December 2, 2014

TO THE MEMBERS OF THE UNITED STATES SENATE:

Our organizations, which represent nearly every sector of the American economy, strongly urge the Senate to pass S. 2588, the Cybersecurity Information Sharing Act of 2014 (CISA), before lawmakers complete their work for the 113th Congress.

S. 2588 passed the Select Committee on Intelligence in July with broad support from both Democrats and Republicans. CISA would promote business security and resilience against cyberattacks, including rogue hackers, sophisticated criminal groups, and foreign powers or their proxies. The bill would help businesses achieve timely and actionable situational awareness to improve detection, mitigation, and response capabilities against cyber threats.

Importantly, the bipartisan bill safeguards privacy and civil liberties, preserves the roles of civilian and intelligence agencies, and incentivizes sharing with narrow liability protections. CISA represents a workable compromise among many stakeholders. The following pages provide additional background on CISA's benefits to the U.S. private sector and its privacy-enhancing provisions.

Cyber threats against U.S. industry are advancing in scope and complexity. We urge the Senate to bring up CISA and pass it during the 113th Congress.

Sincerely,

American Bankers Association
Building Success. Together.

American Chemistry Council

AFPM
American Fuel & Petrochemical Manufacturers

AGA
American Gas Association

energy API
AMERICAN PETROLEUM INSTITUTE

APPA
American Public Power Association

ASIS INTERNATIONAL
Advancing Security Worldwide

American Water Works Association
Dedicated to the World's Most Important Resource

CTIA
The Wireless Association

EEI
Edison Electric Institute
Power by Association

Federation of American Hospitals

FSR BITS

GRIDWISE ALLIANCE

LPPC
LARGE PUBLIC POWER COUNCIL

naed
National Association of Chemical Distributors

National Association of Manufacturers

cable

National Rural Electric Cooperative Association
A Touchstone Energy Cooperative

sifma

U.S. CHAMBER OF COMMERCE

USTELECOM
THE BROADBAND ASSOCIATION

Industry Urges the Senate to Pass CISA

The bipartisan bill safeguards privacy, preserves the roles of civilian and intelligence agencies, and incentivizes appropriate sharing with narrow liability protections.

Our organizations, which represent nearly every sector of the American economy, support S. 2588, the Cybersecurity Information Sharing Act of 2014 (CISA), which the Select Committee on Intelligence passed on July 8 by a strong bipartisan vote. The bill would promote business security and resilience against cyberattacks.[1]

CISA would create a voluntary program, strengthening businesses' protection and resilience against cyberattacks.

- Legislation is necessary to fundamentally improve information-sharing practices between the U.S. government and the business community that reflect the conditions of an increasingly digital world. CISA would create a *voluntary* program to help strengthen the protection and resilience of businesses' information networks and systems against increasingly sophisticated and malicious actors.[2]

- A primary goal of our organizations is to expand government-to-business information sharing, which is progressing but needs improvement.[3] Companies frequently tell us that they need more actionable and up-to-the-minute threat data that only government entities have. We also seek to incent businesses to share cyber threat data with appropriate industry peers and civilian government entities to bolster our critical infrastructure, lifelines, first responders, and business systems.

Limited liability and other protections are vital for expanded sharing.

- Businesses need practical safeguards to increase their information-sharing capabilities. CISA's narrow protections—including limited liability, disclosure, and antitrust provisions—would constructively influence businesses' decisions to share cyber threat data and countermeasures more quickly and frequently.

CISA would complement the administration's cybersecurity executive order and the new framework.

- CISA would complement the new National Institute of Standards and Technology (NIST)-coordinated cybersecurity framework, which many business associations and companies are embracing and promoting with their constituents.

- The 2013 executive order that created the framework is focused, in large part, on increasing "the volume, timeliness, and quality of cyber threat information" shared with businesses. This positive element of the directive calls on government officials to produce timely classified and unclassified reports on cyber threats to specific targets, such as U.S. critical infrastructure.[4]

- Industry welcomes recent calls by John Carlin, assistant attorney general for the Department of Justice, for Congress to pass an information-sharing bill.[5]

The bill would strengthen the protection of personal information residing on business systems.

- Enhancing the situational awareness of companies *would actually increase the security of personal information* that is maintained on company networks and systems. Improved information sharing would bolster individuals' privacy protections, not detract from them. (See CISA's privacy-enhancing protections.)

CISA is one of several cyber legislative priorities of the business community.

- At the outset of the 113th Congress, our organizations urged Congress and the administration to focus on improving information sharing and related protections, pursuing international cooperation against cybercrime and the theft of intellectual property, enhancing national cybersecurity research and development, reforming the Federal Information Security Management Act of 2002, and heightening public awareness and education.

The goal of CISA is to help companies achieve timely and actionable situational awareness to improve the business community's and the nation's detection, mitigation, and response capabilities against increasingly sophisticated and dangerous cyber threats.

Industry urges the Senate to bring up CISA and pass it.

Privacy-Enhancing Provisions in CISA (Select Examples)

CISA would spur information sharing in smart ways and protect and respect privacy. The bill represents a workable compromise among multiple stakeholders.

Shared cyber threat information is narrow in scope.

- CISA's definition of cyber threat indicators (CTIs)—information that is shared and received by appropriate private and federal entities—focuses on information about malicious reconnaissance patterns, methods for defeating security controls, security vulnerabilities, and the actual or potential harm caused by an incident—not on personal information. (p. 4 of the bill)

- CISA calls for public and private entities to *remove personal information* unrelated to a cyber threat when sharing CTIs and countermeasures. The bill would also mandate that entities implement security controls to protect CTIs and countermeasures from unauthorized access. (p. 13 of the bill)

- CTIs and countermeasures received by public sector entities may be used only for "cybersecurity purposes" to ensure that the government does not engage in inappropriate investigations or regulation. The government is prohibited from disclosing, retaining, or using information in ways not authorized by CISA. (pp. 3, 14, 27–29 of the bill)

CISA contains several, overlapping oversight provisions to guard privacy and civil liberties.

- State and local law enforcement agencies or departments need written (or verbal in emergency situations) consent of entities sharing CTIs before preventing, investigating, or prosecuting a computer crime. (pp. 14–15 of the bill)

- CISA would require the attorney general to develop and promulgate procedures for the federal government's use, dissemination, and retention of CTIs that accord with the fair information practice principles (FIPPs)—i.e., appendix A of the *National Strategy for Trusted Identities in Cyberspace*. (p. 19 of the bill)

- The attorney general must, in coordination with other appropriate federal officers, develop and review guidelines on privacy and civil liberties governing the receipt, retention, use, and dissemination of CTIs obtained by a federal entity. The guidelines are expressly meant to limit the impact and use of CTIs that may contain personal information.

  Further, any information containing personal data is to be safeguarded against unapproved access; personal information that is not related to cybersecurity is to be destroyed in a timely manner. (pp. 20–22 of the bill)

- CISA would direct appropriate federal entities to report to Congress every two years to examine the impact that information sharing has on privacy and civil liberties. The Privacy and Civil Liberties Oversight Board (PCLOB) would also report every two years on the policies, procedures, and guidelines established to preserve privacy.

  On top of these protections, inspectors general of the departments of Homeland Security, Justice, and Defense and the intelligence community would jointly report to Congress biennially and may include recommendations from the PCLOB. (pp. 32–36 of the bill)

- CISA contains an "anti-tasking" provision that would prohibit the federal government from requiring a business to share information with the government. (p. 39 of the bill)

Liability protections are conditioned on businesses sharing CTIs with the Department of Homeland Security.

- CISA would establish a "capability and process" in the Department of Homeland Security (DHS)—commonly known as a portal—to accept CTIs submitted in an "electronic format." The bill would require businesses to share electronic threat data exclusively through DHS, a *civilian* entity, in order to receive limited liability protections.

  In contrast, businesses that share cyber information in an electronic format directly with the Defense Department, the FBI, or the NSA would not receive liability protections, outside of limited exceptions in the bill. (pp. 22–25 of the bill)

Notes

[1] See July 10, 2014, Senate Intelligence committee press release, available at www.intelligence.senate.gov/press/record.cfm?id=355018. The text of S. 2588 is available at https://beta.congress.gov/bill/113th-congress/senate-bill/2588?q=%7B%22search%22%3A%5B%22s+2588%22%5D%7D.

[2] Cyber threats are a leading concern to business. "John Dillinger couldn't do a thousand robberies in the same day in all 50 states in his pajamas halfway around the world," FBI Director James Comey told a Senate committee. "That's the challenge we now face with the Internet," he said. The director's comparison to the notorious, Depression-era bank robber reflects a bigger and troubling trend today: The escalating scope and sophistication of cyberattacks outpace our ability to battle them. www.cq.com/doc/congressionaltranscripts-4481146?4

Malicious hackers have been able to prey on households, businesses, and consumers as the Internet and the proliferation of smartphones, tablets, and apps have become increasingly dominant elements in people's lives. It is not easy to get a complete picture of Internet crime. However, organizations such as the Internet Crime Complaint Center (IC3), a partnership established in 2000 between the FBI and the National White Collar Crime Center, provide a window into a troubling trend. According to an IC3 analysis, cybercrime cost the economy $782 million in 2013—a massive jump from $17.8 million in 2001.

The Office of the National Counterintelligence Executive estimates that losses from economic espionage, including the state-sponsored theft of trade secrets, range widely—from $2 billion to hundreds of billions of dollars annually—reflecting a relative scarcity of data and a variety of methods used to assess losses. Nevertheless, losses of sensitive economic information and technologies to foreign entities represent significant costs to U.S. national and economic security.

There is no shortage of reports that calculate the economic impact of cybercrime and espionage. Many companies—including Dell, IBM, McAfee, Microsoft, Symantec, and Verizon—regularly write on the latest threats to organizations, trends in security breaches, and costs to business.

[3] For example, the Department of Homeland Security's Office of Inspector General has reported that the department needs to improve expanding the Enhanced Cybersecurity Services program to all 16 critical infrastructure sectors. See *Implementation Status of the Enhanced Cybersecurity Services Program* (OIG-14-119, July 2014), available at www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-119_Jul14.pdf.

[4] See section 4, "Cybersecurity Information Sharing," of the cyber executive order *Improving Critical Infrastructure Protection*, available at www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[5] On July 30, John Carlin, assistant attorney general for the Department of Justice, spoke on cybercrime at Carnegie Mellon University. His prepared remarks stress the need to go beyond current law and policy to enact an information-sharing bill. "In April [2014], [the FBI] teamed up with the Federal Trade Commission to issue a policy statement making it clear that antitrust law is not and should not be a bar to legitimate cybersecurity information sharing. . . . This guidance will help the private sector collaborate more freely to protect itself. *All of this is just a start. Going forward, we need legislation to facilitate greater information sharing between the private sector and the government* [italics added]." www.justice.gov/nsd/pr/remarks-assistant-attorney-general-john-p-carlin-cyber-crime-carnegie-mellon-university

On March 27, the National Security Council staff issued a statement to *Inside Cybersecurity* affirming the president's support for information-sharing legislation, which includes "targeted liability protection," safeguards for privacy and civil liberties, and the preservation of the "respective roles and missions of civil and intelligence agencies."

The council's statement goes on to say, "Many sophisticated companies currently share cybersecurity information under existing laws. . . . While there is bipartisan consensus on the need for such legislation, it should adhere to the following priorities: (1) carefully safeguard privacy and civil liberties; (2) preserve the long-standing, respective roles and missions of civilian and intelligence agencies; and (3) provide for appropriate sharing with targeted liability protections." See "White House stresses principles for info-sharing legislation, 'targeted' liability protection," *Inside Cybersecurity*, March 28, 2014, available at http://insidecybersecurity.com/Cyber-Daily-News/Daily-News/white-house-stresses-principles-for-info-sharing-legislation-targeted-liability-protection/menu-id-1075.html.