October 4, 2021

TO THE MEMBERS OF THE SENATE COMMITTEES ON INTELLIGENCE, HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS AND THE HOUSE COMMITTEE ON HOMELAND SECURITY:

Our organizations, which represent sectors across the U.S. economy, are providing input on legislation that would require private sector entities to report certain cyber incidents to the U.S. government. Many of the undersigned groups worked with Congress to develop and pass the Cybersecurity Information Sharing Act of 2015 (CISA 2015). We appreciate the fundamental interests of government to enhance the nation's cybersecurity and the vital contributions of public-private collaboration. Our organizations also recognize the efforts of lawmakers—including Sens. Warner, Rubio, Collins, Peters, and Portman and Reps. Clarke and Katko—and their staff in developing the cyber incident reporting legislation and engaging the business community.

The legislation would create a compulsory cyber incident notification program that imposes serious obligations on the business community. Our groups strongly believe that legislation in this area should include several important provisions. While this list is not comprehensive of our views, these elements would be central to a functioning mandatory incident reporting regime.

- **Establish a prompt reporting timeline of not less than 72 hours.** Legislation should reflect an appropriate, flexible standard for notifying government about significant cyber incidents. Covered entities need time to investigate an intrusion before reporting to an agency, such as the Cybersecurity and Infrastructure Security Agency (CISA). Covered entities should report an incident after conducting initial mitigation and response efforts. Even relatively minor cyber incidents can absorb hundreds of personnel hours to accurately assess.

- **Attach reporting to confirmed cyber incidents.** Businesses need clarity in reporting requirements, which should be targeted to well-defined and confirmed cyber incidents. Some bill language that we have considered—such as "potential cyber intrusions" and incidents that could be "reasonably believed" to be reportable—is overly subjective. Covered cyber incidents should be attached to clear, objective criteria in legislation and any rule that agency and industry stakeholders develop.

- **Confine reports to significant and relevant incidents.** First, legislation should take a step-by-step approach to covering private organizations. A list should be limited in reach—particularly excluding small businesses using existing federal rules—and risk based. Second, per the bills that our organizations have reviewed, the bar for the types of incidents that CISA would determine to be reportable is too low. Reporting the vast number of cyber events of comparatively little importance could easily overwhelm CISA. Third, businesses should not be forced to report insignificant cyber activity when reports on harmful incidents are needed most by stakeholders.

- **Include robust liability protections.** The legislation should establish that the act of reporting a covered incident and the contents of any report, including supplemental reporting, are protected from legal liability. Information contained in notifications should not be subject to discovery in any civil or criminal action. Reporting entities, in essence, should not be penalized after the fact for complying with a legal obligation. In addition, bill writers are urged to aggressively limit the amount of information that covered entities would be required to submit to CISA or their relevant sector regulator.

- **Harmonize federal reporting requirements.** Several critical infrastructure sectors have existing obligations to report significant cyber incidents to federal and/or state regulatory agencies. It is crucial that Congress streamlines federal and state reporting requirements to ensure that industry resources are used efficiently to combat malicious cyber threats, rather than customizing reports on the same incident for multiple agencies. A single report to one agency should suffice to meet legislative and regulatory mandates. Reporting should be made either to CISA or the appropriate sector risk management agency (SRMA), which should then disseminate reports to other relevant agencies.

- **Ensure compliance is supportive, not punitive.** A final bill must create a compliance regime that treats cyberattack victims as victims. A reporting program needs to encourage cooperation and strengthen trust between the public and private sectors. A regulatory-based approach that focuses on punitive actions, such as fines or penalties, rather than mutual gains would run counter to the goal of creating a strong national partnership model to address the increasing cyber threats facing the U.S.

- **Restrict government use of reported data.** This legislation needs to limit the use of information that is provided to the government pursuant to the law. Restrictions on government use of data should closely align with CISA 2015, which contains provisions to exempt reported information from federal and state disclosure laws and regulatory use; treat shared information as commercial, financial, and proprietary; waive governmental rules related to ex parte communications; and preserve trade secret protections and any related privileges or protections.

- **Protect the rulemaking process to guarantee substantial input from industry.** The bills would require CISA to take the lead in writing an interim final rule. Lawmakers are urged to step back from this line of thinking and call on CISA to first provide notice that it intends to promulgate a rule. Aspects of the rule should not be determined by CISA without substantial input from industry. The rulemaking process must include coordination with impacted industry entities because many of the programmatic details, such as definitions and the contents of reporting, would be determined through the rulemaking process. At a minimum, the rulemaking process should feature an initial 90-day consultation period with industry followed by a 90-day comment period.

- **Limit reporting to a victim entity or its designee.** Legislation should generally limit reporting to a victim entity or its designee, including an information sharing and analysis organization or center. Cyber incident response service providers, such as cybersecurity firms, law firms, and insurers, should not be required to report incidents to government

that have occurred on their customers' networks unless explicitly authorized by their customers to do so on their behalf. This approach would avoid unintended outcomes like compelling cybersecurity providers to disclose clients' sensitive business information, breach contractual obligations, and dissuade businesses from employing outside experts to the detriment of businesses' cyber defenses.

- **Treat reporting as a means to bidirectional sharing and collaboration.** Cybersecurity information sharing must be bidirectional. Information reported to government needs to be promptly aggregated, anonymized, analyzed, and shared with industry to foster the mitigation and/or prevention of future cyber incidents. A persistent shortcoming experienced by businesses across many sectors is a lack of timely and effective action or feedback on cyber reports from government. We need legislation that leads to businesses telling our associations that they are receiving actionable data and assistance from CISA, law enforcement, and other agencies to enhance industry groups' security postures.

Our organizations are committed to working with lawmakers and their staff on cyber incident reporting legislation to strengthen our national security and the protection and resilience of U.S. industry. We also believe that the legislation can and must address private sector concerns with forced notifications. It needs to enhance agencies' situational awareness so that government can better inform and partner with businesses that become cyberattack targets or victims.

Sincerely,

ACT | The App Association

Agricultural Retailers Association (ARA)

Airlines for America (A4A)

Alliance for Automotive Innovation

American Chemistry Council (ACC)

American Council of Engineering Companies (ACEC)

American Fuel & Petrochemical Manufacturers (AFPM)

American Gas Association (AGA)

American Petroleum Association (API)

American Property Casualty Insurance Association (APCIA)

American Public Power Association (APPA)

Association of American Railroads (AAR)

Association of Equipment Manufacturers (AEM)

Association of Home Appliance Manufacturers (AHAM)

Association of Metropolitan Water Agencies (AMWA)

BSA | The Software Alliance

CompTIA

CTIA—The Wireless Association

Edison Electric Institute (EEI)

Electronic Transactions Association (ETA)

Global Business Alliance (GBA)

Healthcare Information and Management Systems Society (HIMSS)

Interstate Natural Gas Association of America (INGAA)

National Association of Chemical Distributors (NACD)

National Association of Mutual Insurance Companies (NAMIC)

National Defense Industrial Association (NDIA)

National Retail Federation (NRF)

National Rural Electric Cooperative Association (NRECA)

NCTA—The Internet & Television Association

NTCA—The Rural Broadband Association

The Real Estate Roundtable

Rural Wireless Association (RWA)

SAFE—Securing America's Future Energy

Telecommunications Industry Association (TIA)

U.S. Chamber of Commerce

USTelecom—The Broadband Association

Utilities Technology Council (UTC)