closing an internal investigation pertaining to a previously disclosed incident."[6] We request that the Commission provide clarity on how it intends to keep such confidential information from being inadvertently leaked (to threat actors, the public, etc.).

Further, the 48-hours reporting requirement is problematic as it may not afford enough time for an adviser to properly conclude whether a "significant cybersecurity incident" occurred or is occurring.

Therefore, we respectfully request that the Commission strongly consider that the adviser need only notify the Commission via telephone within 48-hours of having a reasonable basis to conclude that a significant cybersecurity incident has occurred or is occurring. This would put the Commission on notice of a potential significant cybersecurity incident, and it would afford the adviser more time to focus on responding to and resolving a potential significant cybersecurity incident. This would be a similar approach to that of the recently adopted rule of the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System and the Federal Deposit Insurance Corporation whereby an entity need only notify its primary federal regulator of any "computer-security incident" that rises to the level of a "notification incident," as soon as possible and no later than 36 hours after the banking organization determines that a notification incident has occurred.[7] In general, overall consistency, with respect to cybersecurity incident reporting obligations, regardless of industry, alleviates confusion. Accordingly, we ask that the Commission consider, where possible, the idea of synchronization of notification efforts across the Commission's proposals related to cybersecurity incident reporting and other federal laws, including the aforementioned recently adopted rule.

We further respectfully request that the Commission consider requiring Form ADV-C be filed at the conclusion of a significant cybersecurity incident. This would alleviate the need to continuously file amended Form ADV-Cs as details regarding cybersecurity incidents evolve.

---

[4] *See* Proposed rule 204-6 under Advisers Act in Proposing Release
[5] Proposing Release at 42
[6] *Id*. at 42
[7] 86 Fed. Reg. 66424 (to be codified at 12 C.F.R. 53; 12 C.F.R. 225, 12 C.F.R. 304) (effective date April 1, 2022).

III. Cybersecurity Risk and Incident Disclosure

Under the Proposal, the Commission is proposing amendments to adviser and fund disclosure requirements to provide current and prospective clients and shareholders with information regarding cybersecurity risks. The Proposal also requires advisers and funds to provide a description of any significant cybersecurity incident that has occurred in the last two (2) years. These disclosure obligations impact an adviser's Form ADV (Part 2A and new Form ADV- C) and a fund's registration statement. Additionally, the Commission is proposing: (i) that advisers "promptly" deliver interim brochure supplements to existing clients if the adviser adds any disclosure of a cybersecurity incident to its brochure or materially revises information related to an already disclosed cybersecurity incident; and (ii) a fund would be required to supplement its prospectus in the event of a significant cybersecurity incident.

We appreciate the Commission's desire to "enhance investor protection by requiring that cybersecurity risk or incident-related information is available to increase understanding in these areas and help ensure that investors and clients can make informed investment decision."[8] However, we raise a general concern on the public disclosure of significant cybersecurity incidents as it may have unintended consequences. Disclosures should not contain any sensitive details of cybersecurity incidents that are not critical for the public's knowledge as revealing such details could lead to exploitation in future cybersecurity incidents. Accordingly, we respectfully recommend that incident disclosures only contain limited, general information that cannot be used by cyber threat actors to orchestrate future cybersecurity incidents (i.e., specific details regarding successful attack strategies or an adviser's/fund's remediation efforts should be omitted).

The Proposal would require an adviser to deliver interim brochure amendments "promptly" to clients. Rather than providing amended brochure supplements to clients every time an adviser adds disclosure of a new cybersecurity incident or materially revises existing incident disclosure on its brochure, we propose that the Commission only require advisers to provide amended brochure supplements to clients once the incident is fully resolved, recognizing premature disclosures may not be fully informed, could be potentially misleading when viewed in hindsight and would, therefore, be of limited use to investors. To the extent PII is compromised, there are a myriad of privacy laws that require notification to clients and law enforcement. Another periodic disclosure requirement, while an incident is ongoing, will only increase costs for advisers and funds, and ultimately clients and shareholders.

IV. Compliance Date

We note that the Proposal does not set forth a compliance date or transition period. Accordingly, while the Commission does not request comment on timing, we request that the Commission provide a reasonable transition period that will give advisers and funds sufficient time to comply with the final rules' requirements. We recommend a minimum compliance period of at least 24 months, should the Proposal be adopted substantially as proposed.

* * *

[8] *Id*. at 13.

Federated Hermes sincerely hopes that the Commission finds these comments helpful and constructive. We are readily available to provide any additional information relating to our comments or discuss any questions that the Commission may have.

Sincerely,

Peter J. Germain
Chief Legal Officer

Cc: The Honorable Gary Gensler
The Honorable Allison Herren Lee
The Honorable Caroline A. Crenshaw
The Honorable Hester M Peirce
William Birdthistle, Director, Division of Investment Management