(Current through June 3, 2015)

U.S. Industry Urges the Senate to Pass CISA

The Bill Protects Businesses' and Individuals' Privacy

Agricultural Retailers Association (ARA)
Airlines for America (A4A)
Alliance of Automobile Manufacturers
American Bankers Association (ABA)
American Cable Association (ACA)
American Chemistry Council (ACC)
American Council of Life Insurers (ACLI)
American Fuel & Petrochemical Manufacturers (AFPM)
American Gaming Association
American Gas Association (AGA)
American Insurance Association (AIA)
American Petroleum Institute (API)
American Public Power Association (APPA)
American Water Works Association (AWWA)
ASIS International
Association of American Railroads (AAR)
BITS–Financial Services Roundtable
College of Healthcare Information Management Executives (CHIME)
CTIA–The Wireless Association
Edison Electric Institute (EEI)
Federation of American Hospitals (FAH)
Food Marketing Institute (FMI)
GridWise Alliance
HIMSS–Healthcare Information and Management Systems Society
HITRUST–Health Information Trust Alliance
Large Public Power Council (LPPC)
National Association of Chemical Distributors (NACD)
National Association of Manufacturers (NAM)
National Association of Mutual Insurance Companies (NAMIC)
National Association of Water Companies (NAWC)
National Business Coalition on e-Commerce & Privacy
National Cable & Telecommunications Association (NCTA)
National Rural Electric Cooperative Association (NRECA)
NTCA–The Rural Broadband Association
Property Casualty Insurers Association of America (PCI)
The Real Estate Roundtable
Securities Industry and Financial Markets Association (SIFMA)
Society of Chemical Manufacturers & Affiliates (SOCMA)
Telecommunications Industry Association (TIA)
Transmission Access Policy Study Group (TAPS)
United States Telecom Association (USTelecom)
U.S. Chamber of Commerce
Utilities Telecom Council (UTC)

S. 754, the Cybersecurity Information Sharing Act (CISA) of 2015

- ✓ CISA passed the Senate Select Committee on Intelligence in March with broad support from both political parties and industry.
- ✓ The bill would help businesses achieve timely and actionable situational awareness to improve theirs and the nation's detection, mitigation, and response capabilities against cyber threats.
- ✓ 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.
- ✓ CISA is *not* a surveillance bill.[1]

(Continue to next page.)

U.S. Industry Urges the Senate to Pass CISA

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

The Protecting America's Cyber Networks Coalition (the coalition), which represents nearly every sector of the U.S. economy, supports S. 754, the Cybersecurity Information Sharing Act (CISA) of 2015. The Select Committee on Intelligence passed CISA on March 17 by a strong bipartisan vote of 14 to 1. The bill would promote business security and resilience against cyberattacks.[2]

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.[3]

- A primary goal of our organizations is to expand government-to-business information sharing, which is progressing but needs improvement.[4] 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, lifeline, first responder, 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 defensive measures 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 focuses, 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.[5]

- Industry welcomes the Obama administration's support for two House-passed bills—H.R. 1560, the Protecting Cyber Networks Act (PCNA), and H.R. 1731, the National Cybersecurity Protection Advancement Act (NCPAA) of 2015—that are similar to CISA.[6]

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

- While CISA includes appropriate safeguards for privacy and civil liberties, the bill is designed to enhance the situational awareness of companies, thus increasing the security of data maintained on company networks and systems. Improved information sharing would reinforce individuals' privacy protections, not detract from them. It is simply inaccurate to call S. 754 a surveillance bill.

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 that protect and respect privacy. The bill represents a workable compromise among multiple stakeholders. The coalition rejects privacy groups' efforts to link information sharing to the debate over NSA surveillance reform.

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 defensive measures. The bill would also mandate that entities implement security controls to protect CTIs and defensive measures from unauthorized access. (p. 16 of the bill)

- CTIs and defensive measures 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, 17, 27, 33, 35, and 47 of the bill)

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

- State and local law enforcement agencies or departments need the written (or verbal in emergency situations) consent of entities sharing CTIs before preventing, investigating, or prosecuting a computer crime. (p. 8 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. 23 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. 25–28 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. 38–44 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. 47 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 primarily 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.[7] (pp. 28–31 of the bill)

Sharing Cyber Threat Indicators (CTIs)—Separating Fact From Fiction

Some privacy groups perpetuate the falsehood that "personal information" is typically necessary to identify cyber threats. This position is inaccurate and used to oppose cybersecurity information-sharing legislation.

CISA's definition of cyber threat indicators (CTIs) limits the information that can be shared by businesses and government entities to essentially the tactics, techniques, and procedures used by malicious actors to compromise the computer networks of their victims—not sensitive personal information contained in such networks.

CTIs, according to the bill, describe or identify malicious reconnaissance, a method of defeating a security control or exploitation of a security vulnerability, malicious cyber command and control, the actual or potential harm caused by an incident, among other types of cyber threat data. (pp. 4–5 of the bill)

Here are some types of clinical information that, in the vast majority of cyber incidents, do not implicate a person's behavioral, financial, or social information.

Select Examples of CTIs

- **Domain names** refer to the location of an organization on the Internet.
- **Internet protocol (IP) addresses** are unique numerical identifiers assigned to every computing device connected to the Internet.
- **Log data** can be thought of as the exhaust gas of an information system and often reveals clues associated with a cyberattack.
- **Malware** includes viruses, worms, and Trojan horses.

  Methods of delivering malware include **botnets,** a type of malware that allows an attacker to take control of an infected computer and launch **phishing attacks.** Cybercriminals send out waves of spam email in hopes of "hooking" an unsuspecting individual into clicking on an infected attachment or Web link in an email.
- All communications on the Internet are broken up into **packets** when they are transmitted from, for example, a smartphone to a laptop computer; the packets are reassembled when they reach the destination computer. Each packet contains "header" information (similar to the outside of a mailing envelope), which includes IP addresses.
- Computers use different **ports** to handle various types of Internet traffic (e.g., email traffic is handled on certain ports while website traffic is handled on others). Port information does not reveal traffic contents.
- **Signatures** refer to recognizable, distinguishing patterns associated with a cyberattack (e.g., a binary string in a virus or a particular set of keystrokes used to gain unauthorized access to a network).
- **Time/date stamps** are used to identify the timing of a cyberattack.
- **Uniform Resource Locator (URL)** is a Web (www) address.

In those rare instances where an individual's personal information is embedded within CTIs or defensive measures, CISA calls for public and private entities to *remove such personal information* unrelated to a cyber threat when sharing CTIs and defensive measures. (p. 16 of the bill)

Notes

[1] The House Permanent Select Committee on Intelligence recently marked up and passed H.R. 1560, which is comparable to CISA. Ranking Member Adam Schiff (California) stressed, "No one is a bigger advocate for NSA reform than I've been." He said that he sees the issue as separate from cyber information sharing, where "we've done everything we can to meet the demands of the privacy community" (*Inside Cybersecurity*, March 27, 2015, http://insidecybersecurity.com/Cyber-Daily-News/Daily-News/house-intelligence-leaders-seek-to-defuse-privacy-concerns-around-cyber-info-sharing/menu-id-1075.html).

[2] The text of S. 754 is available at www.congress.gov/114/bills/s754/BILLS-114s754pcs.pdf; the committee report is available at www.congress.gov/114/crpt/srpt32/CRPT-114srpt32.pdf.

[3] 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 last year. "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.

[4] For example, the Department of Homeland Security's (DHS') 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.

[5] 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.

[6] On April 21, 2015, the administration expressed qualified support for H.R. 1560, the Protecting Cyber Networks Act (www.whitehouse.gov/sites/default/files/omb/legislative/sap/114/saphr1560r_20150421.pdf), and H.R. 1731, the National Cybersecurity Protection Advancement Act (NCPAA) of 2015 (www.whitehouse.gov/sites/default/files/omb/legislative/sap/114/saphr1731r_20150421.pdf).

[7] However, several associations believe that cybersecurity information-sharing legislation needs to authorize and protect businesses that share cyber threat indicators and defensive measurers both with any private entity and certain federal government agencies and departments. Many businesses believe that DHS—or any federal entity, for that matter—should not be the sole civilian and protected entity to receive cyber threat data.

Further, several associations in the Protecting America's Cyber Networks Coalition support the flexible approach taken by H.R. 1560, which authorizes and protects businesses when they share cyber threat information with the departments of Commerce, Energy, Homeland Security (Secret Service), Justice (the FBI), Treasury, and the Office of the Director of National Intelligence.