Cybersecurity Coalition

The Honorable Gary Peters
Chairman, Committee on Homeland Security & Government Affairs
United States Senate

The Honorable Rob Portman
Ranking Member, Committee on Homeland Security & Government Affairs
United States Senate

Dear Chair and Ranking Member,

We are writing today in support of several key provisions in the Cyber Incident Reporting Act of 2021. As leaders in the cybersecurity industry, we applaud the Committee's effort to enhance and improve our nation's cybersecurity posture, and we appreciate the collaboration with your staff as you continue to develop and advance this important legislation.

The Coalition is composed of leading companies with a specialty in cybersecurity products and services. We are dedicated to achieving and advancing consensus policy solutions that promote the development and adoption of cybersecurity technologies and best practices. We seek to ensure a robust marketplace that will encourage companies of all sizes to take steps to improve their cybersecurity risk management.

Our comments focus on the incident reporting requirement, specifically Sec. 2322(a)(1) ["Required Reporting of Certain Cyber Incidents"], where a "***covered entity shall report a covered cyber incident to the Director not later than 72 hours after the covered entity reasonably believes that a covered cyber incident has occurred.***"[1] Based on our conversations with your staff and reviewing the legislation, we understand this to mean:

- A company that owns or operates critical infrastructure must report to the Cybersecurity & Infrastructure Security Agency (CISA) a substantial cyber incident within 72 hours of reasonably believing that the integrity, availability, or confidentiality of its information or information system has been unlawfully jeopardized.

[1] • A "covered entity" is defined as an entity that owns or operates critical infrastructure that satisfies the definition that CISA will establish in an interim and then final rule. Our understanding is the term critical infrastructure has the meaning assigned in the Homeland Security Act of 2002.

• A "covered cyber incident" is a substantial cyber incident experienced by a covered entity that satisfies the definition CISA will establish in an interim and then final rule.

•And a "cyber incident" is an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system.

- The “clock” for the 72 hours does not start when the incident began, or when the victim entity learned of the incident, but when the entity reasonably believes that it was a victim of a substantial cyber incident.

We believe that any cyber reporting legislation should 1) provide actionable and timely information to the U.S. Government to reduce and prevent additional harm; 2) balance urgency of notification with accuracy of information; 3) recognize and consider the incident response process for most businesses and organizations, which is identification, containment, eradication, and recovery; and 4) complement, not compete with, the incident response procedures of victim entities.

The Cyber Incident Reporting Act of 2021 meets the above criteria for the following reasons:

Timeliness: The language in Sec. 2322 recognizes that entities need time to determine the significance and severity of an attack, and if in fact a substantial cyber incident has occurred and not a “false positive.” Allowing time for an entity to reasonably believe that a cyber incident has occurred and containment of that harm is essential, and for that reason, we believe any reporting time limit shorter than 72 hours may do more harm than good, both for the entity and for the U.S. Government.

Reporting entity: We strongly agree with the draft legislation that only victim entities and not third-parties should be required to report substantial cyber incidents to the U.S. Government. Third-parties may be able to notify the victim entities of a possible incident but are not in a position of complete knowledge of the entity’s information, nor in a position to determine if an incident meets the “substantial” threshold. Moreover, any third-party reporting obligation that applied to cybersecurity vendors would disrupt confidential customer-vendor relationships that are vital to improving the larger cybersecurity ecosystem.

Regulation: The draft legislation leaves details, such as the definition of a covered entity and a covered cyber incident, for CISA to determine through a rule-making process. This is appropriate since what is useful to report could change over time. We agree that CISA is best positioned to know what information will be most useful and actionable, and we appreciate the direction in the draft legislation requiring CISA to collaboratively engage industry throughout the rule-making process. We recommend ensuring sufficient time for commentary is provided as part of such rulemaking.

Again, thank you for your time and consideration. Should you have any questions, or if we can assist in any other way, please let us know.

Sincerely,

The Cybersecurity Coalition