May 9, 2022

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

RE: Cybersecurity Risk Management, Strategy, Governance, and Incidence Disclosure Proposed Rule (File Number S7-09-22)

Dear Ms. Countryman:

The Alliance for Automotive Innovation ("Auto Innovators") is pleased to submit comments to the Securities and Exchange Commission ("SEC" or "Commission") on its proposed rule entitled, "Cybersecurity Risk Management, Strategy, Governance, and Incidence Disclosure." Auto Innovators welcomes the opportunity to share the automotive industry's perspectives on the Commission's proposals to require reporting about material cybersecurity incidents; mandate updates about previously reported cybersecurity incidents; and provide periodic disclosures about cybersecurity policies and procedures, their implementation by management, the cybersecurity expertise of Boards of Directors, and Board oversight of cybersecurity risk.

Auto Innovators is the singular, authoritative, and respected voice of the automotive industry. Focused on creating a safe and transformative path for personal mobility, Auto Innovators represents the manufacturers that produce nearly 98 percent of cars and light trucks sold in the United States, original equipment suppliers, technology companies, and other value chain partners within the automotive ecosystem. The automotive industry is the nation's largest manufacturing sector, representing 5.5 percent of the country's GDP and responsible for roughly 10 million jobs.

Automotive companies operate across multiple domains when it comes to cybersecurity, including cybersecurity engineering and product security, operational technology and cyber-physical systems, and information technology. Managing evolving cybersecurity risks, adopting cybersecurity best practices, and engaging in cross-sectoral and public-private partnerships are critical to securing the entirety of the automotive ecosystem. Auto Innovators and its member companies understand the importance of remaining nimble in responding to a dynamic cybersecurity threat environment, particularly as connectivity, electrification, and automation results in the integration of vehicles into a broader ecosystem of connected infrastructure, devices, features, and stakeholders.

While the proposed rule intends to better inform investors about a registrant's "risk management, strategy, and governance and to provide timely notification of material cybersecurity incidents," the disclosures required under the proposed rule may actually undermine the cybersecurity posture of

registrants and their ability to respond to, and recover from, cybersecurity incidents. Specifically, we have the following concerns with the proposed rule:

- **Requiring Registrants to Publicly Report on Ongoing Cybersecurity Incidents:** Having to publicly report on an ongoing cybersecurity incident detracts from a firm's ability to fully remediate by directing resources to the reporting requirement, while also potentially alerting additional bad actors that a firm may be vulnerable. The proposed rule may also have the inadvertent consequence of creating more onerous reporting for firms that invest in strong cybersecurity risk management programs which are more robust and detect more minor threats. Furthermore, the inability to delay reporting due to an external investigation involving law enforcement could negate national security interests and is inconsistent with other cybersecurity incident reporting notification requirements.[1] A foundational underlying principle of the recently enacted Cyber Incident Reporting for Critical Infrastructure Act of 2022[2] is the protection and confidentiality of shared incident information.

- **Mandating Reporting within Four Business Days After Materiality Determination:** While the proposed rule requires a registrant to disclose an incident four business days after it has determined that it has experienced a material event, the SEC states that it expects "management to make a materiality determination about the incident as reasonably practicable after its discovery of the incident."[3] In the immediate aftermath of discovering a cybersecurity incident, a firm is often working with incomplete information about its scope, affected systems and / or data, potential actor(s) responsible, etc. Making a materiality determination quickly may detract from core incident response and remediation activity, particularly because the proposed rule's examples of cybersecurity incidents that may trigger disclosure are so broad. This is layered on top of potential risks and harms to investors that may result when businesses act too quickly to assess the materiality of an event as information rapidly develops and may initially be incomplete. Furthermore, having only four business days to disclose will likely result in multiple incomplete (and potentially inaccurate) disclosures, creating significant administrative burden and cost for registrants, and contributing to confusion for investors and shareholders.

- **Providing Disclosures on Cybersecurity Risk Management, Strategy, and Governance:** The proposed rule would require registrants to periodically disclose their policies and procedures regarding their cybersecurity risk management and strategy, but such information provides little benefit to investors and shareholders without also knowing a firm's system architecture and data practices. Obviously, this level of granularity could provide a bad actor with information to perpetrate a potential cyber-attack. Disclosing whether a registrant's Board of Directors has specific cybersecurity expertise also has little bearing on the overall cybersecurity posture of a firm, especially when a firm may have other personnel, such as a Chief Information Security Officer or CISO, who directs day-to-day cybersecurity risk management operations.

---

[1] For example, state data breach notification laws require firms to report "in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement…or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system." See California Civil Code § 1798.82(a) as an example.

[2] See Division Y of Public Law 117-103.

[3] See 87 FR 16596.

Auto Innovators recommends that the SEC consider certain principles from existing cybersecurity incident reporting requirements, including the recently enacted Cyber Incident Reporting for Critical Infrastructure Act of 2022. These include:

- Protecting sensitive incident information from unnecessary premature disclosure that can further enable malicious cyber threat actors
- Harmonizing cybersecurity incident reporting requirements across the federal government
- Prohibiting the use of incident reporting information for enforcement purposes or regulatory actions
- Incorporating confidentiality, liability, legal privilege, and trade secrets protections for incident reporting information
- Exempting reporting requirements when law enforcement investigations are ongoing

Auto Innovators appreciates being able to weigh in on the SEC's proposed rule. We look forward to continued engagement with the Commission as it considers how to better inform investors about registrants' cybersecurity risk management, strategy, and governance approaches, while also ensuring that firms can maintain strong cybersecurity postures.

Sincerely.

Tara Hairston
Senior Director, Technology, Innovation & Mobility Policy