ALLIANCE FOR AUTOMOTIVE INNOVATION

November 14, 2022

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

RE: Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022 [Docket ID: 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") in response to its request for information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA"). Auto Innovators welcomes the opportunity to share the automotive industry's perspectives on CISA's proposed regulations to implement CIRCIA's requirements as they relate to definitions for, and interpretations of, the terminology to be used in the proposed regulations; the form, manner, content, and procedures for submission of required reports; information regarding other incident reporting requirements including descriptions of exploited vulnerabilities; and other policies and procedures that will be required for regulatory implementation.

Auto Innovators is the singular, authoritative, and respected voice of the automotive industry. Auto Innovators represents the manufacturers that produce nearly 98 percent of cars and light trucks sold in the U.S., original equipment suppliers, technology companies, and other value-chain partners within the automotive ecosystem. Representing approximately 5.5 percent of the country's GDP and responsible for roughly 10 million jobs, the automotive industry is the nation's largest manufacturing sector.

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. As a result, the automotive industry has a unique perspective regarding CIRCIA's important objective of protecting critical infrastructure and CISA's role in developing an effective and efficient cybersecurity incident reporting regime.

Given the various implementation aspects of CIRCIA that Congress directs CISA to develop and oversee, Auto Innovators offers the following feedback:

- **<u>Risk-Management Approach to "Covered Entity" Definition:</u>** CIRCIA defines a "covered entity" as "an entity in a critical infrastructure sector, as defined in Presidential Policy Directive

21."[1] CIRCIA also lists factors on which CISA should base its description of "covered entities" including: "the consequences that disruption to or compromise of such an entity could cause to national security, economic security, or public health and safety; the likelihood that such an entity may be targeted by a malicious cyber actor, including a foreign country; *and* the extent to which damage, disruption, or unauthorized access to such an entity, including the accessing of sensitive cybersecurity vulnerability information or penetration testing tools or techniques, will likely enable the disruption of the reliable operation of critical infrastructure" (emphasis added). To focus on the most significant critical infrastructure entities with the greatest potential for debilitating impacts on the U.S., CISA should develop a risk-based approach that encompasses the definitional context from Presidential Policy Directive 21 and the Homeland Security Act of 2002, as amended, and the CIRCIA statutory language. Such an approach should acknowledge and account for the complex operations of potential "covered entities" and apply only to the operations that meet the CIRCIA criteria.

- **Cybersecurity Incident Reporting Triggers:** CIRCIA requires a "covered entity" to report a "covered cyber incident" to CISA no later than 72 hours "after the covered entity reasonably believes that the covered cyber incident has occurred." Auto Innovators contends that "covered entities" should only have to report incidents that are confirmed and that directly impact critical infrastructure. Reporting only confirmed incidents that directly impact critical infrastructure will ensure that the incident information is credible and actionable, minimize reporting burdens on organizations, and avoid inundating CISA with minor events that have negligible impact on the country's national security, economic security, or public health and safety. We also recommend that CISA adhere to CIRCIA's and Presidential Policy Directive 41's[2] definition of "significant cyber incident" to reiterate CISA's focus on cybersecurity incidents, or a group of related cybersecurity incidents, that are "likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the people of the United States."

- **Cybersecurity Incident Reporting Details and Format:** CISA should adopt a standard incident reporting template that sets forth the key information that covered entities should report, if available, within 72 hours after a confirmed~~, material event~~ incident that directly impacts critical infrastructure occurs. A covered entity's primary focus during these early hours must be in investigating and mitigating the cybersecurity incident, and a standard template that identifies key facts, such as the type and vector of attack, will streamline the reporting process and allow "covered entities" to focus on mission critical functions while providing essential information to CISA. CISA should also establish a flexible and permissive regime for supplemental reporting of "covered cyber incidents."

---

[1] Presidential Policy Directive 21 lists 16 critical infrastructure sectors and references the statutory definition of "critical infrastructure" – "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" (see 42 U.S.C. 5195c(e)).

[2] Presidential Policy Directive 41 – United States Cyber Incident Coordination, July 26, 2016. See: Presidential Policy Directive -- United States Cyber Incident Coordination | whitehouse.gov (archives.gov).

- **<u>Third Party Submissions:</u>** CISA should look to its existing information sharing initiatives to provide guidelines or procedures for third-party report submissions, particularly those that may occur through information sharing and analysis centers ("ISACs"). For ISACS and other organizations that participate in previously established programs like CISA's Automated Information Sharing ("AIS") or Cyber Information Sharing and Collaboration Program ("CISCP"), as well as CISA's more recent Joint Cyber Defense Collaborative ("JCDC") initiative, CISA should leverage existing mechanisms through which the Agency and industry bi-directionally share information to facilitate CIRCIA-directed cybersecurity incident reporting by third parties. CISA should also consider negotiating information sharing agreements through the National Council of ISACs and the ISAO Standards Organization to ensure consistency across industry sectors for entities that choose to use the constituent organizations of these two bodies for third party reporting of "covered cyber incidents."

- **<u>Other Reporting Obligations:</u>** CIRCIA directs other Federal agencies to share cybersecurity incident reports with CISA no later than 24 hours after receipt. The law also directs CISA and other Federal agencies to negotiate information sharing agreements that "establish policies, processes, procedures, and mechanisms" to ensure CISA receives cybersecurity incident reports filed with other agencies. To harmonize reporting requirements and to reduce the regulatory burden on organizations, Auto Innovators also urges CISA to consider 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. In addition, we suggest that CISA proactively publish the list of Federal agencies with which it has information sharing/report transmittal agreements already in place, as well as those agencies with which such agreements are in progress. Furthermore, CISA should consider expanding its harmonization and cooperation efforts to its international partners as well, given the global operations of potential "covered entities."

Auto Innovators and its member companies appreciate CISA's interest in public input on approaches to implement the various aspects of its new authorities under CIRCIA. We look forward to further engagement with CISA as it continues this important work.

Sincerely,

Tara Hairston

Tara Hairston
Senior Director, Technology, Innovation, & Mobility Policy