

May 9, 2022



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

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

Dear Ms. Countryman:

RE: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, File Number S7-09-22

Thank you for the opportunity to comment on the Securities and Exchange Commission (SEC) proposal on Risk Management, Strategy, Governance, and Incident Disclosure. We appreciate the importance of timely monitoring of cybersecurity incidents that could adversely impact an individual company or industry, for investors tracking investment performance, and for regulators identifying and monitoring potential systemic risks caused by cybersecurity incidents. We support the requirement in the proposal that cybersecurity incident data be reported in Inline XBRL format to enhance the timeliness and granularity of data reported, and to allow consistent tracking of such incidents over time. Capturing this information in machine-readable format will ensure that cybersecurity information is more readily available, accessible, and comparable.

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.

As a standards organization we have assisted in the development of taxonomies that are used today by U.S. entities reporting to regulators including the Federal Energy Regulatory Commission (FERC), and the SEC itself. Developing effective standards that support market participants requires collaborating with all stakeholders along the supply chain, from reporting entities to data collectors to data users. Given the importance of cybersecurity data, we plan to convene a working group to prepare a prototype taxonomy of cybersecurity incident data which may be of assistance to the Commission as it works towards finalizing this rule.

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

*Proposal Question 1. Would investors benefit from current reporting about material cybersecurity incidents on Form 8-K? Does the proposed Form 8-K disclosure requirement appropriately balance the informational needs of investors and the reporting burdens on registrants?*

We agree that investors would benefit from timely disclosure of cybersecurity incidents on Form 8-K, and we recommend that the Commission require that the cover pages of Form 8-Ks published about cybersecurity incidents be XBRL-tagged, as are other Form 8-Ks prepared by public companies. We also suggest that the Item numbers on Form 8-Ks be tagged as well to alert investors that a cybersecurity incident has been reported. This would allow investors and other users to easily identify the topic of a Form 8-K which would help in analysis.

*Proposal Question 9. Should certain registrants that would be within the scope of the proposed requirements, but that are subject to other cybersecurity-related regulations, or that would be included in the scope of the Commission's recently-proposed cybersecurity rules for advisers and funds, if adopted, be excluded from the proposed requirements? For example, should the proposed Form 8-K reporting requirements or the other disclosure requirements described in this release, as applicable, exclude business development companies ("BDCs"), or the publicly traded parent of an adviser?*

All registrants should be required to report in the same way for ease of data use and comparability. The ability to capture all cybersecurity incidents in the same fashion would facilitate understanding trends across market participants, and eliminate the need for data users to cobble together information from multiple data sources prepared in different formats. It would allow data users to collect data from different reporting entities using the same application and commingle the data in the same data store.

*Proposal Question 40. Should we require registrants to tag the disclosures required by proposed Item 1.05 of Form 8-K and Items 106 and 407(j) of Regulation S-K in Inline XBRL, as proposed? Are there any changes we should make to ensure accurate and consistent tagging? If so, what changes should we make? Should we require registrants to use a different structured data language to tag these disclosures? If so, what structured data language should we require? Are there any registrants, such as smaller reporting companies, emerging growth companies, or FPIs that we should exempt from the tagging requirement?*

We agree with the proposal to require Inline XBRL formatting for both text block tagging of narrative and detail tagging of quantitative disclosures. Taking a different structured data approach such as developing a custom XML schema, would result in added costs for all stakeholders, reduced efficiencies in adapting to changes, and the inability to commingle data sets such as financial performance and cybersecurity incident data. Adopting an Inline XBRL approach is most efficient as the data will be rendered in both human- and machine-readable format.

Most reporting entities today are familiar with preparing their data in Inline XBRL so the added cost will be minimized. Data users are accustomed to extracting and analyzing data in Inline XBRL format. Adopting a widely used standard will limit costs for all stakeholders.

To ensure consistent, accurate tagging, we urge the Commission to provide detailed, concrete guidance on the tagging process, as well as early access to a draft taxonomy, sample Inline XBRL

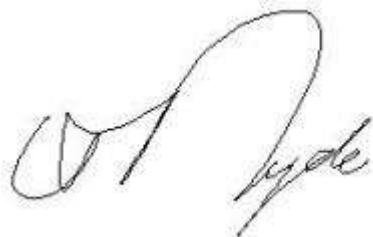
reports and technical guidance, along with the ability to test file in an EDGAR Beta test environment prior to compliance date. Ideally, we ask for a 12-15 month window for testing, with materials as noted above available from the start. Taking these steps will help filers and the providers who work with them to implement the rule successfully and efficiently.

*Proposal Question: Evaluate whether the Commission's estimates of the burden of the proposed collection of information are accurate.*

We agree with the Commission's assertion that the cost of XBRL-formatting will be minimal due to the fact that most filers already comply with XBRL reporting requirements and therefore have the process and applications in place to facilitate the process. Tagging additional cybersecurity incident disclosures will be incremental to their current workflow.

We appreciate the opportunity to provide input to the Commission's proposal on cybersecurity. As noted above, we will report back to the Commission once we have a draft set of standards developed for cybersecurity incidents developed in a working group by collaborating with various market participants. Please feel free to contact me if you have questions concerning our responses, or would like to discuss further. I can be reached at (917) 582 - 6159 or [campbell.pryde@xbrl.us](mailto:campbell.pryde@xbrl.us).

Respectfully,

A handwritten signature in black ink, appearing to read 'Campbell Pryde', is positioned above the typed name.

Campbell Pryde,  
President and CEO