Cyber Incident Reporting for Critical Infrastructure Act

The bipartisan Peters-Portman *Cyber Incident Reporting for Critical Infrastructure Act of 2021* provides necessary tools to identify, warn, and defend against foreign government and criminal organizations conducting ransomware and other cyber-attacks against U.S. critical infrastructure.

Cyber-attacks against U.S. critical infrastructure are a serious national security threat. Today no one U.S. Government agency has visibility into all cyber-attacks occurring against U.S. critical infrastructure on a daily basis. This bill would change that—enabling a coordinated, informed U.S. response to the foreign governments and criminal organizations conducting these attacks against the U.S.

According to Jen Easterly, the Director of the Cybersecurity and Infrastructure Security Agency (CISA) at the Department of Homeland Security, cyber incident reporting legislation is now more important than ever in the context of the recently identified and pervasive log4j vulnerability:

> **"CISA estimates that hundreds of millions of devices in use around the world are potentially susceptible to the log4j vulnerability. We know malicious actors are actively exploiting this vulnerability in the wild. While we are not at this time tracking any confirmed incidents impacting critical infrastructure directly related to log4j, the Federal Government simply does not have the level of information it needs to definitively understand the breadth or nature of intrusions occurring as a result of this severe vulnerability. A cybersecurity incident reporting law would ensure CISA and our partners receive timely information about successful exploitation of critical infrastructure networks quickly after they are discovered, enabling us to help victims mitigate the effects, stop the spread to additional victims, and better track the size, scope, and scale of any adversary campaigns to exploit widespread vulnerabilities like log4j."** *–Jen Easterly, CISA Director*

The *Cyber Incident Reporting for Critical Infrastructure Act*:

- Requires critical infrastructure organizations to report to CISA within 72 hours if they experience a substantial cybersecurity incident and to report within 24 hours of making a ransom payment in response to ransomware.
- Requires other Federal agencies to share reports they receive with CISA and, once they have established processes for doing so, exempts entities that already have to report to another Federal agency from also having to report to CISA.
- Provides robust protections to victim organizations for complying with the law, including liability, privacy, and data use protections.
- Establishes a regulatory harmonization task force for existing Federal cybersecurity regulations.
- Authorizes CISA to first ask and then subpoena critical infrastructure organizations for reports of a substantial cyber incident.
- Establishes a Ransomware Task Force to coordinate ransomware activities across agencies.
- Requires CISA to establish a vulnerability warning pilot program to identify the most commonly used vulnerabilities in ransomware attacks and then notify owners of systems that have those security vulnerabilities exposed on the open internet.
- This information will allow CISA to provide additional assistance to avoid cyber-attacks against our critical infrastructure, like the attacks on Colonial Pipeline and JBS Foods.

The *Cyber Incident Reporting for Critical Infrastructure Act* is supported by industry.
Several industry associations and businesses have signed onto letters of support to commend the work that Sens. Portman and Peters have undertaken with this bill. These associations and businesses include:

- 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)
- AT&T
- Avast
- Broadcom
- BSA | The Software Alliance
- CISCO
- Citrix
- CompTIA
- CTIA—The Wireless Association
- Cyberreason
- Edison Electric Institute (EEI)
- Electronic Transactions Association (ETA)
- Global Business Alliance (GBA)
- Google
- Healthcare Information and Management Systems Society (HIMSS)
- Intel
- Interstate Natural Gas Association of America (INGAA)
- McAfee
- Microsoft
- Mozilla
- 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
- Netscout
- Norton Lifelock
- NTCA—The Rural Broadband Association
- Palo Alto Networks
- Rapid7
- Red Hat
- Resilience
- Rural Wireless Association (RWA)
- SAFE—Securing America's Future Energy
- Schneider Electric
- Telecommunications Industry Association (TIA)
- Tenable
- The Bank Policy Institute
- The Real Estate Roundtable
- U.S. Chamber of Commerce
- USTelecom—The Broadband Association
- Utilities Technology Council (UTC)