August 27, 2021

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

The Honorable Mark Warner
Chairman, Select Committee on Intelligence
United States Senate

The Honorable Marco Rubio
Vice Chairman, Select Committee on Intelligence
United States Senate

The Honorable Bennie Thompson
Chairman, Committee on Homeland Security
United States House of Representatives

The Honorable John Katko
Ranking Member, Committee on Homeland Security
United States House of Representatives

The Honorable Yvette Clarke
Chairwoman, Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation
United States House of Representatives

The Honorable Andrew Garbarino
Ranking Member, Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation
United States House of Representatives

Dear Chairs, Vice Chairman, and Ranking Members:

The undersigned associations, representing major sectors of the American economy, including the owners, operators, and those that support and maintain the nation's critical infrastructure, appreciate Congress's ongoing focus on cybersecurity incident reporting legislation. Our industries recognize the value of public-private collaboration facilitated by mutual sharing of actionable information on significant cybersecurity incidents and intrusions with federal agencies. Incident Reporting legislation pending in Congress, when harmonized with the requirements of Section 2 of President Biden's *Executive Order on Improving the Nation's Cybersecurity*, have the potential to improve the nation's cybersecurity posture if appropriately developed and implemented.

To ensure an effective incident reporting regime that leverages the limited resources of federal agencies, enables regulatory compliance, provides liability protections, and advances national cybersecurity interests, we believe that policymakers in Congress should, at a minimum, follow five key principles:

Establish feasible reporting timelines of no less than 72 hours. Cybersecurity incidents are crisis moments for victim organizations. To ensure that the Cybersecurity and Infrastructure Security Agency (CISA) and its interagency partners receive actionable information on truly significant incidents, it is essential to give incident responders time to evaluate the intrusion to determine its impact. Shorter timelines also greatly increase the likelihood that the entity will report inaccurate or inadequately contextualized information that will not be helpful, potentially even undermining cybersecurity response and remediation efforts. A formal report on a verified, significant incident should not preclude less-fulsome notifications to CISA on a more flexible timeline."

Limit reporting regulations to verified incidents and intrusions. Incident reporting should focus on verified incidents rather than potential incidents or "near misses." Reporting verified incidents, that have been well defined and scoped, will avoid a culture of overreporting that will strain limited incident response capacity and capabilities inside and outside the government. It also can help ensure that information received is useful and actionable.

Limit reporting obligations to the victim organization, rather than third-party vendors or providers. Any legislation should ensure that the reporting obligation falls only on compromised affected entities. Vendors and third-party service providers should not be required to report cybersecurity incidents to the US Government that have occurred on their customers' networks and vice versa. Such a requirement would pose numerous challenges to normal business operations, including potentially forcing vendors or third parties to disclose business confidential information of that customer or breach their contractual obligations. Requiring third-parties to report incidents could even disincentivize companies from employing outside cybersecurity services to the detriment of those companies' own security and resilience.

Harmonize federal cybersecurity incident reporting requirements. It is imperative that Congress streamline and normalize federal reporting requirements to ensure resources are used to combat malicious cyber threat activity, rather than customizing reports on the same incident to multiple agencies. Numerous federal agencies currently have disparate incident reporting requirements, many of which are just being implemented. Reported information should be aggregated, anonymized, analyzed, and shared, with government and industry, in a manner to assist in the mitigation and/or prevention of future cyber incidents.

Ensure confidentiality and nondisclosure of incident information provided to the government. It is imperative that any legislation have strong and transparent rules about the confidentiality of incident information that is shared with or by federal agencies. Such rules should govern not only the dissemination of incident information with relevant interagency partners, but should specifically preclude direct or indirect use of such information by the Federal government. These rules must be crafted to guarantee compliance with existing legal regimes, including contractual, intellectual property, and privacy obligations.

Our industries strongly believe that securing the nation's digital assets is a shared responsibility requiring collaboration between the private sector and federal partners. We stand ready to assist policymakers as they develop their proposals on this important national security issue.

Sincerely,

ACT | The App Association

Airlines for America (A4A)

American Fuel & Petrochemical Manufacturers

American Petroleum Institute

American Gas Association

Business Roundtable

BSA | The Software Alliance

The Computing Technology Industry Association

Consumer Technology Association (CTA)

Cyber Coalition

Cyber Threat Alliance

Edison Electric Institute

Electronic Transactions Association

Information Technology Industry Council (ITI)

Internet Association

Software & Information Industry Association

TechNet

Telecommunications Industry Association (TIA)