PPG
One PPG Place
Pittsburgh, Pennsylvania 15272 USA
Tel: [redacted]
Fax: [redacted]
vmorales@ppg.com

Vincent J. Morales
Senior Vice President and Chief Financial Officer

May 9, 2022

VIA Electronic Delivery
Vanessa A. Countryman
Secretary
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, D.C. 20549-1090

RE: Comments on File No. S7-09-22: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

Dear Ms. Countryman:

PPG Industries, Inc. ("PPG") respectfully submits comments to the Securities and Exchange Commission (the "Commission") providing its perspective on the Commission's proposed rules entitled "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," Release Nos. 33-11038, 34-94382 (the "Proposed Rules"). PPG is a New York Stock Exchange listed, global manufacturer of paints, coatings and specialty materials with 2021 sales of $16.8 billion.

PPG appreciates the Commission's efforts to standardize the reporting of cybersecurity incidents. PPG, like most companies its size, has taken extensive efforts and spent significant resources to build-out its cybersecurity protections using state-of-the-art protocols, including the National Institute of Standards and Technology's cybersecurity framework. Even with such protections, security breaches will occur, and the Commission's disclosure regime should take into account the unique nature of cybersecurity events. PPG believes that cybersecurity protection benefits all issuers and their shareholders and that disclosure of material cybersecurity incidents and cybersecurity governance is in the best interest of all market participants. However, PPG has concerns about certain aspects of the Proposed Rules and respectfully requests that the Commission consider these comments when formulating the final rules.

A. The Proposed Rules require disclosure of cybersecurity incidents before the time when disclosure may be appropriate.

Prompt reporting of any material incident affecting a public company is generally beneficial to the market and to investors. However, publicly reporting a material cybersecurity incident within four business days of the determination of materiality may result in harm to the reporting company or inhibit an ongoing investigation. PPG appreciates that only material cybersecurity events would require reporting, but it often takes more than four days from the discovery of an incident to determine the extent of the impact of the incident. After discovery of a cybersecurity incident, the issuer will be focused on understanding and mitigating the incident and potentially coordinating with law enforcement. It is only after

these steps are taken that an issuer will be able to determine whether the incident is material. It may take several days for an issuer to determine if the incident is still ongoing, how to mitigate the incident and if sensitive information was stolen, and if so, how much. Requiring a Form 8-K filing within four business days of the determination of materiality could lead to a number of misleading "false positives," as issuers may feel the need to file a Form 8-K before they have had a chance to fully assess the severity of the incident. Because the Proposed Rules state that "a registrant shall make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident,"[1] issuers will be required to make a materiality determination at the same time that they are actively repelling an attack. For example, a retailer learns that its customer credit card database was accessed by an unauthorized party, which appears on its face to be material, so the retailer files a Form 8-K. But after several days, the retailer determines that unauthorized party did not download customers' credit card information. Arguably, this incident only would have been material if the credit card numbers were stolen, but because that appeared to be the case at first, the Form 8-K filed to report the incident likely caused unnecessary harm to the company, its reputation and its stock price.

Moreover, reporting within four business days could hinder the response to the incident. For example, a perpetrator targeting many companies could use certain targets as a test to see if they discover the attack within four business days, and if so, change tactics, regardless of the level of detail required in the Form 8-K. In addition, PPG believes that delaying a Form 8-K during the time an active law enforcement investigation regarding the incident is underway or if requested by the Attorney General is warranted, as the premature disclosure could tip off the perpetrator and render an investigation ineffective. Providing issuers with the flexibility to respond to the incident before making a public disclosure would better protect the issuer, other companies and investors.

B. The Commission should adopt a more principles-based approach to risk management disclosure.

Proposed Item 106(b) of Regulation S-K solicits a level of detail that could provide a potential bad actor with information that could endanger the issuer. In its 2018 *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, the Commission stated that a company need not "make detailed disclosures that could compromise its cybersecurity efforts—for example, by providing a 'roadmap' for those who seek to penetrate a company's security protections."[2] However, PPG is concerned that the disclosures required by proposed Item 106(b) could provide just such a roadmap. PPG supports disclosure of principles-based information about issuers' cybersecurity governance and risk-mitigation activities, but PPG believes that the prescriptive requirements of Item 106(b) could put companies at risk. Principles-based disclosures can provide significant information to investors about the issuer's cybersecurity governance framework and risk-mitigation actions without compromising the issuer's security.

[1] File No. S7-09-22: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure at p. 22.
[2] *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, 83 Fed. Reg. 8166 (26 February 2018). Release Nos. 33-10459, 34-82746.

C. Issuers should not be required to disclose the existence of a cybersecurity expert on the Board of Directors.

Principles-based disclosure about an issuer's cybersecurity risk governance should be sufficient for investors to determine if the issuer has appropriate risk management oversight in place. The requirement to disclose whether the issuer has a cybersecurity expert on the Board of Directors could evolve into a market expectation that all issuers have an expert on their Board. PPG does not believe that the Commission's disclosure rules should be a "de facto" governance requirement. Thousands of companies would become subject to this requirement simultaneously, many of which would need to add a new director to their Board. To meet this requirement, issuers may have to create a new seat on the Board solely for a cybersecurity expert. Unlike the experience necessary to be an "audit committee financial expert," the requirements of proposed Item 407(j) are so specific that there likely is not a large pool of director candidates with this level of expertise who also have the general leadership and business experience to serve as a director of a public company. Directors can gain expertise on cybersecurity (or many other company risks) through educational opportunities, table-top exercises and from the issuer's own cybersecurity team. Issuers would be better served having a cybersecurity expert with the qualifications set forth in proposed Item 407(j) on their management team, rather than on the Board.

PPG appreciates this opportunity to provide feedback and our perspectives on the Proposed Rules. For the reasons set forth above and those in the comment letters submitted by the National Association of Manufacturers, the New York Stock Exchange and other manufacturers, PPG respectfully requests that the Commission consider these comments when formulating the final cybersecurity disclosure rules. If you have any questions about these comments, please do not hesitate to contact me at vmorales@ppg.com or 412-434-3740.

Sincerely,

Vincent J. Morales