Dimensional Fund Advisors LP
6300 Bee Cave Rd., Building One
Austin, TX 78746

April 26, 2022

Vanessa A. Countryman
Secretary
US Securities and Exchange Commission
100 F Street NE
Washington, DC 20549-1090

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

Dear Ms. Countryman,

Dimensional Fund Advisors LP ("Dimensional") welcomes the opportunity to provide the US Securities and Exchange Commission (the "Commission") with our views on its proposed Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies (the "Proposed Rules").[1] Cybersecurity risk management is a critical area of focus for Dimensional and the funds that we manage, and we support the Commission's goal of improving the efficacy of industry-wide practices to address cybersecurity risks and incidents. Generally, we agree with the recommendations made by the Investment Company Institute (the "ICI") in its April 11, 2022 comment letter,[2] and we urge the Commission to consider the following recommendations.

1. The Commission should give funds and advisers flexibility in how they implement their cybersecurity risk management programs.

We support the Commission's proposal to require funds and advisers[3] to adopt, implement and maintain cybersecurity risk management programs, and we believe it is critical that registrants have the flexibility to customize their programs based on their own business operations. In particular, we believe that the Commission should expressly recognize that a registrant's periodic assessment of its cybersecurity risks—which would be required under the Proposed Rules—should inform how the registrant structures and implements its cybersecurity risk program. For example, a fund should be able to determine that a service provider subject to regulations relating to its cybersecurity program presents comparatively less risk to the fund than a service provider not subject to regulations, and therefore deem it appropriate to review such a service provider's activities on a less frequent basis.

2. The Commission should revise the definitions of "cybersecurity threat" and "significant fund cybersecurity incident."

The proposed definition of "cybersecurity threat" would include "any potential occurrence that may result in an unauthorized effort to adversely affect the confidentiality, integrity or availability of a fund's information systems or any fund information residing therein." As the ICI notes in its letter, the proposed

---

1 *Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies*, Release Nos. 33-11028; 34-94197; IA-5956; IC-34497 (Feb. 9, 2022).

2 Letter from Susan Olson, General Counsel of the ICI, to Vanessa Countryman, Secretary of the Commission, dated April 11, 2022, available at https://www.sec.gov/comments/s7-04-22/s70422-20123076-279408.pdf.

3 Throughout this letter, we use the terms "funds," "advisers," and "registrants" to refer to the registered investment companies and investment advisers that would be subject to the Proposed Rules.

definition of "cybersecurity threat" is overbroad and would reach conduct that may, but is unlikely to, impact fund information and fund systems. We urge the Commission to limit the definition to potential occurrences that are likely to result in a cybersecurity incident, which would be more consistent with the proposed definitions of "cybersecurity risk" and "cybersecurity vulnerability."

Similarly, we believe the proposed definition of "significant fund cybersecurity incident" is too broad. The definition would include an incident that "disrupts or degrades" a fund's ability to maintain critical operations. In our view, the degradation of a fund's systems should not be considered a "significant fund cybersecurity incident" unless it then disrupts the fund's ability to maintain critical operations. We urge the Commission to delete the phrase "or degrades" from the final definition.[4]

3. We believe the proposed requirements to confidentially report and publicly disclose significant cybersecurity incidents could be harmful to funds and advisers.

Under the Proposed Rules, advisers would be required to report significant fund or adviser cybersecurity incidents to the Commission promptly, but not more than 48 hours, after having a reasonable basis to conclude that any such incident has occurred, on new Form ADV-C. While we appreciate that this reporting would help the Commission monitor the effects of a cybersecurity incident on investors, we are concerned that during a cybersecurity incident, an adviser's electronic systems could be compromised. Instead, we urge the Commission to require registrants to confidentially report significant cybersecurity incidents to the Commission by telephone or another method that would avoid the use of potentially compromised electronic systems. Furthermore, requiring advisers to report within 48 or even 72 hours would be difficult and an unnecessary burden during a cybersecurity incident, especially if the incident occurs over a weekend or holiday, is ongoing, and affecting the firm's communication and systems. We strongly urge the Commission to provide advisers with a significantly longer, more reasonable period to report a cybersecurity incident, which would be less burdensome under the circumstances.

The Proposed Rules would also require funds and advisers to publicly disclose in their registration statements or on Form ADV Part 2A, respectively, all significant cybersecurity incidents that have occurred in the last two fiscal years. We are very concerned that the level of detail that the Commission is proposing to require could prove to serve—albeit unintentionally—as a valuable road map for bad actors that have attempted or plan to initiate a cyberattack. For example, the Proposed Rules would require funds to publicly disclose the entities affected by the incident, when the incident was discovered, whether it is ongoing, whether any data was stolen, the effect of the incident, and whether the fund has remediated or is currently remediating the incident. Notably, registrants subject to the Commission's rules[5] would be singled out in having to publicly disclose such detailed information about a cybersecurity incident. We presume that one reason other regulators have chosen *not* to impose burdensome public disclosure requirements is because of the recognition that potential additional harm could result from such disclosures—both to the victim of the cybersecurity incident but also to other similarly situated companies that could become the target of an

---

4 We also believe the same changes should be made to the corresponding definitions of "cybersecurity threat" and "significant adviser cybersecurity incident" proposed under the Investment Advisers Act of 1940 (the "Advisers Act").

5 We note that the Commission has also proposed rules that would require public companies to disclose material cybersecurity incidents. *See Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, Release Nos. 33-11038, 34-94382, and IC-34529 (March 9, 2022).

attack. In our view, the details about cybersecurity incidents are best left outside of the public domain to avoid copycat breaches or intrusions. We believe that the potential harm to funds and advisers of requiring such detailed disclosures outweighs any perceived benefits to investors, and we urge the Commission not to require funds or advisers to publicly disclose significant cybersecurity incidents.

4. The Commission should adopt its cybersecurity risk management program for advisers under Section 211 of the Advisers Act.

Finally, we strongly recommend that the Commission adopt its cybersecurity risk management program for advisers under Section 211 of the Advisers Act, rather than under Section 206. As the ICI explains in its letter, adopting rules governing an adviser's cybersecurity risk program under Section 206 would mean that any time an adviser's program is found to be deficient, the adviser could be cited for engaging in fraudulent, deceptive, or manipulative conduct. We strongly believe that a deficient cybersecurity risk management program should not constitute fraudulent, deceptive, or manipulative conduct, and we urge the Commission to adopt its cybersecurity risk program under Section 211 of the Advisers Act.

* * *

If we can be of further assistance, please do not hesitate to contact Stephanie Hui, Vice President and Counsel. We would welcome the opportunity to expand on our discussion of these issues.

Sincerely,

Catherine L. Newell
General Counsel and Executive Vice President