CISA amendments should strengthen the bill—not weaken its clarity and effectiveness
October 19, 2015

Included here is a summary of the coalition's position on the amendments made in order to S. 754, the Cybersecurity Information Sharing Act of 2015 (CISA) on August 5. A more detailed review of each one begins on page 10.

Brief amendment analyses	Coalition position				
	Strongly supports	**Supports**	**Neutral**	**Opposes**	**Strongly opposes**
Managers' amendment (Sens. Burr and Feinstein)—The coalition believes that CISA should pass the Senate relatively cleanly. However, Sens. Burr and Feinstein have prudently revised their bill this summer to expand its already robust privacy protections. Among other things, the managers' amendment (MA) further limits the sharing of cyber threat data to "cybersecurity purposes." The revised measure also eliminates the government's ability to use cyber threat indicators to investigate and prosecute "serious violent felonies." Taken together, these two changes put to rest any false claims that CISA is a surveillance bill. The MA also ensures that the use of defensive measures (DMs) does not allow an entity to gain unauthorized access to a computer network. The bill's writers have worked diligently to address the concerns of privacy and civil liberties organizations. The Senate should *support* the MA.		✓			
1. No. 2564 (Sen. Paul)—The coalition *strongly opposes* this amendment. It jeopardizes a core purpose of CISA, which is granting businesses legal certainty. If private entities believe that they will face frivolous lawsuits when monitoring their computer systems for malicious behavior and sharing threat data, then they are unlikely to participate in positive cyber information-sharing programs that CISA is designed to foster.					✓

Brief amendment analyses (cont.)	Coalition position				
	Strongly supports	**Supports**	**Neutral**	**Opposes**	**Strongly opposes**
2. No. 2548 (Sen. Heller)—Sen. Heller's amendment, which the coalition *opposes*, addresses a provision in CISA related to the sharing of information by the federal government. The amendment deletes the word "knows" and inserts "reasonably believes" in a key part of section 3. The coalition supports the current "knows-at-the-time-of-sharing" language in section 3 of CISA, which directs the removal of personal information from cyber threat indicators (CTIs) before they are shared by federal entities with cleared individuals. The difficulty with the seemingly simple tweak in wording is that interpreting language such as "reasonably believes" and "reasonable efforts" in legislation is far from simple. It would likely create a lack of legal clarity, which is contrary to the goal of real-time information sharing. The coalition's preference is to maintain the "knows" standard in a final bill.				✓	
3. No. 2582 (Sen. Flake)—A sunset provision is unwise policy, given the scope and pace of state-sponsored attacks, and the coalition *strongly opposes* it. Including a provision in CISA that allows the key authorizations and safeguards to expire would fail to account for the substantial resources required to sustain an information-sharing program. The coalition will oppose a sunset provision in a final, House-Senate bill.					✓
4. No. 2578 (Sen. Vitter)—This amendment would enable more Senate staff to obtain security clearances. The coalition takes a *neutral* position on it.			✓		

Brief amendment analyses (cont.)	Coalition position				
	Strongly supports	**Supports**	**Neutral**	**Opposes**	**Strongly opposes**
5. No. 2579 (Sen. Vitter)—This amendment would fund a Small Business Cyber Security Operations Center for three years to be administered by the Department of Homeland Security (DHS). Many coalition members have small businesses among their members. The coalition *strongly supports* Sen. Vitter's amendment.	✓				
6. No. 2581 to S. 754 (Sen. Cotton)—The coalition *strongly supports* this important improvement to CISA, which would allow businesses to share cyber indicators with the FBI and the Secret Service with appropriate protections.	✓				
7. No. 2603 (Sen. Kirk)—Policymakers are correct in pushing back on international cybercrime, which is the focus of this amendment. The United States needs to shift the costs associated with cyberattacks to criminals in ways that are timely, legal, and proportionate. The coalition *supports* Sen. Kirk's amendment.		✓			
8. No. 2604 (Sen. Coats)—This proposal calls on DHS to study cyber threats to mobile devices and issue a report to Congress. The coalition is *neutral* on Sen. Coats' amendment.			✓		
9. No. 2631 (Sen. Gardner)—The coalition *supports* Sen. Gardner's amendment. Government entities and businesses, working in partnership, should have a menu of legal options (political, economic, diplomatic, etc.) at their disposal to push back against nefarious actors. The U.S. government needs to send a credible message to America's adversaries that cyberattacks on industry and government will not be tolerated.		✓			
10. No. 2580 (Sen. Flake)—The coalition *supports* Sen. Flake's amendment. It emphasizes that CISA would establish a genuinely voluntary information-sharing program.		✓			

Brief amendment analyses (cont.)	Coalition position				
	Strongly supports	**Supports**	**Neutral**	**Opposes**	**Strongly opposes**
11. No. 2627 to S. 754 (Sen. Carper et al.)—Sen. Carper's bipartisan amendment, titled the bipartisan Federal Cybersecurity Enhancement Act of 2015 (the act), focuses on improving the security of federal information networks and systems. The coalition takes a relatively *neutral* stance on the amendment. Coalition members that are engaged in DHS' EINSTEIN system support the act. At the same time, some public and private entities have raised concerns that provisions in the act could negatively impact the wider business community beyond those involved with EINSTEIN. Principally, critics of the act argue that the National Institute of Standards and Technology (NIST) should be setting cybersecurity standards, guidance, and best practices rather than DHS.			✓		
12. No. 2552 (Sen. Coons)—This amendment would attempt to address the "second scrub" issue by requiring DHS to perform another scrub of cyber threat data for personal information before disseminating indicators to appropriate federal entities. The coalition *opposes* Sen. Coons' amendment. Granting authority to DHS to conduct a second scrub is not inherently bad if viewed only through the vague lens of "privacy." But privacy is just one of several considerations in CISA. For example, when one recognizes that CTIs rarely if ever contain personal information, the second scrub would bog down the sharing of CTIs from businesses to the federal entities that need them in a timely manner.				✓	

Brief amendment analyses (cont.)	Coalition position				
	Strongly supports	**Supports**	**Neutral**	**Opposes**	**Strongly opposes**
13. No. 2612 (Sen. Franken)—This amendment would change the definitions of "cybersecurity threat" and CTIs. It narrows what constitutes a cyber threat to "is reasonably likely to result in an unauthorized effort to adversely impact" an information system's security from "may result in an unauthorized effort to adversely impact" an information system's security. The amendment changes a part of the definition of CTIs to "the harm caused by an incident" from "the actual or potential harm caused by an incident." The coalition *strongly opposes* this amendment. Both changes would likely result in extended litigation over the meanings of cyber threats and CTIs. CISA is supposed to do the exact opposite.					✓
14. No. 2632 (Sen. Tester)—Sen. Tester's amendment would add at least eight reporting requirements to CISA's *Biennial Report on Implementation*, which is to be written by the heads and the inspectors general of certain agencies and departments. The coalition is *neutral* on Sen. Tester's amendment. Still, while we do not argue with the amendment's goal of achieving greater oversight of CISA, the granular reporting of cyber threat data could dissuade or intimidate some businesses from participating in information-sharing programs.			✓		
15. No. 2587 (Sen. Leahy)—The managers' amendment strikes one of two pillars of CISA that would grant a new Freedom of Information Action (FOIA) exemption under the bill. As problematic as this change is, information shared under CISA would still be exempt from disclosure, including under existing FOIA exemptions. However, Sen. Leahy's amendment would seemingly eliminate businesses' appeals to any existing FOIA protections when sharing CTIs and DMs with the federal government. The coalition *strongly opposes* eliminating the protection from public disclosure.					✓

Brief amendment analyses (cont.)	Coalition position				
	Strongly supports	**Supports**	**Neutral**	**Opposes**	**Strongly opposes**
16. No. 2589 (Sen. Murphy)—This amendment, which is supported by the administration and many industry organizations, would extend the Federal Privacy Act to citizens in other "covered countries." The coalition *supports* it.		✓			
17. No. 2626 (Sen. Whitehouse)—Sen. Whitehouse's amendment includes provisions to (1) strengthen U.S. laws prohibiting the sale of Americans' financial information, (2) expand the Department of Justice's (DOJ's) authority to shut down botnets, (3) boost penalties for damaging critical infrastructure computers, and (4) increase penalties for trafficking in passwords. The coalition *supports* this amendment. Malicious organizations perpetrating cybercrime do not fear attribution, extradition, and prosecution to the degree that it seriously impacts their cost/benefit calculations. This amendment would help tip the scales of justice more toward American law enforcement and industry.		✓			
18. No. 2621 (Sen. Wyden)—Sen. Wyden's amendment would eliminate the language "knows at the time of sharing," which pertains to private entities' removal of personal information in cyber indicators that is "not directly related to a cybersecurity threat." The coalition *strongly opposes* the amendment. If adopted, the amendment would give rise to added legal ambiguity. It would act as a disincentive to share—including sharing in a timely manner—which cuts against the grain of the bill. The coalition will push to maintain the "knows" standard in a final bill.					✓

Brief amendment analyses (cont.)	Coalition position				
	Strongly supports	**Supports**	**Neutral**	**Opposes**	**Strongly opposes**
19. No. 2622 (Sen. Wyden)—This amendment would add to the numerous requirements placed on the federal government to facilitate the sharing of cyber threat information and guard individual's privacy and civil liberties. The amendment requires the government to notify in a timely manner any person whose information is shared in contravention of CISA, which is not an issue on the surface. However, the coalition *opposes* this amendment for three reasons: First, this amendment would slow down, if not halt, government-to-businesses information sharing. Second, the amendment suggests that harms would be done to individuals whose personal data are unintentionally shared—and such negative outcomes are unclear. Third, the amendment perpetuates a myth that shared cyber threat information is broad in scope. In fact, CISA's definition of CTIs is very limited.				✓	
20. No. 2557 (Sen. Mikulski)—This amendment would appropriate $37M until September 30, 2017, related to the Office of Personnel Management (OPM) hacking incident. The coalition is *neutral* on the proposal.			✓		
21. No. 2615 (Sen. Carper)—Sen. Carper's amendment pertains to the sharing of CTIs first through the DHS portal, and then the indicators are disseminated to other federal entities. The coalition is relatively neutral on this amendment. The word "unnecessary" describes any potential modifications (e.g., scrubbing personal information) to CTIs before sharing them with other federal entities. However, in most instances, it should not be necessary to scrub cyber indicators of personal information, which the amendment seems to recognize.			✓		
Total (22)	2	6	6	3	5

CISA is smart, compromise legislation that needs to be passed this fall

The Protecting America's Cyber Networks Coalition (the coalition) urges the Senate to take up and pass S. 754, the Cybersecurity Information Sharing Act of 2015 (CISA), as soon as possible. Cyber risks to U.S. interests—including the government, industry, households, and individuals—are by most accounts steadily increasing, not waning. Some of the most virulent attacks are originating from foreign states or their proxies and sophisticated criminals, whose conduct is tethered neither to emerging cyber norms nor the rule of law.

Given the scope and sophistication of malicious cyber behavior, the private sector is supplying security against nation-states and other hostile actors in a manner that has traditionally been supplied by government bodies at all levels. The coalition, which represents leading associations of nearly every sector of the America economy, strongly backs CISA so that businesses can better defend themselves and their customers. Industry has a legitimate right to self-defense, which is why we believe that most policymakers support the bill.

The legislation benefits from widespread bipartisan backing. In March, the Senate Intelligence Committee approved CISA by a vote of 14 to 1. In April, the House passed two cybersecurity information-sharing 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. The coalition welcomes that the White House has signaled its support for S. 754.

There is little dispute that cybersecurity information-sharing legislation should be enacted—and swiftly. Still, the form that it takes is the focal point of the Senate's debate over CISA. The coalition believes that the bill should be passed, as reported, relatively cleanly. However, Sens. Burr and Feinstein, the authors of CISA, have prudently revised their bill this summer to expand its already robust privacy protections, which the coalition accepts. Among other things, the managers' amendment further limits the sharing of cyber threat data to "cybersecurity purposes."

Closely related, the revised measure eliminates the government's ability to use cyber threat indicators to investigate and prosecute "serious violent felonies." Taken together, these two changes put to rest any false claims that CISA is a surveillance bill. The managers' amendment also ensures that the use of defensive measures does not allow an entity to gain unauthorized access to a computer network. The bill's writers have worked diligently to address the concerns of privacy and civil liberties organizations. Amending CISA further in the name of "privacy" would only weaken its effectiveness against U.S. adversaries and the attraction of threat-sharing programs to businesses.

Our organizations believe that Congress needs to send a bill to the president that gives businesses legal certainty that they have safe harbor against frivolous lawsuits when voluntarily sharing and receiving threat indicators and defensive measures in real time and taking actions to mitigate cyberattacks. The legislation also needs to offer protections related to public disclosure, regulatory, and antitrust matters in order to increase the timely exchange of information among public and private entities. CISA reflects sound compromises among many stakeholders on these issues.

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 Coatings Association
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)
Association of Metropolitan Water Agencies (AMWA)
BITS–Financial Services Roundtable
College of Healthcare Information Management Executives (CHIME)
CompTIA–The Computing Technology Industry Association
CTIA–The Wireless Association
Edison Electric Institute (EEI)
Electronic Payments Coalition (EPC)
Electronic Transactions Association (ETA)
Federation of American Hospitals (FAH)
Food Marketing Institute (FMI)
Global Automakers
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 Retail Federation (NRF)
National Rural Electric Cooperative Association (NRECA)
NTCA–The Rural Broadband Association
Property Casualty Insurers Association of America (PCI)
The Real Estate Roundtable
Retail Industry Leaders Association (RILA)
Security Industry Association
Software & Information Industry Association (SIIA)
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)

***

1. Floor amendment No. 2564 to S. 754 (Sen. Paul)—Strongly oppose

Analysis and position

- **Analysis:** Sen. Paul's amendment jeopardizes a core purpose of CISA. The bill was created to counter cyberattacks against the United States by protecting businesses as they monitor their networks for malicious behavior and share cybersecurity data. Companies' security and technical professionals need legal clarity to swiftly counter attacks—in other words, to quickly improvise and match the speeds at which bad actors are attacking their networks.

  Businesses go to great lengths and spend countless sums to safeguard the sensitive information (e.g., consumer data) that they maintain on their systems. It is in their overriding interest to do so. Under CISA as reported, a business is authorized to monitor its networks and share threat data "notwithstanding any other provision of law" with peers in industry and government partners, which is critical to making the legislation effective (section 4).

  However, if a private entity inadvertently violates a user agreement or a privacy notice (legally prescribed obligations) while monitoring or sharing, the protection from liability afforded to businesses disappears. The amendment, which could trigger the negation of liability protections for relatively trivial matters is out of step with the purpose of the bill.

  There are four key protections in CISA that are afforded to businesses. Such safeguards are linked to limited liability, regulatory, public disclosure, and antitrust matters. The protection from liability rises to the top one for most companies.

- **Coalition position:** The coalition strongly urges the Senate to oppose Sen. Paul's amendment. Businesses need legal certainty. If private entities believe that they will face frivolous lawsuits when monitoring their computer systems and sharing threat data, then they are unlikely to participate in positive cyber information-sharing programs that CISA is designed to foster.

Text of the amendment

SA 2564. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 38, line between lines 19 and 20, insert the following:
(d) Exception.—This section shall not apply to any private entity that, in the course of monitoring information under section 4(a) or sharing information under section 4(c), breaks a user agreement or privacy agreement with a customer of the private entity.

2. Floor Amendment No. 2548 to S. 754 (Sen. Heller)—Oppose

Analysis and position

- **Analysis:** Sen. Heller's amendment addresses a provision in CISA related to the sharing of information by the federal government. The amendment deletes the word "knows" and inserts "reasonably believes" before "at the time of sharing . . ." under section 3(b)(1)(E)(i) of the bill.

- **Coalition position:** The coalition opposes Sen. Heller's amendment for much the same reason that we oppose a comparable amendment being offered by Sen. Wyden (No. 2621), which centers on business-to-government sharing.

  The coalition supports the current "knows-at-the-time-of-sharing" language in section 3 of CISA, as reported, which directs the removal of personal information from cyber threat indicators (CTIs) before they are shared by federal entities with cleared representatives in the public and private sectors. The text was carefully negotiated over a lengthy period of time among stakeholders.

  The difficulty with the seemingly simple tweak in wording is that interpreting language such as "reasonably believes" and "reasonable efforts" in legislation is far from simple. It would create legal uncertainty and is contrary to the goal of real-time information sharing. The coalition will press lawmakers to maintain the "knows" standard in a final bill.

Text of the amendment

SA 2548. Mr. HELLER submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 11 [of the managers' amendment, labeled EAS15A35], line 22, strike "knows" and insert "reasonably believes".

3. Floor Amendment No. 2582 to S. 754 (Sen. Flake)—Strongly oppose

Analysis and position

- **Analysis:** A sunset provision would imperil businesses' security and resilience if threat-sharing systems are turned off because of lapsed authorizations and related safeguards, such as liability protection. Companies cannot easily turn on their information-sharing infrastructures like a light switch. The time, logistics, and costs associated with establishing an information-sharing program are significant.

A sunset provision would almost certainly inhibit businesses' ability to make long-term planning decisions related to risk management and information-sharing investments—which policymakers should want businesses to regularly undertake.

Coalition members opposed similar sunset amendments to House cybersecurity legislation—H.R. 1560, the Protecting Cyber Networks Act, and H.R. 1731, the National Cybersecurity Protection Advancement Act of 2015.

- **Coalition position:** Given the persistence and speed of cyberattacks, a sunset provision is unwise policy, and the coalition opposes it. Including a provision in CISA that allows the key authorizations and safeguards to expire would fail to account for the substantial resources required to sustain an information-sharing program. The coalition strongly opposes including a sunset provision in a final House-Senate bill.

Text of the amendment

SA 2582. Mr. FLAKE (for himself and Mr. FRANKEN) submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the end, add the following:
SEC. 11. EFFECTIVE PERIOD.
(a) In General.—Except as provided in subsection (b), this Act and the amendments made by this Act shall be in effect during the 6-year period beginning on the date of the enactment of this Act.
(b) Exception.—With respect to any action authorized by this Act or information obtained pursuant to an action authorized by this Act, which occurred before the date on which the provisions referred to in subsection (a) cease to have effect, the provisions of this Act shall continue in effect.

4. Floor Amendment No. 2578 to S. 754 (Sen. Vitter)—Neutral

Analysis and position

- **Analysis:** This amendment by Sen. Vitter seems designed to spur a review of the adequacy of the guidance used by U.S. government officials for clearing Senate staff. All things considered, ensuring that appropriate Senate staff members have access to classified information related to U.S. cybersecurity interests is a good idea.

- **Coalition position:** The coalition is neutral on Sen. Vitter's security clearance amendment (No. 2578).

Text of the amendment

SA 2578. Mr. VITTER (for himself and Mr. TESTER) submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through

enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. __X. REVIEW AND UPDATE OF GUIDANCE REGARDING SECURITY CLEARANCES FOR CERTAIN SENATE EMPLOYEES.

(a) *Definitions*.—In this section—

(1) the term "covered committee of the Senate" means—

(A) the Committee on Armed Services of the Senate;

(B) the Committee on Foreign Relations of the Senate;

(C) the Subcommittee on Defense of the Committee on Appropriations of the Senate;

(D) the Subcommittee on State, Foreign Operations, and Related Programs of the Committee on Appropriations of the Senate;

(E) the Committee on Homeland Security and Governmental Affairs of the Senate; and

(F) the Committee on the Judiciary of the Senate;

(2) the term "covered Member of the Senate" means a Member of the Senate who serves on a covered committee of the Senate; and

(3) the term "Senate employee" means an employee whose pay is disbursed by the Secretary of the Senate.

(b) *Review of Procedures*.—

(1) **IN GENERAL**.—Not later than 60 days after the date of enactment of this Act, the Director of Senate Security, in coordination with the Director of National Intelligence and the Chairperson of the Suitability and Security Clearance Performance Accountability Council established under Executive Order 13467 (73 Fed. Reg. 38103), shall—

(A) conduct a review of whether procedures in effect enable 1 Senate employee designated by each covered Member of the Senate to obtain security clearances necessary for access to classified national security information, including top secret and sensitive compartmentalized information, if the Senate employee meets the criteria for such clearances; and

(B) if the Director of Senate Security, in coordination with the Director of National Intelligence and the Chairperson of the Suitability and Security Clearance Performance Accountability Council established under Executive Order 13467 (73 Fed. Reg. 38103), determines the procedures described in subparagraph (A) are inadequate, issue guidelines on the establishment and implementation of such procedures.

(2) **REPORT**.—Not later than 90 days after the date of enactment of this Act, the Director of Senate Security shall submit to each covered committee of the Senate a report regarding the review conducted under paragraph (1)(A) and guidance, if any, issued under paragraph (1)(B).

(c) *Rule of Construction*.—Nothing in this section shall be construed to alter—

(1) the rule of the Information Security Oversight Office implementing Standard Form 312, which Members of Congress sign in order to be permitted to access classified information;

(2) the requirement that Members of the Senate satisfy the "need-to-know" requirement to access classified information;

(3) the scope of the jurisdiction of any committee or subcommittee of the Senate; or

(4) the inherent authority of the executive branch of the Government, the Office of Senate Security, any Committee of the Senate, or the Department of Defense to determine recipients of all classified information.

5. Floor Amendment No. 2579 to S. 754 (Sen. Vitter)—Strongly support

Analysis and position

- **Analysis:** Sen. Vitter's second amendment would fund the Department of Homeland Security (DHS) to establish a Small Business Cyber Security Operations Center as part of the three-year pilot program dedicated to strengthening small businesses' cybersecurity.

  If this amendment becomes part of CISA, policymakers should consider revising the language to enable large firms to work with businesses, especially small and midsize businesses, in their supply chains to manage cyber risks, which is an ongoing, expensive, and time-consuming undertaking.

- **Coalition position:** The coalition strongly supports Sen. Vitter's amendment (No. 2579).

Text of the amendment

SA 2579. Mr. VITTER submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:
SEC. __X. SMALL BUSINESS CYBER SECURITY OPERATIONS CENTER.
(a) *Findings*.—Congress finds the following:
(1) The Federal Government has been hit by a barrage of high-profile cyber assaults over the past year, including the attacks on the Office of Personnel Management and the Department of State.
(2) These attacks exposed the most sensitive personal information of millions of Federal employees and their families.
(3) The President has instituted emergency procedures to immediately deploy so-called indicators, or tell-tale signs of cybercrime operations, into agency anti-malware tools.
(4) According to the Federal Bureau of Investigation, small business concerns have lost more than $1,000,000,000 during the period beginning October 2013 and ending June 2015 as a result of cyber corporate account takeover and business email fraud.
(5) The Federal Government leverages the creative genius of small business concerns across the country to accomplish its missions.
(6) The Federal Acquisition Regulations dictates that a percentage of all Federal Government acquisition be set aside for small business concerns.
(7) Over 90 percent of small business concerns use the Internet through the course of their activities to conduct business.
(8) Small business concerns tend to have weaker online security and do not have necessary funding for high-end encryption technology or staff expertise.
(9) Industry reports indicate that 30 percent of cyber attacks target small business concerns and of those businesses that are attacked, 59 percent have no contingency plan, while according to a First Data report, the average cost for a data breach at a small business concern is $36,000 and rising annually.
(10) A 2012 Verizon study shows that in 855 data breaches examined, 71 percent occurred in

businesses with fewer than 100 employees.
(11) Small business concerns are increasingly attacked with data breaches and ransomware, where an attacker encrypts the businesses data until a ransom is paid to the attacker.
(12) It is imperative that small business concerns are provided improved secured guidance to limit negative impacts on the economy of the United States.
(13) There is a vast cyber threat facing the business sector of the United States, which poses a direct threat against the national security of the United States, the Department of Defense, private industry, and critical infrastructure components.
(14) The current layer of protection from cyber threats does not exist for small business concerns.
(b) *Definitions*.—In this section—
(1) the term "Center" means the Small Business Cyber Security Operations Center established under subsection (c);
(2) the term "cyber lab" means—
(A) a Joint Cyber Training Lab; and
(B) a facility that works in conjunction with the National Guard Cyber Teams;
(3) the term "Secretary" means the Secretary of Homeland Security; and
(4) the term "small business concern" has the meaning given that term under section 3 of the Small Business Act (15 U.S.C. 632).
(c) *Establishment*.—Not later than 1 year after the date of enactment of this Act, the Secretary shall begin carrying out a 3-year pilot program to establish a cybersecurity operations center for small business concerns, to be known as the Small Business Cyber Security Operations Center.
(d) *Part of Existing Center*.—The Secretary shall establish the Center as part of and co-locate the Center with a center providing situational awareness information to businesses on the date of enactment of this Act.
(e) *Duties*.—The Center shall—
(1) work with cyber labs to provide realistic scenario based training to network managers and security personnel of small business concerns, including monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities;
(2) provide periodic sharing, through publication and targeted outreach, of cybersecurity best practices that are developed based on ongoing analysis of cyber threat indicators and information in possession of—
(A) the Federal Government;
(B) the Business Emergency Operations Center operated by the Federal Emergency Management Agency; and
(C) other technology and cyber research centers, as determined appropriate by the Secretary;
(3) collaborate with private industry, academia, and the Department of Defense to develop a secure business supply chain which is capable of adapting, evolving, and responding to emergent cybersecurity threats;
(4) review and develop the necessary tools to—
(A) facilitate security information flow and mitigation actions;
(B) provide cyber attack sensing, warning, and response services;
(5) place an emphasis on accessibility and relevance to small business concerns; and
(6) review the policy limitations and restrictions on information sharing relating to cybersecurity.
(f) *Authorization of Appropriations*.—
(1) **IN GENERAL**.—There is authorized to be appropriated to carry out this section $2,000,000 for each of fiscal years 2016 through 2019, to remain available until expended.

(2) **OFFSET**.—Section 21(a)(4)(C)(vii) of the Small Business Act (15 U.S.C. 648(a)(4)(C)(vii)) is amended—
(A) in subclause (I), by striking "and" at the end;
(B) in subclause (II), by striking the period at the end and inserting "; and"; and
(C) by adding at the end the following:
"(III) $133,000,000 for each of fiscal years 2016 through 2019.".

6. Floor Amendment No. 2581 to S. 754 (Sen. Cotton)—Strongly support

Analysis and position

- **Analysis:** Legislation needs to protect businesses that share cyber threat indicators (CTIs) and defensive measures (DMs) both with private entities and with appropriate federal agencies and departments authorized in CISA. Such entities include the departments of Commerce, Energy, Homeland Security, Justice, Treasury, and the Office of the Director of National Intelligence. Notably, House legislation (H.R. 1560, the Protecting Cyber Networks Act) that follows this approach precisely passed in April by a vote of 307 to 116.

  Coalition members believe that DHS—or any federal entity for that matter—should not be the sole civilian and protected entity to receive cyber threat data. After all, with the recent creation of the Cyber Threat Intelligence Integration Center (CTIIC), which is meant to connect the cyber dots among various federal departments and agencies, it makes little sense to establish in law that DHS would be the only recipient of protected cyber threat information coming from the private sector.

  CISA does not protect businesses that share CTIs and DMs directly with the Department of Defense (DoD), including the National Security Agency (NSA). This aspect of CISA represents a nod to the politics of cyber information sharing, and it makes little sense from a policy or security standpoint.

  Despite the disincentive to share with DoD and NSA, the coalition assumes that policymakers will make every effort to access, analyze, and disseminate cyber threat data to public and private entities and not leave the data in a compartmentalized channel, whether located at DHS, the FBI, or another government entity.

Coalition position: The coalition strongly supports the adoption of Sen. Cotton's amendment.

Text of the amendment

SA 2581. Mr. COTTON submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 29, strike line 9 and insert the following:

authority regarding a cybersecurity threat; and (iii) communications between a private entity and the Federal Bureau of Investigation or the United States Secret Service regarding a cybersecurity threat;

7. Floor Amendment No. 2603 to S. 754 (Sen. Kirk)—Support

Analysis and position

- **Analysis:** This amendment dovetails with coalition members' increasing engagement of law enforcement to confront cyber attackers. Businesses are building trusted relationships with the FBI and the Secret Service, which are essential to confirming a cybercrime and beginning criminal investigations. The coalition urges its members to partner with law enforcement before, during, and after a cyber incident.

  Coalition members have supported closely related legislation in the past (e.g., S. 1469, the International Cybercrime Reporting and Cooperation Act from the 112th Congress), which would provide the United States with more tools to strengthen other countries' ability to develop their cybersecurity policies and fight cybercrime.

- **Coalition position:** The coalition supports this amendment. We believe that the United States needs to coherently shift the costs associated with cyberattacks to criminals in ways that are timely, legal, and proportionate. Policymakers need to help the law enforcement community, which is a key asset of the business community, but numerically overmatched compared to hackers.

Text of the amendment

SA 2603. Mr. KIRK (for himself and Mrs. GILLIBRAND) submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:
SEC. __. APPREHENSION AND PROSECUTION OF INTERNATIONAL CYBER CRIMINALS.
(a) *International Cyber Criminal Defined*.—In this section, the term "international cyber criminal"' means an individual—
(1) who is physically present within a country with which the United States does not have a mutual legal assistance treaty or an extradition treaty;
(2) who is believed to have committed a cybercrime or intellectual property crime against the interests of the United States or its citizens; and
(3) for whom—
(A) an arrest warrant has been issued by a judge in the United States; or
(B) an international wanted notice (commonly referred to as a "Red Notice") has been circulated by Interpol.
(b) *Bilateral Consultations*.—The Secretary of State, or designee, shall consult with the appropriate government official of each country in which one or more international cyber

criminals are physically present to determine what actions the government of such country has taken—
(1) to apprehend and prosecute such criminals; and
(2) to prevent such criminals from carrying out cybercrimes or intellectual property crimes against the interests of the United States or its citizens.
(c) *Annual Report*.—
(1) **IN GENERAL**.—The Secretary of State shall submit to the appropriate congressional committees an annual report that identifies—
(A) the number of international cyber criminals who are located in countries that do not have an extradition treaty or mutual legal assistance treaty with the United States, broken down by country;
(B) the dates on which an official of the Department of State, as a result of this Act, discussed ways to thwart or prosecute international cyber criminals in a bilateral conversation with an official of another country, including the name of each such country; and
(C) for each international cyber criminal who was extradited into the United States during the most recently completed calendar year—
(i) his or her name;
(ii) the crimes for which he or she was charged;
(iii) his or her previous country of residence; and
(iv) the country from which he or she was extradited into the United States.
(2) **APPROPRIATE CONGRESSIONAL COMMITTEES**.—For purposes of this subsection, the term "appropriate congressional committees" means—
(A) the Committee on Foreign Relations of the Senate;
(B) the Committee on Appropriations of the Senate;
(C) the Committee on Homeland Security and Governmental Affairs of the Senate;
(D) the Committee on Banking, Housing, and Urban Affairs of the Senate;
(E) the Committee on Foreign Affairs of the House of Representatives;
(F) the Committee on Appropriations of the House of Representatives;
(G) the Committee on Homeland Security of the House of Representatives; and
(H) the Committee on Financial Services of the House of Representatives.

8. Floor Amendment No. 2604 to S. 754 (Sen. Coats)—Neutral

Analysis and position

- **Analysis:** Mobile technology has dramatically changed where and how people work and communicate with colleagues and friends. Increasing the security and resilience of mobile platforms would benefit the government and the private sector.

  Sen. Coats' amendment would likely complement the work being done by federal entities such as DHS' Science and Technology Directorate, which administers the department's Mobile Device Security program.

  This initiative apparently focuses on developing technologies in the area of security and privacy for the adoption of secure mobile technologies throughout the marketplace. Also, the National Institute of Standards and Technology has crafted guidelines for managing

the security of mobile devices in enterprise settings.

- **Coalition position:** The coalition is neutral on Sen. Coats' amendment.

Text of the amendment

SA 2604. Mr. COATS submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 51, strike line 8 and insert the following:
SEC. 10. STUDY ON CYBERSECURITY THREATS TO MOBILE DEVICES.
(a) In General.—Not later than 1 year after the date of the enactment of this Act, the Secretary of Homeland Security shall—
(1) complete a study on cybersecurity threats relating to mobile devices; and
(2) submit a report to Congress that contains the findings of such study and the recommendations developed under subsection (b)(3).
(b) Matters Studied.—In carrying out the study under subsection (a)(1), the Secretary shall—
(1) assess cybersecurity threats relating to mobile devices;
(2) assess the effect such threats may have on the cyber security of the information systems and networks of the Federal Government (except for the information systems and networks of the Department of Defense and the Intelligence Community); and
(3) develop recommendations for addressing such threats.
SEC. 11. CONFORMING AMENDMENTS.

9. Floor Amendment No. 2631 to S. 754 (Sen. Gardner)—Support

Analysis and position

- **Analysis:** Sen. Gardner's amendment calls on the Department of State to produce a comprehensive strategy relating to U.S. international cyber policies.

  The strategy would involve reviewing (1) activities undertaken by the secretary of state to support the goal of the *International Strategy for Cyberspace*, (2) actions to guide the U.S. diplomacy with our allies and adversaries, (3) the state of play regarding international norms in cyberspace, and (4) policy tools available to the administration to deter foreign powers and criminals that launch cyberattacks against America.

- **Coalition position:** The coalition supports the amendment. Government entities and businesses, working in partnership, should have a menu of legal options (political, economic, diplomatic, etc.) at their disposal to push back against nefarious actors. The U.S. government needs to send a credible message to America's adversaries that cyberattacks on industry and government will not be tolerated.

  The coalition believes that the National Institute of Standards and Technology's (NIST's)

Framework for Improving Critical Infrastructure Cybersecurity (the framework) is a useful tool to help businesses strengthen their cybersecurity. However, much more must be done to give businesses and government the policy instruments necessary to adequately increase costs on malicious cyber activity.

Despite the existence of written blueprints, such as ones related to global prosperity and defense, the United States' overarching cybersecurity strategy is uncertain—both to many in the private sector and our adversaries alike. The coalition believes that the United States needs to refocus national efforts toward heightening the costs on sophisticated attackers that willfully hack America's private sector for illicit purposes.

Coalition members agree with an essential aim of Sen. Gardner's amendment, which is that public- and private-sector stakeholders need to conduct a review of actions (e.g., improved cyber defenses and enhanced attribution capabilities) that can be prudently taken by business and government to deter bad actors.

There is a gulf between a major cyber armed conflict—which we have yet to see—and the more frequent, relatively minor attacks launched by unskilled actors that many businesses can mitigate on their own.

However, in the widening middle are costly attacks against U.S. businesses (e.g., cybercrime and intellectual property theft) that are linked to sophisticated criminal groups and foreign powers or their surrogates. This is one area where deterrence policy and international norms are especially needed.

Text of the amendment

SA 2631. Mr. GARDNER (for himself and Mr. CARDIN) submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. __X. DEPARTMENT OF STATE INTERNATIONAL CYBERSPACE POLICY STRATEGY.

(a) *In General*.—Not later than 90 days after the date of the enactment of this Act, the Secretary of State shall produce a comprehensive strategy relating to United States international policy with regard to cyberspace.

(b) *Elements*.—The strategy required by subsection (a) shall include the following:

(1) A review of actions and activities undertaken by the Secretary of State to date to support the goal of the President's International Strategy for Cyberspace, released in May 2011, to "work internationally to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation.".

(2) A plan of action to guide the diplomacy of the Secretary of State, with regard to foreign countries, including conducting bilateral and multilateral activities to develop the norms of responsible international behavior in cyberspace, and status review of existing discussions in

multilateral fora to obtain agreements on international norms in cyberspace.
(3) A review of the alternative concepts with regard to international norms in cyberspace offered by foreign countries that are prominent actors, including China, Russia, Brazil, and India.
(4) A detailed description of threats to United States national security in cyberspace from foreign countries, state-sponsored actors, and private actors to Federal and private sector infrastructure of the United States, intellectual property in the United States, and the privacy of citizens of the United States.
(5) A review of policy tools available to the President to deter foreign countries, state-sponsored actors, and private actors, including those outlined in Executive Order 13694, released on April 1, 2015.
(6) A review of resources required by the Secretary, including the Office of the Coordinator for Cyber Issues, to conduct activities to build responsible norms of international cyber behavior.
(c) *Consultation*.—In preparing the strategy required by subsection (a), the Secretary of State shall consult, as appropriate, with other agencies and departments of the United States and the private sector and nongovernmental organizations in the United States with recognized credentials and expertise in foreign policy, national security, and cybersecurity.
(d) *Form of Strategy*.—The strategy required by subsection (a) shall be in unclassified form, but may include a classified annex.
(e) *Availability of Information*.—The Secretary of State shall—
(1) make the strategy required in subsection (a) available the public; and
(2) brief the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives on the strategy, including any material contained in a classified annex.

10. Floor Amendment No. 2580 to S. 754 (Sen. Flake)—Support

Analysis and position

- **Analysis:** The coalition believes that cybersecurity incident reporting is most powerful when government and industry collaborate. Public policies that attempt to compel private sector enterprises to report cybersecurity incidents often unintentionally lead to less—not more—information sharing compared with architectures that are dynamic and collaborative in nature.

  Information-sharing initiatives that foster cooperative environments, and which are rooted in trust and legal safeguards, deliver more effective risk mitigation strategies.

- **Coalition position:** The coalition supports Sen. Flake's amendment, which emphasizes the fact that CISA would establish a genuinely voluntary information-sharing program; the Senate should support it.

Text of the amendment

SA 2580. Mr. FLAKE submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

Beginning on page 46, strike line 10 and all that follows through page 47, line 12, and insert the following:
(3) to require a new information sharing relationship between any entity and the Federal Government or another entity; or
(4) to require the use of the capability and process within the Department of Homeland Security developed under section 5(c).
(g) *Preservation of Contractual Obligations and Rights*.—Nothing in this Act shall be construed—
(1) to amend, repeal, or supersede any current or future contractual agreement, terms of service agreement, or other contractual relationship between any entities, or between any entity and a Federal entity; or
(2) to abrogate trade secret or intellectual property rights of any entity or Federal entity.
(h) *Anti-Tasking Restriction*.—Nothing in this Act shall be construed to permit the Federal Government—
(1) to require an entity to provide information to the Federal Government or anther entity;
(2) to condition the sharing of cyber threat indicators with an entity on such entity's provision of cyber threat indicators to the Federal Government or another entity; or
(3) to condition the award of any Federal grant, contract, or purchase on the provision of a cyber threat indicator to a Federal entity or another entity.

11. Floor Amendment No. 2627 to S. 754 (Sen. Carper)—Neutral, with qualifications

Analysis and position

- **Analysis:** Sen. Carper's bipartisan amendment, titled the bipartisan Federal Cybersecurity Enhancement Act of 2015 (the act), focuses on improving the security of federal information networks and systems. But section 203 of the act allows DHS to enter into contracts and related agreements with private entities to deploy and operate technologies both to detect cyber risks on agencies' computer systems and remove them.

  Private contractors may not disclose any network traffic without the consent of DHS or an agency. Private vendors are also prohibited from using any of the network traffic for purposes other than to protect government information systems against malicious cyber activity or to implement a contract with DHS.

  The act provides liability protection to private contractors. A rule of construction says that nothing related to the limitation on liability authorizes an Internet service provider from breaking a user agreement without the consent of the customer. (Select provisions

specific to private contractors are highlighted in green below.)

- **Coalition position:** The coalition takes a relatively neutral stance on the amendment/act and offers further points for lawmakers' consideration. Coalition members that are engaged in DHS' EINSTEIN system, which is meant to create a governmentwide defense mechanism around agency networks, support the act. At the same time, concerns have been raised by some public and private entities that provisions in the act could negatively impact the wider business community beyond those involved with EINSTEIN.

  Principally, critics of the act argue that the National Institute of Standards and Technology (NIST) should be setting cybersecurity standards, guidance, and best practices rather than DHS.

  The act is designed to stop the next Office of Personnel Management (OPM)-like breach through vigorous government actions. Yet the act seems to blur the roles of NIST and DHS, such as when the department is authorized to issue binding directives to agencies under sections 205 and 209. This outcome does not appear to be the intent of the amendment's writers. However, industry believes that DHS' role in determining cybersecurity standards, especially vis-à-vis the private sector, needs to be bounded.

  Also, some of the technical mandates in section 205 may be too specific and could become rapidly outdated. Technically explicit mandates should generally not be written into law. The coalition agrees with these views.

Text of the amendment

SA 2627. Mr. CARPER (for himself, Mr. JOHNSON, Ms. AYOTTE, Mrs. MCCASKILL, Ms. COLLINS, and Mr. WARNER) submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the end, add the following:

TITLE II—FEDERAL CYBERSECURITY ENHANCEMENT ACT
SECTION 201. SHORT TITLE.
This title may be cited as the "Federal Cybersecurity Enhancement Act of 2015".
SEC. 202. DEFINITIONS.
In this title—
(1) the term "agency" has the meaning given the term in section 3502 of title 44, United States Code;
(2) the term "agency information system" has the meaning given the term in section 228 of the Homeland Security Act of 2002, as added by section 203(a);
(3) the term "appropriate congressional committees" means—
(A) the Committee on Homeland Security and Governmental Affairs of the Senate; and
(B) the Committee on Homeland Security of the House of Representatives;
(4) the terms "cybersecurity risk" and "information system" have the meanings given those terms

in section 227 of the Homeland Security Act of 2002, as so redesignated by section 203(a);
(5) the term “Director” means the Director of the Office of Management and Budget;
(6) the term “intelligence community” has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)); and
(7) the term “Secretary” means the Secretary of Homeland Security.

SEC. 203. IMPROVED FEDERAL NETWORK SECURITY.

(a) *In General*.—Subtitle C of title II of the Homeland Security Act of 2002 (6 U.S.C. 141 et seq.) is amended—
(1) by redesignating section 228 as section 229;
(2) by redesignating section 227 as subsection (c) of section 228, as added by paragraph (4), and adjusting the margins accordingly;
(3) by redesignating the second section designated as section 226 (relating to the national cybersecurity and communications integration center) as section 227;
(4) by inserting after section 227, as so redesignated, the following:

“SEC. 228. CYBERSECURITY PLANS.

“(a) *Definitions*.—In this section—
“(1) the term ‘agency information system' means an information system used or operated by an agency or by another entity on behalf of an agency;
“(2) the terms ‘cybersecurity risk' and ‘information system' have the meanings given those terms in section 227;
“(3) the term ‘information sharing and analysis organization' has the meaning given the term in section 212(5); and
“(4) the term ‘intelligence community' has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).
“(b) *Intrusion Assessment Plan*.—
“(1) **REQUIREMENT**.—The Secretary, in coordination with the Director of the Office of Management and Budget, shall develop and implement an intrusion assessment plan to identify and remove intruders in agency information systems.
“(2) **EXCEPTION**.—The intrusion assessment plan required under paragraph (1) shall not apply to the Department of Defense or an element of the intelligence community.”;
(5) in section 228(c), as so redesignated, by striking “section 226” and inserting “section 227”; and
(6) by inserting after section 229, as so redesignated, the following:

“SEC. 230. FEDERAL INTRUSION DETECTION AND PREVENTION SYSTEM.

“(a) *Definitions*.—In this section—
“(1) the term ‘agency' has the meaning given that term in section 3502 of title 44, United States Code;
“(2) the term ‘agency information' means information collected or maintained by or on behalf of an agency;
“(3) the term ‘agency information system' has the meaning given the term in section 228; and
“(4) the terms ‘cybersecurity risk' and ‘information system' have the meanings given those terms in section 227.
“(b) *Requirement*.—
“(1) **IN GENERAL**.—Not later than 1 year after the date of enactment of this section, the Secretary shall deploy, operate, and maintain, to make available for use by any agency, with or without reimbursement—
“(A) a capability to detect cybersecurity risks in network traffic transiting or traveling to or from

an agency information system; and
“(B) a capability to prevent network traffic associated with such cybersecurity risks from transiting or traveling to or from an agency information system or modify such network traffic to remove the cybersecurity risk.
“(2) **REGULAR IMPROVEMENT**.—The Secretary shall regularly deploy new technologies and modify existing technologies to the intrusion detection and prevention capabilities described in paragraph (1) as appropriate to improve the intrusion detection and prevention capabilities.
“(c) *Activities*.—In carrying out subsection (b), the Secretary—
“(1) may access, and the head of an agency may disclose to the Secretary or a private entity providing assistance to the Secretary under paragraph (2), information transiting or traveling to or from an agency information system, regardless of the location from which the Secretary or a private entity providing assistance to the Secretary under paragraph (2) accesses such information, notwithstanding any other provision of law that would otherwise restrict or prevent the head of an agency from disclosing such information to the Secretary or a private entity providing assistance to the Secretary under paragraph (2);
“(2) may enter into contracts or other agreements with, or otherwise request and obtain the assistance of, private entities to deploy and operate technologies in accordance with subsection (b);
“(3) may retain, use, and disclose information obtained through the conduct of activities authorized under this section only to protect information and information systems from cybersecurity risks;
“(4) shall regularly assess through operational test and evaluation in real world or simulated environments available advanced protective technologies to improve detection and prevention capabilities, including commercial and non-commercial technologies and detection technologies beyond signature-based detection, and utilize such technologies when appropriate;
[Page: S6417]
“(5) shall establish a pilot to acquire, test, and deploy, as rapidly as possible, technologies described in paragraph (4);
“(6) shall periodically update the privacy impact assessment required under section 208(b) of the E-Government Act of 2002 (44 U.S.C. 3501 note); and
“(7) shall ensure that—
“(A) activities carried out under this section are reasonably necessary for the purpose of protecting agency information and agency information systems from a cybersecurity risk;
“(B) information accessed by the Secretary will be retained no longer than reasonably necessary for the purpose of protecting agency information and agency information systems from a cybersecurity risk;
“(C) notice has been provided to users of an agency information system concerning access to communications of users of the agency information system for the purpose of protecting agency information and the agency information system; and
“(D) the activities are implemented pursuant to policies and procedures governing the operation of the intrusion detection and prevention capabilities.
“(d) *Private Entities*.—
“(1) **CONDITIONS**.—A private entity described in subsection (c)(2) may not—
“(A) disclose any network traffic transiting or traveling to or from an agency information system to any entity without the consent of the Department or the agency that disclosed the information under subsection (c)(1); or
“(B) use any network traffic transiting or traveling to or from an agency information system to

which the private entity gains access in accordance with this section for any purpose other than to protect agency information and agency information systems against cybersecurity risks or to administer a contract or other agreement entered into pursuant to subsection (c)(2) or as part of another contract with the Secretary.
"(2) **LIMITATION ON LIABILITY**.—No cause of action shall lie in any court against a private entity for assistance provided to the Secretary in accordance with this section and any contract or agreement entered into pursuant to subsection (c)(2).
"(3) **RULE OF CONSTRUCTION**.—Nothing in paragraph (2) shall be construed to authorize an Internet service provider to break a user agreement with a customer without the consent of the customer.
"(e) *Attorney General Review*.—Not later than 1 year after the date of enactment of this section, the Attorney General shall review the policies and guidelines for the program carried out under this section to ensure that the policies and guidelines are consistent with applicable law governing the acquisition, interception, retention, use, and disclosure of communications.".
(b) *Prioritizing Advanced Security Tools*.—The Director and the Secretary, in consultation with appropriate agencies, shall—
(1) review and update governmentwide policies and programs to ensure appropriate prioritization and use of network security monitoring tools within agency networks; and
(2) brief appropriate congressional committees on such prioritization and use.
(c) *Agency Responsibilities*.—
(1) **IN GENERAL**.—Except as provided in paragraph (2)—
(A) not later than 1 year after the date of enactment of this Act or 2 months after the date on which the Secretary makes available the intrusion detection and prevention capabilities under section 230(b)(1) of the Homeland Security Act of 2002, as added by subsection (a), whichever is later, the head of each agency shall apply and continue to utilize the capabilities to all information traveling between an agency information system and any information system other than an agency information system; and
(B) not later than 6 months after the date on which the Secretary makes available improvements to the intrusion detection and prevention capabilities pursuant to section 230(b)(2) of the Homeland Security Act of 2002, as added by subsection (a), the head of each agency shall apply and continue to utilize the improved intrusion detection and prevention capabilities.
(2) **EXCEPTION**.—The requirements under paragraph (1) shall not apply to the Department of Defense or an element of the intelligence community.
(d) *Table of Contents Amendment*.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (6 U.S.C. 101 note) is amended by striking the items relating to the first section designated as section 226, the second section designated as section 226 (relating to the national cybersecurity and communications integration center), section 227, and section 228 and inserting the following:
"Sec..226..Cybersecurity recruitment and retention.
"Sec..227..National cybersecurity and communications integration center.
"Sec..228..Cybersecurity plans.
"Sec..229..Clearances.
"Sec..230..Federal intrusion detection and prevention system.".
SEC. 204. ADVANCED INTERNAL DEFENSES.
(a) *Advanced Network Security Tools*.—
(1) **IN GENERAL**.—The Secretary shall include in the Continuous Diagnostics and Mitigation Program advanced network security tools to improve visibility of network activity, including

through the use of commercial and free or open source tools, to detect and mitigate intrusions and anomalous activity.
(2) **DEVELOPMENT OF PLAN**.—The Director shall develop and implement a plan to ensure that each agency utilizes advanced network security tools, including those described in paragraph (1), to detect and mitigate intrusions and anomalous activity.
(b) *Improved Metrics*.—The Secretary, in collaboration with the Director, shall review and update the metrics used to measure security under section 3554 of title 44, United States Code, to include measures of intrusion and incident detection and response times.
(c) *Transparency and Accountability*.—The Director, in consultation with the Secretary, shall increase transparency to the public on agency cybersecurity posture, including by increasing the number of metrics available on Federal Government performance websites and, to the greatest extent practicable, displaying metrics for department components, small agencies, and micro agencies.
(d) *Maintenance of Technologies*.—Section 3553(b)(6)(B) of title 44, United States Code, is amended by inserting ", operating, and maintaining" after "deploying".
SEC. 205. FEDERAL CYBERSECURITY REQUIREMENTS.
(a) *Implementation of Federal Cybersecurity Standards*.—Consistent with section 3553 of title 44, United States Code, the Secretary, in consultation with the Director, shall exercise the authority to issue binding operational directives to assist the Director in ensuring timely agency adoption of and compliance with policies and standards promulgated under section 11331 of title 40, United States Code, for securing agency information systems.
(b) *Cybersecurity Requirements at Agencies*.—
(1) **IN GENERAL**.—Consistent with policies, standards, guidelines, and directives on information security under subchapter II of chapter 35 of title 44, United States Code, and the standards and guidelines promulgated under section 11331 of title 40, United States Code, and except as provided in paragraph (2), not later than 1 year after the date of enactment of this Act, the head of each agency shall—
(A) identify sensitive and mission critical data stored by the agency consistent with the inventory required under the first subsection (c) (relating to the inventory of major information systems) and the second subsection (c) (relating to the inventory of information systems) of section 3505 of title 44, United States Code;
(B) assess access controls to the data described in subparagraph (A), the need for readily accessible storage of the data, and individuals' need to access the data;
(C) encrypt or otherwise render indecipherable to unauthorized users the data described in subparagraph (A) that is stored on or transiting agency information systems;
(D) implement a single sign-on trusted identity platform for individuals accessing each public website of the agency that requires user authentication, as developed by the Administrator of General Services in collaboration with the Secretary; and
(E) implement identity management consistent with section 504 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7464), including multi-factor authentication, for—
(i) remote access to an agency information system; and
(ii) each user account with elevated privileges on an agency information system.
(2) **EXCEPTION**.—The requirements under paragraph (1) shall not apply to—
(A) the Department of Defense or an element of the intelligence community; or
(B) an agency information system for which—
(i) the head of the agency has personally certified to the Director with particularity that—
(I) operational requirements articulated in the certification and related to the agency information

system would make it excessively burdensome to implement the cybersecurity requirement;
(II) the cybersecurity requirement is not necessary to secure the agency information system or agency information stored on or transiting it; and
(III) the agency has all taken necessary steps to secure the agency information system and agency information stored on or transiting it; and
(ii) the head of the agency or the designee of the head of the agency has submitted the certification described in clause (i) to the appropriate congressional committees and the authorizing committees of the agency.
(3) **RULES OF CONSTRUCTION**.—Nothing in this section shall be construed—
(A) to alter the authority of the Secretary, the Director, or the Director of the National Institute of Standards and Technology in implementing subchapter II of chapter 35 of title 44, United States Code;
(B) to affect the National Institute of Standards and Technology standards process or the requirement under section 3553(a)(4) of title 44, United States Code; or
(C) to discourage continued improvements and advancements in the technology, standards, policies, and guidelines used to promote Federal information security.
SEC. 206. ASSESSMENT; REPORTS.
(a) *Definitions*.—In this section—
(1) the term "intrusion assessments" means actions taken under the intrusion assessment plan to identify and remove intruders in agency information systems;
[Page: S6418]
(2) the term "intrusion assessment plan" means the plan required under section 228(b)(1) of the Homeland Security Act of 2002, as added by section 203(a) of this Act; and
(3) the term "intrusion detection and prevention capabilities" means the capabilities required under section 230(b) of the Homeland Security Act of 2002, as added by section 203(a) of this Act.
(b) *Third Party Assessment*.—Not later than 3 years after the date of enactment of this Act, the Government Accountability Office shall conduct a study and publish a report on the effectiveness of the approach and strategy of the Federal Government to securing agency information systems, including the intrusion detection and prevention capabilities and the intrusion assessment plan.
(c) *Reports to Congress*.—
(1) **INTRUSION DETECTION AND PREVENTION CAPABILITIES**.—
(A) **SECRETARY OF HOMELAND SECURITY REPORT**.—Not later than 6 months after the date of enactment of this Act, and annually thereafter, the Secretary shall submit to the appropriate congressional committees a report on the status of implementation of the intrusion detection and prevention capabilities, including—
(i) a description of privacy controls;
(ii) a description of the technologies and capabilities utilized to detect cybersecurity risks in network traffic, including the extent to which those technologies and capabilities include existing commercial and non-commercial technologies;
(iii) a description of the technologies and capabilities utilized to prevent network traffic associated with cybersecurity risks from transiting or traveling to or from agency information systems, including the extent to which those technologies and capabilities include existing commercial and non-commercial technologies;
(iv) a list of the types of indicators or other identifiers or techniques used to detect cybersecurity risks in network traffic transiting or traveling to or from agency information systems on each

iteration of the intrusion detection and prevention capabilities and the number of each such type of indicator, identifier, and technique;
(v) the number of instances in which the intrusion detection and prevention capabilities detected a cybersecurity risk in network traffic transiting or traveling to or from agency information systems and the number of times the intrusion detection and prevention capabilities blocked network traffic associated with cybersecurity risk; and
(vi) a description of the pilot established under section 230(c)(5) of the Homeland Security Act of 2002, as added by section 203(a) of this Act, including the number of new technologies tested and the number of participating agencies.
(B) **OMB REPORT**.—Not later than 18 months after the date of enactment of this Act, and annually thereafter, the Director shall submit to Congress, as part of the report required under section 3553(c) of title 44, United States Code, an analysis of agency application of the intrusion detection and prevention capabilities, including—
(i) a list of each agency and the degree to which each agency has applied the intrusion detection and prevention capabilities to an agency information system; and
(ii) a list by agency of—
(I) the number of instances in which the intrusion detection and prevention capabilities detected a cybersecurity risk in network traffic transiting or traveling to or from an agency information system and the types of indicators, identifiers, and techniques used to detect such cybersecurity risks; and
(II) the number of instances in which the intrusion detection and prevention capabilities prevented network traffic associated with a cybersecurity risk from transiting or traveling to or from an agency information system and the types of indicators, identifiers, and techniques used to detect such agency information systems.
(2) **OMB REPORT ON DEVELOPMENT AND IMPLEMENTATION OF INTRUSION ASSESSMENT PLAN, ADVANCED INTERNAL DEFENSES, AND FEDERAL CYBERSECURITY BEST PRACTICES**.—The Director shall—
(A) not later than 6 months after the date of enactment of this Act, and 30 days after any update thereto, submit the intrusion assessment plan to the appropriate congressional committees;
(B) not later than 1 year after the date of enactment of this Act, and annually thereafter, submit to Congress, as part of the report required under section 3553(c) of title 44, United States Code—
(i) a description of the implementation of the intrusion assessment plan;
(ii) the findings of the intrusion assessments conducted pursuant to the intrusion assessment plan;
(iii) advanced network security tools included in the Continuous Diagnostics and Mitigation Program pursuant to section 204(a)(1);
(iv) the results of the assessment of the Secretary of best practices for Federal cybersecurity pursuant to section 205(a); and
(v) a list by agency of compliance with the requirements of section 205(b); and
(C) not later than 1 year after the date of enactment of this Act, submit to the appropriate congressional committees—
(i) a copy of the plan developed pursuant to section 204(a)(2); and
(ii) the improved metrics developed pursuant to section 204(b).
SEC. 207. TERMINATION.
(a) *In General*.—The authority provided under section 230 of the Homeland Security Act of 2002, as added by section 203(a) of this Act, and the reporting requirements under section 206(c) shall terminate on the date that is 7 years after the date of enactment of this Act.
(b) *Rule of Construction*.—Nothing in subsection (a) shall be construed to affect the limitation of

liability of a private entity for assistance provided to the Secretary under section 230(d)(2) of the Homeland Security Act of 2002, as added by section 203(a) of this Act, if such assistance was rendered before the termination date under subsection (a) or otherwise during a period in which the assistance was authorized.

SEC. 208. IDENTIFICATION OF INFORMATION SYSTEMS RELATING TO NATIONAL SECURITY.

(a) *In General*.—Except as provided in subsection (c), not later than 180 days after the date of enactment of this Act—

(1) the Director of National Intelligence, in coordination with the heads of other agencies, shall—

(A) identify all unclassified information systems that provide access to information that may provide an adversary with the ability to derive information that would otherwise be considered classified;

(B) assess the risks that would result from the breach of each unclassified information system identified in subparagraph (A); and

(C) assess the cost and impact on the mission carried out by each agency that owns an unclassified information system identified in subparagraph (A) if the system were to be subsequently designated as a national security system, as defined in section 11103 of title 40, United States Code; and

(2) the Director of National Intelligence shall submit to the appropriate congressional committees, the Select Committee on Intelligence of the Senate, and the Permanent Select Committee on Intelligence of the House of Representatives a report that includes the findings under paragraph (1).

(b) *Form*.—The report submitted under subsection (a)(2) shall be in unclassified form, and shall include a classified annex.

(c) *Exception*.—The requirements under subsection (a)(1) shall not apply to the Department of Defense or an element of the intelligence community.

SEC. 209. DIRECTION TO AGENCIES.

(a) *In General*.—Section 3553 of title 44, United States Code, is amended by adding at the end the following:

“(h) *Direction to Agencies*.—

“(1) **AUTHORITY**.—

“(A) **IN GENERAL**.—Subject to subparagraph (B), in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency, the Secretary may issue an emergency directive to the head of an agency to take any lawful action with respect to the operation of the information system, including such systems owned or operated by another entity on behalf of an agency, that collects, processes, stores, transmits, disseminates, or otherwise maintains agency information, for the purpose of protecting the information system from, or mitigating, an information security threat.

“(B) **EXCEPTION**.—The authorities of the Secretary under this subsection shall not apply to a system described in paragraph (2) or (3) of subsection (e).

“(2) **PROCEDURES FOR USE OF AUTHORITY**.—The Secretary shall—

“(A) in coordination with the Director, establish procedures governing the circumstances under which a directive may be issued under this subsection, which shall include—

“(i) thresholds and other criteria;

“(ii) privacy and civil liberties protections; and

“(iii) providing notice to potentially affected third parties;
“(B) specify the reasons for the required action and the duration of the directive;
“(C) minimize the impact of a directive under this subsection by—
“(i) adopting the least intrusive means possible under the circumstances to secure the agency information systems; and
“(ii) limiting directives to the shortest period practicable;
“(D) notify the Director and the head of any affected agency immediately upon the issuance of a directive under this subsection;
“(E) consult with the Director of the National Institute of Standards and Technology regarding any directive issued under this subsection that implements standards and guidelines developed by the National Institute of Standards and Technology;
“(F) ensure that directives issued under this subsection do not conflict with the standards and guidelines issued under section 11331 of title 40;
“(G) consider any applicable standards or guidelines developed by the National Institute of Standards and issued by the Secretary of Commerce under section 11331 of title 40; and
“(H) not later than February 1 of each year, submit to the appropriate congressional committees a report regarding the specific actions the Secretary has taken pursuant to paragraph (1)(A).
“(3) **IMMINENT THREATS**.—
“(A) **IN GENERAL**.—Notwithstanding section 3554, the Secretary may authorize the use of protective capabilities under the control of the Secretary for communications or other
[Page: S6419]
system traffic transiting to or from or stored on an agency information system for the purpose of ensuring the security of the information or information system or other agency information systems, if—
“(i) the Secretary determines that there is an imminent threat to agency information systems;
“(ii) the Secretary determines that a directive issued under subsection (b)(2)(C) or paragraph (1)(A) is not reasonably likely to result in a timely response to the threat;
“(iii) the Secretary determines that the risk posed by the imminent threat outweighs any adverse consequences reasonably expected to result from the use of protective capabilities under the control of the Secretary;
“(iv) the Secretary provides prior notice to the Director and the head and chief information officer (or equivalent official) of each agency to which specific actions will be taken pursuant to this subparagraph, and notifies the appropriate congressional committees and authorizing committees of each such agencies within 7 days of taking an action under this subparagraph, of—
“(I) any action taken under this subparagraph; and
“(II) the reasons for and duration and nature of the action;
“(v) the action of the Secretary is consistent with applicable law; and
“(vi) the Secretary authorizes the use of protective capabilities in accordance with the advance procedures established under subparagraph (C).
“(B) **LIMITATION ON DELEGATION**.—The authority under subparagraph (A) may not be delegated by the Secretary.
“(C) **ADVANCE PROCEDURES**.—The Secretary shall, in coordination with the Director and in consultation with the heads of agencies, establish procedures governing the circumstances under which the Secretary may authorize the use of protective capabilities under subparagraph (A). The Secretary shall submit the procedures to Congress.
“(4) **LIMITATION**.—The Secretary may direct or authorize lawful action or protective

capability under this subsection only to—
"(A) protect agency information from unauthorized access, use, disclosure, disruption, modification, or destruction; or
"(B) require the remediation of or protect against identified information security risks with respect to—
"(i) information collected or maintained by or on behalf of an agency; or
"(ii) that portion of an information system used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.
"(i) *Annual Report to Congress*.—Not later than February 1 of each year, the Director shall submit to the appropriate congressional committees a report regarding the specific actions the Director has taken pursuant to subsection (a)(5), including any actions taken pursuant to section 11303(b)(5) of title 40.
"(j) *Appropriate Congressional Committees*.—In this section, the term 'appropriate congressional committees' means—
"(1) the Committee on Appropriations, the Committee on Homeland Security and Governmental Affairs, and the Committee on Commerce, Science, and Transportation of the Senate; and
"(2) the Committee on Appropriations, the Committee on Homeland Security, the Committee on Oversight and Government Reform, and the Committee on Science, Space, and Technology of the House of Representatives.".
(b) *Technical Amendment*.—Section 3554(a)(1)(B) of title 44, United States Code, is amended—
(1) in clause (iii), by striking "and" at the end; and
(2) by adding at the end the following: "(v) emergency directives issued by the Secretary under section 3553(h); and".
"(v) emergency directives issued by the Secretary under section 3553(h); and".

12. Floor amendment No. 2552 (Sen. Coons)—Oppose

Analysis and position

- **Analysis:** The amendment would seemingly address the "second scrub" issue, which is being advocated by some privacy groups. It requires DHS to perform a second scrub of the cyber threat indicators (CTIs) and defensive measures (DMs) for personal information that is received through the DHS portal before passing the threat information to other federal agencies and departments.

  References to "real-time" sharing—language that is meant to spur operational speediness—have been replaced with references to "as quickly as operationally possible." This change suggests that information sharing could be brought to a halt, which is clearly an undesirable outcome. The amendment also adds language facilitating the modification of CTIs and DMs, which is practically synonymous with delayed sharing.

  It is unclear how federal entities would respond to this so-called second scrub of personal information, but excessive caution and a reluctance to share on the part of federal officials information are likely results.

  From industry's standpoint, there are two changes to the guidelines in CISA that

determine what businesses may share with the federal government (section 5) and are edited directly below.

- Identification of types of information that would qualify as a cyber threat indicator under this Act that would be unlikely to include personal information of or identifying a specific person not ~~directly related to a cybersecurity threat~~ **necessary to describe or identify a cyber security threat**.
- Identification of types of information protected under otherwise applicable privacy laws that are unlikely to be ~~directly related to a cybersecurity threat~~ **necessary to describe or identify a cybersecurity threat**.

These tweaks may seem minor to the casual reader, but the inclusion of "necessary" adds a layer of subjectivity as to what may or may not be a cybersecurity threat. Such ambiguity would almost certainly lead to delayed and uncertain decision making, which greatly concerns coalition members.

- **Coalition position:** The coalition opposes this amendment. Granting authority to DHS to conduct a second scrub is not inherently bad if viewed only through the vague lens of "privacy." But privacy is just one of several considerations in CISA. For example, when one understands that CTIs rarely if ever contain personal information, the second scrub would bog down the sharing of CTIs from businesses to the federal entities that need them in a timely manner.

  Also, scrubbing by DHS could become, in reality, a bureaucratic end in itself; it is critical to highlight that the DHS portal is intended to serve as an efficient entry point for the receipt of CTIs and DMs coming from both private and public entities.

Text of the amendment

SA 2552. Mr. COONS submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

Beginning on page 21, strike line 23 and all that follows through page 31, line 5 and insert the following:
(3) **REQUIREMENTS CONCERNING POLICIES AND PROCEDURES**.—Consistent with the guidelines required by subsection (b), the policies and procedures developed and promulgated under this subsection shall—
(A) ensure that cyber threat indicators shared with the Federal Government by any entity pursuant to section 4 that are received through the process described in subsection (c) of this section and that satisfy the requirements of the guidelines developed under subsection (b)—
(i) are shared in an automated manner with all of the appropriate Federal entities;
(ii) are not subject to any unnecessary delay, interference, or any other action that could impede receipt by all of the appropriate Federal entities; and
(iii) may be provided to other Federal entities;
(B) ensure that cyber threat indicators shared with the Federal Government by any entity

pursuant to section 4 in a manner other than the process described in subsection (c) of this section—
(i) are shared as quickly as operationally practicable with all of the appropriate Federal entities;
(ii) are not subject to any unnecessary delay, interference, or any other action that could impede receipt by all of the appropriate Federal entities; and
(iii) may be provided to other Federal entities;
(C) consistent with this Act, any other applicable provisions of law, and the fair information practice principles set forth in appendix A of the document entitled "National Strategy for Trusted Identities in Cyberspace" and published by the President in April 2011, govern the retention, use, and dissemination by the Federal Government of cyber threat indicators shared with the Federal Government under this Act, including the extent, if any, to which such cyber threat indicators may be used by the Federal Government; and
(D) ensure there is—
(i) an audit capability; and
(ii) appropriate sanctions in place for officers, employees, or agents of a Federal entity who knowingly and willfully conduct activities under this Act in an unauthorized manner.
(4) **GUIDELINES FOR ENTITIES SHARING CYBER THREAT INDICATORS WITH FEDERAL GOVERNMENT**.—
(A) **IN GENERAL**.—Not later than 60 days after the date of the enactment of this Act, the Attorney General shall develop and make publicly available guidance to assist entities and promote sharing of cyber threat indicators with Federal entities under this Act.
(B) **CONTENTS**.—The guidelines developed and made publicly available under subparagraph (A) shall include guidance on the following:
(i) Identification of types of information that would qualify as a cyber threat indicator under this Act that would be unlikely to include personal information of or identifying a specific person not necessary to describe or identify a cyber security threat.
(ii) Identification of types of information protected under otherwise applicable privacy laws that are unlikely to be necessary to describe or identify a cybersecurity threat.
(iii) Such other matters as the Attorney General considers appropriate for entities sharing cyber threat indicators with Federal entities under this Act.
(b) *Privacy and Civil Liberties*.—
(1) **GUIDELINES OF ATTORNEY GENERAL**.—Not later than 60 days after the date of the enactment of this Act, the Attorney General shall, in coordination with heads of the appropriate Federal entities and in consultation with officers designated under section 1062 of the National Security Intelligence Reform Act of 2004 (42 U.S.C. 2000ee-1), develop, submit to Congress, and make available to the public interim guidelines relating to privacy and civil liberties which shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with activities authorized in this Act.
(2) **FINAL GUIDELINES**.—
(A) **IN GENERAL**.—Not later than 180 days after the date of the enactment of this Act, the Attorney General shall, in coordination with heads of the appropriate Federal entities and in consultation with officers designated under section 1062 of the National Security Intelligence Reform Act of 2004 (42 U.S.C. 2000ee-1) and such private entities with industry expertise as the Attorney General considers relevant, promulgate final guidelines relating to privacy and civil liberties which shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with activities authorized in this Act.
(B) **PERIODIC REVIEW**.—The Attorney General shall, in coordination with heads of the

appropriate Federal entities and in consultation with officers and private entities described in subparagraph (A), periodically review the guidelines promulgated under subparagraph (A).
(3) **CONTENT**.—The guidelines required by paragraphs (1) and (2) shall, consistent with the need to protect information systems from cybersecurity threats and mitigate cybersecurity threats—
(A) limit the impact on privacy and civil liberties of activities by the Federal Government under this Act;
(B) limit the receipt, retention, use, and dissemination of cyber threat indicators containing personal information of or identifying specific persons, including by establishing—
(i) a process for the timely destruction of such information that is known not to be directly related to uses authorized under this Act; and
(ii) specific limitations on the length of any period in which a cyber threat indicator may be retained;
(C) include requirements to safeguard cyber threat indicators containing personal information of or identifying specific persons from unauthorized access or acquisition, including appropriate sanctions for activities by officers, employees, or agents of the Federal Government in contravention of such guidelines;
(D) include procedures for notifying entities and Federal entities if information received pursuant to this section is known or determined by a Federal entity receiving such information not to constitute a cyber threat indicator;
(E) protect the confidentiality of cyber threat indicators containing personal information of or identifying specific persons to the greatest extent practicable and require recipients to be informed that such indicators may only be used for purposes authorized under this Act; and
(F) include steps that may be needed so that dissemination of cyber threat indicators is consistent with the protection of classified and other sensitive national security information.
(c) *Capability and Process Within the Department of Homeland Security*.—
(1) **IN GENERAL**.—Not later than 90 days after the date of the enactment of this Act, the Secretary of Homeland Security, in coordination with the heads of the appropriate Federal entities, shall develop and implement a capability and process within the Department of Homeland Security that—
(A) shall accept from any entity in real time cyber threat indicators and defensive measures, pursuant to this section;
(B) shall, upon submittal of the certification under paragraph (2) that such capability and process fully and effectively operates as described in such paragraph, be the process by which the Federal Government receives cyber threat indicators and defensive measures under this Act that are shared by a private entity with the Federal Government through electronic mail or media, an interactive form on an Internet website, or a real time, automated process between information systems except—
(i) communications between a Federal entity and a private entity regarding a previously shared cyber threat indicator; and
(ii) communications by a regulated entity with such entity's Federal regulatory authority regarding a cybersecurity threat;
(C) shall require the Department of Homeland Security to review all cyber threat indicators and defensive measures received and remove any personal information of or identifying a specific person not necessary to identify or describe the cybersecurity threat before sharing such indicator or defensive measure with appropriate Federal entities;
(D) ensures that all of the appropriate Federal entities receive in an automated manner such cyber

threat indicators as quickly as operationally possible from the Department of Homeland Security;
(E) is in compliance with the policies, procedures, and guidelines required by this section; and
(F) does not limit or prohibit otherwise lawful disclosures of communications, records, or other information, including—
(i) reporting of known or suspected criminal activity, by an entity to any other entity or a Federal entity;
(ii) voluntary or legally compelled participation in a Federal investigation; and
(iii) providing cyber threat indicators or defensive measures as part of a statutory or authorized contractual requirement.
(2) **CERTIFICATION**.—Not later than 10 days prior to the implementation of the capability and process required by paragraph (1), the Secretary of Homeland Security shall, in consultation with the heads of the appropriate Federal entities, certify to Congress whether such capability and process fully and effectively operates—
(A) as the process by which the Federal Government receives from any entity a cyber threat indicator or defensive measure under this Act; and
(B) in accordance with the policies, procedures, and guidelines developed under this section.
(3) **PUBLIC NOTICE AND ACCESS**.—The Secretary of Homeland Security shall ensure there is public notice of, and access to, the capability and process developed and implemented under paragraph (1) so that—
(A) any entity may share cyber threat indicators and defensive measures through such process with the Federal Government; and
(B) all of the appropriate Federal entities receive such cyber threat indicators and defensive measures as quickly as operationally practicable with receipt through the process within the Department of Homeland Security.

13. Floor amendment No. 2612 to S. 754 (Sen. Franken)—Strongly oppose

Analysis and position

- **Analysis:** This amendment would change the definitions of "cybersecurity threat" and "cyber threat indicator" (CTI).

  The amendment narrows what constitutes a cyber threat to "*is reasonably likely to* result in an unauthorized effort to adversely impact" an information system's security from "*may* result in an unauthorized effort to adversely impact" an information system's security [italics added].

  The amendment changes a part of the definition of CTI to "*the harm* caused by an incident" from "*the actual or potential harm* caused by an incident" [italics added].

- **Coalition position:** The coalition strongly opposes this amendment. Both changes would likely result in increased and extended litigation. CISA is supposed to do the exact opposite.

Text of the amendment

SA 2612. Mr. FRANKEN (for himself, Mr. LEAHY, and Mr. WYDEN) submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

Beginning on page 3, strike line 21 and all that follows through page 5, line 8, and insert the following:
system that is reasonably likely to result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.
(B) **EXCLUSION**.—The term "cybersecurity threat" does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.
(6) **CYBER THREAT INDICATOR**.—The term "cyber threat indicator" means information that is necessary to describe or identify—
(A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;
(B) a method of defeating a security control or exploitation of a security vulnerability;
(C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;
(D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;
(E) malicious cyber command and control;
(F) the harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;
(G) any other attribute of a cybersecurity threat, if disclosure of such information is not otherwise prohibited by law; or

14. Floor amendment No. 2632 to S. 754 (Sen. Tester)—Neutral

Analysis and position

- **Analysis:** Sen. Tester's amendment would add at least eight reporting requirements to CISA's *Biennial Report on Implementation* from the heads and the inspectors general of certain agencies and departments (section 7).

- **Coalition position:** The coalition is neutral on this amendment. However, while we do not argue with the amendment's goal of achieving greater oversight of CISA, the granular reporting of cyber threat data could dissuade some businesses from participating in information-sharing programs.

Text of the amendment

SA 2632. Mr. TESTER (for himself and Mr. FRANKEN) submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 40, between lines 12 and 13, insert the following:
(i) The number of cyber threat indicators and defensive measures shared under this Act, including a breakdown of—
(I) the total number of cyber threat indicators shared through the capability described in section 5(c);
(II) a good faith estimate of the number of cyber threat indicators shared by entities with civilian Federal entities through capabilities other than those described in section 5(c);
(III) a good faith estimate of the number of cyber threat indicators shared by entities with military Federal entities through capabilities other than those described in section 5(c);
(IV) the number of times personal information or information that identifies a specific person was removed from a cyber threat indicator shared under section 5(c);
(V) an assessment of the extent to which personal information or information that identifies a specific person was shared under this Act though such information was not necessary to describe or mitigate a cybersecurity threat or security vulnerability;
(VI) a report on any known harms caused by any defensive measure operated or shared under the authority of this Act;
(VII) the total number of times that information shared under this Act was used to prevent, investigate, disrupt, or prosecute any offense under title 18, United States Code, including an offense under section 1028, 1028A, or 1029, or chapter 37or 90 of such title 18; and
(VIII) the total number of times that information shared under this Act was used to prevent, investigate, disrupt, or prosecute a terrorism offense under chapter 113B of title 18, United States Code.

15. Floor amendment No. 2587 to S. 754 (Sen. Leahy)—Strongly oppose

Analysis and position

- **Analysis:** The managers' amendment by Sens. Burr and Feinstein strikes one of two pillars of CISA that would grant a new FOIA exemption under CISA. As troubling as this is, information shared under CISA would still be exempt from disclosure, including under existing FOIA exemptions (section 5).

  However, Sen. Leahy's amendment would eliminate completely businesses' appeals to Freedom of Information Act (FOIA) protections when sharing cyber threat indicators (CTIs) and defensive measures (DMs) with the federal government pursuant to CISA.

- **Coalition position:** The coalition is seriously reluctant to see the managers' amendment drop the new FOIA exemption from CISA, as reported by the Senate Intelligence Committee. But such an outcome is unlikely to change, and we support the managers'

amendment.

Therefore, it is very important to the coalition that businesses preserve the applicability of the current exemptions—including exemption No. 4 pertaining to protecting trade secrets and commercial or financial information that could harm the competitive posture or business interests of a company—under FOIA for sharing CTIs and DMs.[1]

Companies may, after all, refrain from exchanging cyber threat data with the federal government if such sharing jeopardizes their security, reputational, economic, and proprietary interests—which most policymakers should not view as an ideal outcome.

Text of the amendment

SA 2587. Mr. LEAHY submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

Beginning on page 32, strike line 17 and all that follows through page 33, line 5.

16. Floor amendment No. 2589 to S. 754 (Sen. Murphy)—Support

Analysis and position

- **Analysis:** Sen. Murphy's amendment, titled the Judicial Redress Act of 2015 (the act), would extend the federal Privacy Act to citizens in other "covered countries." Coalition members have supported similar legislation (S. 1600, which was introduced in June by Sens. Hatch and Murphy, and a companion House bill, H.R. 1428).

  The last two years have seen a significant erosion of global public trust in the U.S. government and industry. Many companies are suffering negative commercial consequences abroad (e.g., the loss of contracts). Businesses are facing further burdens due to foreign proposals to limit international data flows and impose onerous localization requirements on digital products and services.

  To help restore the public trust necessary for the continued success of U.S. industry, the act would extend certain rights to the citizens of our designated allies, particularly EU member states. Citizens of these major U.S. allies would be able to avail themselves of the core benefits that Americans enjoy under the Privacy Act. American citizens already enjoy similar rights in most EU member countries.

  The Obama administration, the Department of Justice, and federal law enforcement agencies support the act. Among other things, the act would serve as a clear signal to our European allies that they can feel comfortable sharing critical law enforcement-related

[1] http://www.dhs.gov/foia-exemptions

information with the U.S. government.

The extension of rights provided for in the act is viewed by many American allies as necessary to help restore public trust in both the U.S. government and in U.S. firms.

Coalition position: The coalition backs adding the amendment/act to CISA.

Text of the amendment

SA 2589. Mr. MURPHY (for himself and Mr. HATCH) submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the end, add the following:

SEC. __. JUDICIAL REDRESS.

(a) *Short Title*.—This section may be cited as the "Judicial Redress Act of 2015".

(b) *Extension of Privacy Act Remedies to Citizens of Designated Countries*.—

(1) **CIVIL ACTION; CIVIL REMEDIES**.—With respect to covered records, a covered person may bring a civil action against an agency and obtain civil remedies, in the same manner, to the same extent, and subject to the same limitations, including exemptions and exceptions, as an individual may bring and obtain with respect to records under—

(A) section 552a(g)(1)(D) of title 5, United States Code, but only with respect to disclosures intentionally or willfully made in violation of section 552a(b) of such title; and

(B) subparagraphs (A) and (B) of section 552a(g)(1) of title 5, United States Code, but such an action may only be brought against a designated Federal agency or component.

(2) **EXCLUSIVE REMEDIES**.—The remedies set forth in paragraph (1) are the exclusive remedies available to a covered person under this subsection.

(3) **APPLICATION OF THE PRIVACY ACT WITH RESPECT TO A COVERED PERSON**.—For purposes of a civil action described in paragraph (1), a covered person shall have the same rights, and be subject to the same limitations, including exemptions and exceptions, as an individual has and is subject to under section 552a of title 5, United States Code, when pursuing the civil remedies described in subparagraphs (A) and (B) of paragraph (1).

(4) **DESIGNATION OF COVERED COUNTRY**.—

(A) **IN GENERAL**.—The Attorney General may, with the concurrence of the Secretary of State, the Secretary of the Treasury, and the Secretary of Homeland Security, designate a foreign country or regional economic integration organization, or member country of such organization, as a "covered country" for purposes of this subsection if—

(i) the country or regional economic integration organization, or member country of such organization, has entered into an agreement with the United States that provides for appropriate privacy protections for information shared for the purpose of preventing, investigating, detecting, or prosecuting criminal offenses; or

(ii) the Attorney General has determined that the country or regional economic integration organization, or member country of such organization, has effectively shared information with the United States for the purpose of preventing, investigating, detecting, or prosecuting criminal offenses and has appropriate privacy protections for such shared information.

(B) **REMOVAL OF DESIGNATION**.—The Attorney General may, with the concurrence of

the Secretary of State, the Secretary of the Treasury, and the Secretary of Homeland Security, revoke the designation of a foreign country or regional economic integration organization, or member country of such organization, as a "covered country" if the Attorney General determines that such designated "covered country"—

(i) is not complying with the agreement described under subparagraph (A)(i);

(ii) no longer meets the requirements for designation under subparagraph (A)(ii); or

(iii) impedes the transfer of information (for purposes of reporting or preventing unlawful activity) to the United States by a private entity or person.

(5) **DESIGNATION OF DESIGNATED FEDERAL AGENCY OR COMPONENT**.—

(A) **IN GENERAL**.—The Attorney General shall determine whether an agency or component thereof is a "designated Federal agency or component" for purposes of this subsection. The Attorney General shall not designate any agency or component thereof other than the Department of Justice or a component of the Department of Justice without the concurrence of the head of the relevant agency, or of the agency to which the component belongs.

(B) **REQUIREMENTS FOR DESIGNATION**.—The Attorney General may determine that an agency or component of an agency is a "designated Federal agency or component" for purposes of this subsection, if—

(i) the Attorney General determines that information exchanged by such agency with a covered country is within the scope of an agreement referred to in paragraph (4)(A)(i); or

(ii) with respect to a country or regional economic integration organization, or member country of such organization, that has been designated as a "covered country" under paragraph (4)(A)(ii), the Attorney General determines that designating such agency or component thereof is in the law enforcement interests of the United States.

(6) **FEDERAL REGISTER REQUIREMENT; NONREVIEWABLE DETERMINATION**.—The Attorney General shall publish each determination made under paragraphs (4) and (5). Such determination shall not be subject to judicial or administrative review.

(7) **JURISDICTION**.—The United States District Court for the District of Columbia shall have exclusive jurisdiction over any claim arising under this subsection.

(8) **DEFINITIONS**.—In this section:

(A) **AGENCY**.—The term "agency" has the meaning given that term in section 552(f) of title 5, United States Code.

(B) **COVERED COUNTRY**.—The term "covered country" means a country or regional economic integration organization, or member country of such organization, designated in accordance with paragraph (4).

(C) **COVERED PERSON**.—The term "covered person" means a natural person (other than an individual) who is a citizen of a covered country.

(D) **COVERED RECORD**.—The term "covered record" has the same meaning for a covered person as a record has for an individual under section 552a of title 5, United States Code, once the covered record is transferred—

(i) by a public authority of, or private entity within, a country or regional economic organization, or member country of such organization, which at the time the record is transferred is a covered country; and

(ii) to a designated Federal agency or component for purposes of preventing, investigating, detecting, or prosecuting criminal offenses.

(E) **DESIGNATED FEDERAL AGENCY OR COMPONENT**.—The term "designated Federal agency or component" means a Federal agency or component of an agency designated in

accordance with paragraph (5).
[Page: S6313]
(F) **INDIVIDUAL**.—The term "individual" has the meaning given that term in section 552a(a)(2) of title 5, United States Code.
(9) **PRESERVATION OF PRIVILEGES**.—Nothing in this subsection shall be construed to waive any applicable privilege or require the disclosure of classified information. Upon an agency's request, the district court shall review in camera and ex parte any submission by the agency in connection with this paragraph.
(10) **EFFECTIVE DATE**.—This section shall take effect 90 days after the date of the enactment of this Act.

17. Floor amendment No. 2626 to S. 754 (Sen. Whitehouse)—Support

Analysis and position

Analysis: Sen. Whitehouse's amendment consists of four provisions, each of which is found in the Graham/Whitehouse international cybercrime bill. The amendment includes language designed to (1) strengthen U.S. laws prohibiting the sale of Americans' financial information, (2) expand the Department of Justice's (DOJ's) authority to seek injunctions to shut down botnets, (3) boost penalties for aggravated damage to critical infrastructure computers, and (4) increase penalties for trafficking in passwords.

Computer Fraud and Abuse Act (CFAA) reform is *not* part of the Whitehouse amendment. Specific comments on the four sections of the amendment are bracketed in the text below.

Coalition position: The coalition supports adding this amendment to CISA. U.S. industry is facing a vast array of threat actors, which are operating largely overseas. Criminals use cyber tools like botnets to infect customers' electronic devices and hijack their personal information. Bad actors also seek to disrupt or damage critical infrastructure computer systems.

Businesses' threat detection, information sharing, and incident response capabilities are improving. However, we urge policymakers to increase the costs on attackers. The FBI and the DOJ have had notable successes in indicting members of overseas criminal networks and partnering with the private sector to disrupt botnets and other malicious activity.

However, organizations perpetrating such acts are not fearful of attribution, extradition, and prosecution to the degree that it seriously impacts their cost/benefit calculations. This amendment would help tip the scales of justice toward American law enforcement and industry.

Text of the amendment

SA 2626. Mr. WHITEHOUSE submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the end, add the following:

SEC. __. STOPPING THE SALE OF AMERICANS' FINANCIAL INFORMATION.

Section 1029(h) of title 18, United States Code, is amended by striking "if—" and all that follows through "therefrom." and inserting "if the offense involves an access device issued, owned, managed, or controlled by a financial institution, account issuer, credit card system member, or other entity organized under the laws of the United States, or any State, the District of Columbia, or other Territory of the United States.".

[This section of the amendment would enable the United States to prosecute any foreign individual that unlawfully possesses or traffics access devices (e.g., credit card numbers) that are associated with a U.S. financial institution, regardless of whether the individual stole the financial data initially. Current law applies to use of access devices owned or controlled by entities within the jurisdiction of the United States, including only if the individual transports, delivers, or stores an article used in the offense or proceeds from the offense within U.S. jurisdiction.]

SEC. __. SHUTTING DOWN BOTNETS.

(a) *Amendment*.—Section 1345 of title 18, United States Code, is amended—
(1) in the heading, by inserting "and abuse" after "fraud";
(2) in subsection (a)—
(A) in paragraph (1)—
(i) in subparagraph (B), by striking "or" at the end;
(ii) in subparagraph (C), by inserting "or" after the semicolon; and
(iii) by inserting after subparagraph (C) the following:
"(D) violating or about to violate paragraph (1), (4), (5), or (7) of section 1030(a) where such conduct would affect 100 or more protected computers (as defined in section 1030) during any 1-year period, including by denying access to or operation of the computers, installing malicious software on the computers, or using the computers without authorization;"; and
(B) in paragraph (2), by inserting ", a violation described in subsection (a)(1)(D)," before "or a Federal"; and
(3) by adding at the end the following:
"(c) A restraining order, prohibition, or other action described in subsection (b), if issued in circumstances described in subsection (a)(1)(D), may, upon application of the Attorney General—
"(1) specify that no cause of action shall lie in any court against a person for complying with the restraining order, prohibition, or other action; and
"(2) provide that the United States shall pay to such person a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in complying with the restraining order, prohibition, or other action.".
(b) *Technical and Conforming Amendment*.—The table of section for chapter 63 is amended by striking the item relating to section 1345 and inserting the following:
"1345. Injunctions against fraud and abuse.".

[This amendment would permit the attorney general (AG) to seek a civil injunction to prevent the "operation" of a botnet of 100 or more computers. It also provides that the restraining order may, if requested by the AG, grant immunity to businesses against prosecution as well as reimbursement by the government of reasonable costs incurred in complying with the order.]

SEC. __. AGGRAVATED DAMAGE TO A CRITICAL INFRASTRUCTURE COMPUTER.

(a) *In General*.—Chapter 47 of title 18, United States Code, is amended by inserting after section 1030 the following:

[Page: S6416]

"§1030A. Aggravated damage to a critical infrastructure computer

"(a) *Offense*.—It shall be unlawful, during and in relation to a felony violation of section 1030, to knowingly cause or attempt to cause damage to a critical infrastructure computer, if such damage results in (or, in the case of an attempted offense, would, if completed have resulted in) the substantial impairment—

"(1) of the operation of the critical infrastructure computer; or

"(2) of the critical infrastructure associated with such computer.

"(b) *Penalty*.—Any person who violates subsection (a) shall, in addition to the term of punishment provided for the felony violation of section 1030, be fined under this title, imprisoned for not more than 20 years, or both.

"(c) *Consecutive Sentence*.—Notwithstanding any other provision of law—

"(1) a court shall not place any person convicted of a violation of this section on probation;

"(2) except as provided in paragraph (4), no term of imprisonment imposed on a person under this section shall run concurrently with any term of imprisonment imposed on the person under any other provision of law, including any term of imprisonment imposed for the felony violation of section 1030;

"(3) in determining any term of imprisonment to be imposed for the felony violation of section 1030, a court shall not in any way reduce the term to be imposed for such violation to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and

"(4) a term of imprisonment imposed on a person for a violation of this section may, in the discretion of the court, run concurrently, in whole or in part, only with another term of imprisonment that is imposed by the court at the same time on that person for an additional violation of this section, if such discretion shall be exercised in accordance with any applicable guidelines and policy statements issued by the United States Sentencing Commission pursuant to section 994 of title 28.

"(d) *Definitions*.—In this section

"(1) the terms 'computer' and 'damage' have the meanings given the terms in section 1030; and

"(2) the term 'critical infrastructure' has the meaning given the term in section 1016(e) of the USA PATRIOT Act (42 U.S.C. 5195c(e)).".

(b) *Table of Sections*.—The table of sections for chapter 47 of title 18, United States Code, is amended by inserting after the item relating to section 1030 the following:

"1030A. Aggravated damage to a critical infrastructure computer.".

[This section would add a new criminal penalty for causing or attempting to cause damage to a computer that controls critical infrastructure. The term "critical infrastructure" is defined in relevant statute as "systems and assets . . . so vital to the United States that the[ir] incapacity or destruction . . . would have a debilitating impact on security, national economic security, national public health or safety."]

SEC. __. STOPPING TRAFFICKING IN BOTNETS.
(a) *In General*.—Section 1030 of title 18, United States Code, is amended—
(1) in subsection (a), by striking paragraph (6) and inserting the following:
"(6) knowing such conduct to be wrongful, intentionally traffics in any password or similar information, or any other means of access, further knowing or having reason to know that a protected computer would be accessed or damaged without authorization in a manner prohibited by this section as the result of such trafficking;";
(2) in subsection (c)—
(A) in paragraph (2), by striking ", (a)(3), or (a)(6)" each place it appears and inserting "or (a)(3)"; and
(B) in paragraph (4)—
(i) in subparagraph (C)(i), by striking "or an attempt to commit an offense"; and
(ii) in subparagraph (D), by striking clause (ii) and inserting the following:
"(ii) an offense, or an attempt to commit an offense, under subsection (a)(6);"; and
(3) in subsection (g), in the first sentence, by inserting ", except for a violation of subsection (a)(6)," after "of this section".

[This section of Sen. Whitehouse's amendment removes "intent to defraud" from the definition of the violation for trafficking in computer passwords, potentially making it easier to obtain a conviction. The section also revises the requirement that trafficked password could be used to access a protected computer or a computer used by or for the U.S. government. Instead the proposal would require that the violator knows or have reason to know "that a protected computer would be accessed or damaged without authorization in a manner prohibited" by the existing statute.

Criminal penalties for trafficking in passwords for a first offense would include a fine and prison time of up to 10 years (previously reserved for a second offense), an increase from one year. Further, the amendment eliminates trafficking in passwords from violations for which a private civil action may be brought to recover damages and injunctive relief—meaning, one could not appeal to a court to allow you to continue trafficking in botnets.]

18. Floor amendment No. 2621 to S. 754 (Sen. Wyden)—Strongly oppose

Analysis and position

- **Analysis:** Sen. Wyden's amendment eliminates the language "knows at the time of sharing," which pertains to private entities' removal of personal information in cyber threat indicators (CTIs) that is "not directly related to a cybersecurity threat."

  The amendment would replace the "knows" scrubbing standard with a new one—"to the extent feasible" for information that is "not necessary to describe or identify a cybersecurity threat." The same change is applicable to minimizing personal information in cyber indicators through technical means. (See the italicized text below.)

  What is concerning to industry, the amendment would introduce a higher, presumably more subjective standard. The amendment, in a word, would make sharing more difficult.

It is important to note that since 2011, many coalition members have opposed any form of scrubbing in cybersecurity information-sharing legislation; therefore, in our view, the "knows" construct represents a negotiated compromise.

Industry has argued that mandates in legislation calling for personal information to be removed by businesses would likely have the unintended consequence of preventing small and midsize businesses, and even some large enterprises, from voluntarily engaging in an information-sharing program.

The House cyber bills use the vague "reasonable" phrasing to direct minimizing personal information from CTIs before they are shared. The coalition has argued that the apparently simple concept of "reasonable"—and, similarly, "to the extent feasible"—is certainly not simple when argued over by competing attorneys, security professionals, and government officials.

Interpreting language such as "reasonable efforts" and "to the extent feasible" in legislation is far from straightforward. It would breed legal uncertainty and is contrary to the goal of real-time information sharing. The coalition's strong preference is to maintain the "knows" standard in a final bill.

- **Coalition position:** The coalition strongly opposes the amendment. If adopted, the amendment would give rise to added legal ambiguity; it would act as a disincentive to share—including sharing in a timely manner—which cuts against the grain of the bill. The coalition will push to maintain the "knows" standard in a final bill.

Text of the amendment

SA 2621. Mr. WYDEN (for himself, Mr. UDALL, Mr. BROWN, Mr. FRANKEN, Mr. MARKEY, Mr. BLUMENTHAL, and Ms. BALDWIN) submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 16, strike lines 9 through 21 and insert the following:
(A) review such cyber threat indicator and remove, *to the extent feasible*, any personal information of or identifying a specific individual *that is not necessary to describe or identity a cybersecurity threat*; or
(B) implement and utilize a technical capability configured to remove, to the extent feasible, any personal information of or identifying a specific individual contained within such indicator *that is not necessary to describe or identify a cybersecurity threat* [italics added].

Text of CISA, as reported

(2) REMOVAL OF CERTAIN PERSONAL INFORMATION.—An entity sharing a cyber threat indicator pursuant to this Act shall, prior to such sharing—
(A) review such cyber threat indicator to assess whether such cyber threat indicator contains any information that the entity *knows at the time of sharing* to be personal information of or

identifying a specific person *not directly related to a cybersecurity threat and remove such information*; or
(B) implement and utilize a technical capability configured to remove any information contained within such indicator that the entity *knows at the time of sharing* to be personal information of or identifying a specific person *not directly related to a cybersecurity threat* [italics added].

19. Floor amendment 2622 to S. 754 (Sen. Wyden)—Oppose

Analysis and position

- **Analysis:** The Sen. Wyden amendment would add to the numerous requirements placed on the federal government to facilitate the sharing of cyber threat information and guard individual's privacy and civil liberties, both of which are extensive.

  The amendment requires that the government notify in a timely manner any person whose information is shared in contravention of CISA.

- **Coalition position:** The coalition does not support this amendment for three reasons:

  First, this amendment would likely slow down, if not halt, government-to-businesses information sharing, which is modest and needs improvement. It is not a stretch to think that federal officials would be even more cautious than they already are to share cyber threat data for fear of violating the law.

  Second, arguably, people should know if their information is determined to have been shared in a manner that conflicts with the intent and letter of CISA. Still, the amendment appears to suggest that harm would be done to individuals whose personal data is unintentionally shared, and such harmful outcomes are unclear.

  Third, the amendment perpetuates a myth that shared cyber threat information is broad in scope. In fact, CISA's definition of cyber threat indicators (CTIs) is very limited. In the vast majority of cyber incidents, CTIs do not implicate a person's behavioral, financial, or social information. Businesses and government entities may only share the tactics, techniques, and procedures used by malicious actors to compromise the computer networks of their victims.

Text of the amendment

SA 2622. Mr. WYDEN (for himself, Mr. UDALL, Mr. BROWN, Mr. FRANKEN, Mr. MARKEY, Mr. BLUMENTHAL, and Ms. BALDWIN) submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 12, between lines 7 and 8, insert the following:
(F) include procedures for notifying in a timely manner any person whose personal information

is known or determined to have been shared or disclosed in contravention of this Act.

20. Floor amendment No. 2557 (Sen. Mikulski)—Neutral

Analysis and position

- **Analysis:** Sen. Mikulski's amendment would appropriate $37M until September 30, 2017, related to the Office of Personnel Management (OPM) hacking incident.

- **Coalition position:** Neutral. It is unclear how the dollar figure was arrived at, but many lawmakers will likely support the monetary bump for the agency to mitigate the major data breach.

Text of the amendment

SA 2557. Ms. MIKULSKI (for herself, Mr. CARDIN, and Mr. WARNER) submitted an amendment intended to be proposed by her to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:
SEC. __X. FUNDING.
(a) *In General*.—Effective on the date of enactment of this Act, there is appropriated, out of any money in the Treasury not otherwise appropriated, for the fiscal year ending September 30, 2015, an additional amount for the appropriations account appropriated under the heading **"SALARIES AND EXPENSES"** under the heading *"Office of Personnel Management"*, $37,000,000, to remain available until September 30, 2017, for accelerated cybersecurity in response to data breaches.
(b) *Emergency Designation*.—The amount appropriated under subsection (a) is designated by the Congress as an emergency requirement pursuant to section 251(b)(2)(A)(i) of the Balanced Budget and Emergency Deficit Control Act of 1985, and shall be available only if the President subsequently so designates such amount and transmits such designation to the Congress.

21. Floor amendment No. 2615 to S. 754 (Sen. Carper)—Neutral, with qualifications

Analysis and position

- **Analysis:** Sen. Carper's amendment pertains to the sharing of cyber threat indicators (CTIs) first through the DHS portal, and then they are disseminated to other federal entities. "[U]necessary" describes any potential modifications (e.g., scrubbing personal information) to CTIs before sharing them other federal entities.

  In most instances, it should not be necessary to scrub cyber indicators of personal information, which the amendment seems to recognize. In those rare cases where an individual's personal information may happen to be embedded within CTIs or defensive

measures (DMs), CISA mandates that public and private entities remove such personal data unrelated to a cyber threat when sharing CTIs and DMs.

The amendment seeks wiggle room to perform a "second scrub" of cyber threat information for personal data before it is shared with federal entities in real time under section 5 of the bill.

- **Coalition position:** The coalition is relatively neutral on this amendment. The coalition believes that CTIs and DMs rarely contain personal information, and scrubbing is akin to pumping the breaks on information sharing, which is meant to be fast and disciplined. However, Sen. Carper and Homeland Security Committee staff members are commended for taking a restrained approach to seeking a so-called second scrub of cyber threat data for individuals' personal information.

Text of the amendment

SA 2615. Mr. CARPER submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 22, line 16, insert "unnecessary" after "delay,".