ALLIANCE FOR AUTOMOTIVE INNOVATION

July 3, 2024

The Honorable Jennie M. Easterly
Director, Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security
245 Murray Lane, Stop 380
Washington, DC 20528-0380

RE: Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements [Docket No. CISA-2022-0010]

Dear Director Easterly:

The Alliance for Automotive Innovation ("Auto Innovators") is pleased to submit comments to the Cybersecurity and Infrastructure Security Agency ("CISA" or "Agency") on its proposed rule ("NPRM") related to reporting requirements under the Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA"). Auto Innovators welcomes the opportunity to provide input on several practical and policy issues related to the implementation of these new reporting requirements under CIRCIA.

Auto Innovators represents the manufacturers that produce most of the cars and light trucks sold in the U.S., original equipment suppliers, battery makers, technology companies, and other value chain partners within the automotive ecosystem. Representing approximately 5 percent of the country's GDP, responsible for supporting nearly 10 million jobs, and driving $1 trillion in annual economic activity, the automotive industry is the nation's largest manufacturing sector.

Technological innovation continues to transform personal mobility with connectivity, automation, digitization, and electrification. These innovations are beneficial to consumers, society, the economy, and the environment, but they also introduce cybersecurity challenges. The automotive industry seeks to manage evolving cybersecurity risks by proactively building cybersecurity into its products and services, adopting cybersecurity best practices, and engaging in cross-sectoral and public-private partnerships. 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. Securing the entirety of the automotive ecosystem remains paramount for the industry.

Information sharing constitutes a key component of the automotive industry's cybersecurity strategy. Such sharing helps stakeholders understand the current cyber threat landscape, and it should occur within industry, across sectors, and between government and

industry. To demonstrate its commitment to information sharing, the automotive industry formed the Automotive Information Sharing and Analysis Center, or Auto-ISAC, in 2015, to share and analyze intelligence about emerging cybersecurity risks to vehicles, as well as to collectively enhance the vehicle cybersecurity capabilities across the global industry. Therefore, Auto Innovators recognizes the importance of CISA developing an effective and efficient cybersecurity incident reporting regime under CIRCIA that supports the sharing of timely and actionable intelligence back to the private sector and does not interfere with existing and successful mechanisms for rapid response information sharing such as the Auto-ISAC.

Auto Innovators maintains that CISA would best achieve this goal by focusing first on the reporting of incidents that have the highest impact on the nation's critical infrastructure. CISA has not taken this approach, however, and has instead issued a NPRM that is broad in its scope and approach. While CISA outlines its consideration of industry feedback received in response to its Request for Information and during its various listening sessions in the NPRM, the Agency has rejected much of that feedback. The expansive nature of the NPRM, if codified into a final rule, will raise compliance burdens for covered entities, as well as increase the risk of unintended consequences. Auto Innovators urges CISA to reconsider its previous input,[1] and ensure that any final rule:

- Takes a risk management approach to the "covered entity" definition and focuses on the critical infrastructure entities with the greatest potential for "debilitating impacts" on the U.S.;

- Limits cybersecurity incident reporting to confirmed incidents that directly impact critical infrastructure;

- Leverages existing mechanisms through which CISA and industry bi-directionally share information to facilitate reporting by third parties, like ISACs; and

- Considers cybersecurity incident reporting by "covered entities" to other regulatory authorities, when done in compliance with those regulators' requirements, to be equivalent to reporting to CISA.

Should CISA choose to progress to a final rule without incorporating the above input, largely like the NPRM, Auto Innovators urges that CISA:

- **Clarify the scope and application of the rule:** CISA should make clear that its final rule does not apply to non-U.S. entities and does not apply to every member of a corporate family simply because one part of the corporate family is in a critical infrastructure sector. For example, research arms that develop potential future technologies that are not

[1] Please see comments submitted by Auto Innovators, CISA-2022-0010-0082.

immediately commercialized should not be covered entities. In addition, CISA should provide further and more detailed examples of excluded incidents, including the actions of good-faith security researchers that may technically qualify as an incident. Auto Innovators also recommends that CISA state more clearly that information sharing and analysis centers, or ISACs, that do perform third-party reporting can do so on behalf of a covered entity.

- **Revise the list of required information for covered cyber incident reports:** CISA should not require entities to report the category or categories of information that was, or reasonably believed to have been, accessed or acquired by unauthorized person(s). Instead, the Agency should require the submission of high-level categories to avoid specific descriptions of data. Further, CISA should not require information on an entity's security defenses, controls, or measures that resulted in the detection or mitigation of the incident. Such information could expose a company's cybersecurity posture, as well as the cybersecurity parameters governing end-products, if the systems holding such information are ever compromised. In addition, it is unclear how such information is relevant to incident reporting.

- **Minimize unintended legal consequences related to reporting:** In its final rule, CISA should clearly state that incident reporting content cannot be used for regulatory or enforcement purposes by Federal, State, Territorial, or local authorities. CISA should anonymize any information shared with other agencies as much as possible, as providing specific entity or individual names or other potentially identifying information will not advance cybersecurity purposes in most cases. In fact, such information could be used to identify targets or otherwise support law enforcement activities. CISA should also clarify what is meant when it says that incident reports can be shared for cybersecurity purposes and the purpose of identifying cybersecurity threats, including their sources, or cybersecurity vulnerabilities. There should be a mechanism to let entities know when incident information is shared for these purposes. Furthermore, CISA should outline any specific way entities should label incident reporting information to ensure they receive the protections outlined in Section 226.18. CISA should also seek to protect incident reports from cyber-attacks.

- **Not require the reporting of vehicle-level data while clarifying application of the rule in the vehicle ecosystem:** Automotive companies are committed to protecting vehicles from cyber-attacks, while also preserving individual privacy. To that end, it is important that CISA does not require that vehicle-level data be included in any reporting required under a final rule. Reporting of vehicle-level data may violate the Electronic Communications Privacy Act. Furthermore, including vehicle-level data in any required reporting would not advance the objectives underpinning CIRCIA. Leaving companies to determine the parameters of these various legal requirements—rather than articulating a clear exclusion—would create unnecessary costs for companies and unnecessary risks to privacy. More broadly, Auto Innovators maintains that CISA should further clarify when incidents in the vehicle ecosystem would be covered by the rule. Excessive uncertainty about the scope of the rule

would require the automotive industry to spend time and effort working through unnecessary questions and lead to differing approaches within the industry, instead of responding to potential cybersecurity incidents.

- **Harmonize incident reporting based on stakeholder input:** Automotive companies have multiple regulators with different mandates. As a result, automotive companies are potentially subject to multiple reporting requirements for incidents involving various aspects of their business. While automotive companies would welcome a reduction in unnecessary duplicative reporting, we also contend that it is important for the right information to be provided to the right regulators at the right time. Moving towards a harmonized approach that routes incident reports to regulators that do not have responsibility for the relevant type of incident will create unnecessary distractions for companies during a cyber incident. It also could disrupt existing, legally required reporting of related issues (*e.g.*, software vulnerabilities that must be reported as safety defects under appropriate circumstances). Given the complexity associated with different types of reporting to different agencies, CISA should seek stakeholder perspectives before making any decision to harmonize reporting that serves different purposes.

- **Share actionable information with the private sector:** It will be important for CISA to use information reported under CIRCIA to strengthen the federal cybersecurity mission, but this alone will not be sufficient to justify the compliance costs under the contemplated rule. Instead, CISA will also need to deliver significant value back to the private sector, including through the Agency's continued engagement with ISACs. Such value includes the broad and prompt distribution of cyber threat intelligence and defensive measures derived from incidents. CISA should ensure that vague national security interests do not prevent companies from receiving the intelligence they need to protect themselves. The Agency should also develop mechanisms to measure the effectiveness of the information it distributes to the private sector and use those measures to inform the management of CIRCIA implementation—and potential future revisions to the rule.

- **Modify definitions in the proposed rule:** CISA should modify the definition of "substantial cyber incident" by adding "serious" or "significant" before "disruption" in (3) and "unauthorized access" in (4). The other prongs of a "substantial cyber incident" have some type of harm/impact threshold, which is appropriate to not inundate CISA with unmanageable volumes of lower risk/impact events as well as to not overwhelm companies with reporting obligations under the rule. The Agency should also change the definition of "supply chain compromise" from "an adversary can leverage" to "an adversary does leverage" because the former could arguably require reporting an unexploited vulnerability that is outside the purview of cybersecurity incident reporting.

Auto Innovators and its member companies appreciate CISA seeking public comment on its proposed rule to implement CIRCIA. The automotive industry maintains that CISA should take a different approach to CIRCIA's reporting requirements to reduce the compliance burden on "covered entities," while still achieving the purposes of the statute. That said, should CISA proceed with its current approach, we ask that the Agency, at a minimum, adjust the proposal to make the rule clearer and more effective, and to ensure that actionable cyber threat information will be shared with industry because of the reporting. We look forward to further engagement with CISA as it continues this important work.

Sincerely,

Tara Hairston

Tara Hairston
Senior Director, Technology Policy