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

May 9, 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 Public Companies (File Number S7-09-22.)

Dear Ms. Countryman:

Federated Hermes, Inc. and its subsidiaries ("**Federated Hermes**")[1] 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 for public companies ("**registrants**") that are subject to the reporting requirements of the Securities Exchange Act of 1934 (the "**Proposal**")[2].

The Commission has proposed, among other things:

- Disclosing material cybersecurity incidents within four (4) business days, and providing updates related to previously disclosed cybersecurity incidents;
- Disclosures regarding cybersecurity risk management and strategy;
- Disclosures regarding cybersecurity governance; and
- Disclosures regarding board cybersecurity expertise.

We would like to state in advance that Federated Hermes supports most of the comments and positions of the Securities Industry and Financial Markets Association ("**SIFMA**") as set forth in its comment letter on the Proposal ("**SIFMA Letter**"), including:

i. Questioning the Commission being the proper cybersecurity regulator for registrants;
ii. The proposed materiality standard is subjective and vague, and may lead to registrants over-reporting cybersecurity incidents, weakening the concept of "materiality";
iii. Four (4) business days is an insufficient amount of time to investigate and report a material cybersecurity incident;

[1] Federated Hermes, Inc. (NYSE: FHI) is a global leader in active, responsible investment management, with $631.1 billion in assets under management as of March 31, 2022. We deliver investment solutions that help investors target a broad range of outcomes and provide equity, fixed-income, alternative/private markets, multi-asset and liquidity management strategies to more than 11,000 institutions and intermediaries worldwide. Our clients include corporations, government entities, insurance companies, foundations and endowments, banks and broker-dealers.
[2] Release IC-IC-34529; Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (March 9, 2022) at https://www.sec.gov/rules/proposed/2022/33-11038.pdf (the "Proposal").

iv. There should be consistency among existing state and federal cybersecurity incident reporting requirements;

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

vi. Cybersecurity risk management, strategy, and governance disclosure should not include any sensitive details that are not critical to the public's knowledge; and

vii. Rather than disclose a particular Board member's cybersecurity expertise, the Commission should instead permit registrants to disclose if members of the Board engage in regular cybersecurity training.

We understand the Commission's desire to "better inform investors about material cybersecurity risks and incidents on a timely basis"[3], but have concerns about the Proposal's new disclosure requirements for registrants as noted in the SIFMA letter and herein.

I. Disclosing Material Cybersecurity Incidents

The Proposal would amend Form 8-K to require registrants to disclose information about a cybersecurity incident within four (4) business days "after the registrant determines that it has experienced a material cybersecurity incident."[4] This puts a burden on the registrant to understand what constitutes "a material cybersecurity incident." Registrants "need to thoroughly and objectively evaluate the total mix of information, taking into consideration all relevant facts and circumstances surrounding the cybersecurity incident, including both quantitative and qualitative factors, to determine whether the incident is material."[5] Materiality "depends on the significance the reasonable investor would place on" the information[6], regardless of likelihood of an adverse outcome. This subjective "materiality" standard, coupled with a potentially impending filing deadline in order to comply with the four (4) business day disclosure requirement, will result in registrants over-reporting cybersecurity incidents, which may lead to investors undervaluing cybersecurity incident disclosures.

While the Commission expects a registrant's materiality determination to be made "as soon as reasonably practicable after its discovery of the incident"[7], such a determination can take a registrant a substantial amount of time from the discovery of the cybersecurity incident to determine that the incident is, individually or in aggregate, material. Accordingly, we question the overall benefit of the requirement of filing within four (4) business days of such determination. Although the timeframe for filing is conditioned on the registrant's "determination" that a material event has occurred, the requirement as drafted would likely facilitate early disclosure of events which may eventually turn out to be immaterial, resulting in over-disclosure and potential investor confusion. A regime that required telephonic notification to the Commission of a potential material event, coupled with a requirement to file an 8-K at the resolution of a determined material event, would, in our view, be a better approach.

---

[3] *Id.* at 99.
[4] *Id.* at 18.
[5] *Id.* at 23
[6] Basic Inc. v. Levinson, 485 U.S. at 240 (1988).
[7] Proposal at 22.

We believe in overall consistency with respect to cybersecurity incident reporting obligations, regardless of industry, in order to avoid conflicting or overlapping regulations and requirements. Accordingly, we ask that the Commission consider, where possible, synchronization of any notification required by the Proposal with other existing state and federal laws.

Further, we raise particular concern that the public disclosure of details of significant cybersecurity incidents can have unintended consequences. Disclosure of any sensitive details of cybersecurity incidents that are not critical to the public's knowledge should not be required as disclosing such details can lead to exploitation by cyber threat actors in future cybersecurity incidents. Accordingly, we recommend that cybersecurity incident disclosures only contain limited, general information that cannot be used by cyber threat actors to orchestrate future cybersecurity incidents (specific details regarding successful attack strategies or a registrant's remediation efforts should be omitted).

II. Disclosing Cybersecurity Risk Management, Strategy and Governance

The Proposal further requires enhanced disclosure related to: (i) a registrant's policies and procedures for the identification and management of risks from cybersecurity risks; (ii) the board of directors' role in oversight of cybersecurity risks; and (iii) management's role in implementing cybersecurity policies and procedures. According to the Commission, "disclosure of the relevant policies and procedures, to the extent a registrant has established any, would benefit investors by providing greater transparency as to the registrant's strategies and actions to manage cybersecurity risks."[8] Further, the Commission also stated in the Proposal that disclosure "regarding board oversight of a registrant's cybersecurity risk and the inclusion or exclusion of management from the oversight of cybersecurity risks and the implementation of related policies, procedures, and strategies impacts an investor's ability to understand how a registrant prepares for, prevents, or responds to cybersecurity incidents."[9] However, disclosure of cybersecurity risk management, strategy, and governance may increase the vulnerability of registrants to cybersecurity incidents. As previously mentioned, disclosures should not contain any sensitive details that are not critical to the public's knowledge as disclosing such details can lead to exploitation by cyber threat actors in future cybersecurity incidents. Accordingly, any disclosures related to a registrant's cybersecurity management and governance should only contain limited, general information that cannot be used by cyber threat actors to orchestrate future cybersecurity incidents (i.e., registrants should not be required to disclose the actual content of their policies and procedures as such proprietary information may be used against the registrant by a threat actor).

III. Disclosing Board Expertise

The Proposal also requires disclosure about the cybersecurity expertise of members of the board, if any. While the Proposal does not define "cybersecurity expertise", it does include a non-exclusive list of criteria that a registrant may consider when determining whether a member of the board has expertise, including: prior work experience in cybersecurity; any relevant degrees or certifications; or any knowledge, skills, or other background in cybersecurity. If expertise is to be disclosed, then the Commission should provide a definition of, or clarification on what constitutes, "expertise." This would alleviate potentially misleading

[8] *Id.* at 35.
[9] *Id.* at 39

disclosure. The Commission also should make clear that requiring disclosure of a board member's cybersecurity expertise does not require that a board have any board members that are cybersecurity experts. Alternatively, instead of disclosing a particular Board member's cybersecurity expertise, the Commission should instead permit registrants to disclose if members of the Board engage in regular cybersecurity training.

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 believe that the Commission should provide a reasonable transition period that will give registrants 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.

* * *

Federated Hermes appreciates the opportunity to comment on the Proposal. 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