1211 Avenue of the Americas
19th Floor
New York, NY 10036
Phone: (202) 448-1985
Fax: (866) 516-6923

April 11, 2022

Secretary
Securities and Exchange Commission
100 F Street NE
Washington, DC 20549-1090

Dear Secretary:

RE: Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, File Number S7-04-22

Thank you for the opportunity to comment on the Securities and Exchange Commission (SEC) proposal on Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies. We support the requirement in the proposal that cybersecurity incident data be reported in Inline XBRL format to increase the Commission's ability to assess risk and monitor activities, and to identify trends in cybersecurity incidents, as well as systemic risks across the market. Capturing this information in machine-readable format will ensure that cybersecurity information is more readily available, accessible, and comparable for investors, other market participants, and the Commission.

XBRL US is a nonprofit standards organization, with a mission to improve the efficiency and quality of reporting in the U.S. by promoting the adoption of business reporting standards. XBRL US is a jurisdiction of XBRL International, the nonprofit consortium responsible for developing and maintaining the technical specification for XBRL. XBRL is a free and open data standard widely used in the United States, and around the world, for reporting by public and private companies, as well as government agencies.

This letter provides responses to specific questions raised in the SEC proposal:

*55. Should there be a prospectus disclosure requirement of significant fund cybersecurity incidents for all registered funds? If some types of funds should be exempt, have different disclosure requirements, or not be subject to the proposed structured data requirement, which and why?*

We do not believe there should be an exemption for any type of fund. Although some funds, like Unit Investment Trusts (UIT) are not currently required to report any disclosures in XBRL format, the market of XBRL providers has expanded and matured since the initial program was introduced by the SEC 13 years ago. Given the consistent structure of XBRL, tool providers are easily able to adapt their applications to support reporting by UITs or others who are preparing their filings in XBRL format for the first time. Both tool providers and reporting entities will be able to rapidly

move up the learning curve. The Commission may wish to consider giving additional time to adopt the requirements to those reporting entities like UITs that do not yet file in XBRL format as they may need more time to make changes to current process and identify the appropriate applications to comply.

*63. Should we require all funds to tag significant fund cybersecurity incidents in Inline XBRL, as proposed? Why or why not?*

We support the use of Inline XBRL for fund cybersecurity incidents as the most efficient means to render narrative as well as quantitative disclosures fully searchable and machine-readable. Furthermore, many funds already report other types of data in XBRL format. Requiring cybersecurity data to be reported using the same machine-readable standard will allow many funds to leverage tools they are already using today for financial data; and will reduce the learning curve for reporting. For data consumers, rendering information in the same structured format will enable different types of data to be commingled for comparative and analytical purposes. This, in turn, will facilitate access to the data and keep costs low for funds and for the users of their data, including the Commission itself.

We also support opting for Inline XBRL, rather than traditional XBRL because SEC-reporting entities are accustomed to the Inline XBRL standard which will further facilitate implementation of the new requirements.

*64. Should we require funds to use a different structured data language to tag significant fund cybersecurity incident disclosures? If so, what structured data language should we require?*

XBRL is a mature, widely used standard for financial and narrative data. Given the amount of data already reported by funds in XBRL format, generating cybersecurity incident data in XBRL format as well, will give investors and other data users a complete picture of the investment landscape in a single data format. This will save analysts time and the expense of piecing data together from different data stores. Cybersecurity incident data will be automatically related to other data being reported.

Choosing Inline XBRL will produce cybersecurity information that is immediately both human- and machine-readable. Furthermore, funds will be able to use tools that already exist to prepare their machine-readable cybersecurity incident data. If the Commission chose to create a new (custom) schema, tailored specifically to cybersecurity incident data, data users and data reporting application providers would need to build new applications to generate and consume the data. Custom schema does not generate data that can be shared or commingled with other data, a key objective of the Federal Government's Data Strategy.

As plans are being developed for the final rule, we ask that the Commission ensure that issuers and vendors who support them, receive sufficient compliance date notice, get early access to SEC-supplied resources (draft taxonomy, technical guidance, samples of fully tagged

documents), and have EDGAR Beta test environment access so that test submissions can be conducted. Through discussions with members of an XBRL US working group of filing agents and tool providers that serve the majority of the corporate and investment management community, ideally a 12–15-month window for testing would be provided, starting with providing the market a draft taxonomy, then access to an EDGAR Beta test environment, and on to the initial compliance date. Taking these steps will promote more accurate and consistent tagging, and ensure a successful implementation.

We appreciate the opportunity to provide input to the Commission's proposal on cybersecurity for investment managers. Please feel free to contact me if you have questions concerning our responses, or would like to discuss further. I can be reached at [redacted] or [redacted].

Respectfully,

Campbell Pryde,
President and CEO