KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

CYBER-SURVEILLANCE BILL SET TO MOVE TO SENATE FLOOR

July 28, 2015

The Senate is expected to consider the Cybersecurity Information Sharing Act (CISA, S. 754[1]) on the Senate floor soon. The bill was marked up in secret, thereby denying the public an opportunity to better understand the risks the legislation poses. This document analyzes the bill as reported by the Senate Select Committee on Intelligence on a vote of 14-1.[2]

More sharing of information about cybersecurity threats among companies and between the public and private sectors could help entities better defend themselves against such threats. But CISA (as well as the cybersecurity bills that the House passed[3]) takes a fundamentally flawed and risky approach: it pre-empts all laws that would otherwise prevent a company or government agency from sharing personal information. As CDT has explained,[4] pre-empting all privacy laws is likely to have unintended effects. To compensate, the authorization would need to be quite narrow, and the protections against abuse quite strong. CISA is neither narrow nor adequately protective against abuse. As a result, CDT and other civil society groups oppose the bill, urge members of the Senate to vote against it, and we urge the President to veto the bill should it come to his desk. CDT also supports amendments that ameliorate the privacy and security concerns that we describe below.

Though CISA was improved at the Committee mark-up, every major concern we expressed about the discussion draft of the bill[5] prior to the mark up is also a major concern with the version of the bill coming to the Senate floor. CISA:

- Authorizes companies to share cyber threat indicators (CTIs) with many agencies in the federal government, including the National Security Agency (NSA), and requires that cyber threat indicators a company shares with the Department of Homeland Security (DHS) be

---

[1] Available at https://www.congress.gov/bill/114th-congress/senate-bill/754/text.

[2] Committee Report available at https://www.congress.gov/congressional-report/114th-congress/senate-report/32/1.

[3] *See*, The Center for Democracy & Technology, *Cybersecurity Information Sharing Bills Fall Short on Privacy Protections* (April 22, 2015), *available at* https://cdt.org/insight/cybersecurity-information-sharing-bills-fall-short-on-privacy-protections/.

[4] S*ee*, United States. Senate. Committee on Homeland Security and Governmental Affairs. *Hearing on Protecting America From Cyber Attacks: The Importance of Information Sharing.* January 28, 2015. 114th Cong. 1st sess (*statement of Greg Nojeim, Director of the Freedom, Security, and Technology Project, The Center for Democracy & Technology*), available at https://cdt.org/files/2015/01/HSGAC-Cybersec-tes-1-28-15-final-TEH.pdf.

[5] *See*, The Center for Democracy and Technology, *Cyber-Surveillance Bill to Move Forward, Secretly* (March 4, 2015), *available at* https://cdt.org/insight/cyber-surveillance-bill-to-move-forward-secretly/.

immediately shared with multiple other federal agencies, including the NSA and other elements of the Department of Defense (DOD), thereby discouraging the very information sharing it would be enacted to foster;
- Risks turning the cybersecurity program it creates into a back door wiretap by authorizing sharing and use of cyber threat indicators for a broad array of law enforcement purposes that have nothing to do with cybersecurity;
- Does not effectively require that personally identifiable information irrelevant to a CTI be removed before information about the threat indicator is shared;
- Pre-empts the federal anti-hacking statute and authorizes broadly-defined cybersecurity countermeasures that could damage a network or information stored on a network, encouraging conduct that runs counter to the cybersecurity purpose of the bill; and
- Fails to affirmatively address the cybersecurity-related conduct of the NSA that undermines cybersecurity.

Following some background information about the legislation, we outline below our major concerns with the bill.

I. Background and Overview

Cyber attacks represent a significant and growing threat. A study by the Center for Strategic and International Studies estimated that the global cost of cyber crime has reached over $445 billion annually.[6] According to an HP study released in October 2014, the average cost of cyber crime to each of 50 U.S. companies surveyed had increased to $12.7 million per company from $6.5 million per company just four years ago. Frequency and intricacy of attacks has increased as well.[7] The same study concluded that the number of successful attacks per company per year has risen by 144 percent since 2010, while the average time to resolve attacks has risen by 221 percent.

Major cyber attacks represent an ongoing hazard to the financial and commercial sectors, with potential to harm both important institutions and individual online users. 2014 saw major attacks against companies such as Target, J.P. Morgan Chase, Home Depot, and Sony Pictures. In addition to direct harms – which are substantial – these large scale and highly publicized attacks threaten to chill use of online services. Cyber attacks also pose a hazard to the government sector, and 2015 already saw two major attacks on sensitive data maintained by the Office of Personnel Management.

However, it is unclear that the information sharing legislation would have stopped any of these attacks. For example, the Target attack seemed to result from bad security practices, and most successful attacks can be stopped by basic security measures, such as frequently changing passwords, patching servers, detecting insider attacks, and educating employees about risks. Moreover, an influential group of technologists, academics, and computer and network security professionals have written that they do not need any new legal authority to share information that helps them protect their systems against attacks, and have come out in opposition to the pending bills.[8] Privacy groups[9] have also registered their opposition and are calling for a presidential veto.[10]

---

[6] Center for Strategic and International Studies, *Net Losses: Estimating the Global Costs of Cybercrime* (June 2014), *available at* http://www.mcafee.com/us/resources/reports/rp-economic- impact-cybercrime2.pdf.

[7] HP, *Ponemon Institute 2014 Cost of Cyber Crime Study* (September 2014), *available at* http://h17009.www1.hp.com/pub/msc/29FD917C-64F3-46A7-955C-EF9D2F8D9E3C.pdf.

[8] Available at https://cyberlaw.stanford.edu/files/blogs/technologists_info_sharing_bills_letter_w_exhibit.pdf.

In addition, current law provides substantial authority to communications service providers to monitor their own networks and to share communications that traverse them for cybersecurity reasons.[11] Under the Wiretap Act and the Electronic Communications Privacy Act, they can intercept, use, and disclose communications content and metadata in order to protect their own rights and property. However, they cannot intercept, use, nor disclose communications to protect others. A narrow exception may be needed to fill this narrow gap. However, the approach the bill takes is not narrow.

CISA operates by authorizing companies to monitor information systems for "cybersecurity purposes" to protect them against "cybersecurity threats" and "security vulnerabilities." Sections 4(a), 2(4), 2(5), and 2(17). Information that qualifies as a "cyber threat indicator" or a "defensive measure" can be shared with the federal government or among private entities. Sections 4(c), 2(6) and 2(7). The indicators are defined using broad, functional language, rather than technical language, because of concerns that technical language would become outdated quickly. This expands the information that can be shared beyond technical data. As noted in the technologist letter above, "threat data that security professionals use to protect networks from future attacks is a far more narrow category of information" than CISA's definition of CTIs. To compensate, partially, for the breadth of the information that can be shared, the bill imposes some restrictions on the use of cyber threat indicators and creates some obligations to strip out personal information before they are shared. The bill also authorizes countermeasures against cybersecurity threats. All of this conduct – monitoring, information sharing, and countermeasures – is authorized "notwithstanding any law," so if an existing privacy or security law would prohibit a particular action, it wouldn't matter. Monitoring and information sharing conduct is given strong liability protection, but countermeasures – because they can harm others – are not given specific liability protection. Proponents of the legislation argue that it is needed to respond to and prevent cyber attacks.

II. Problems in the Legislation

(1) Expansive Sharing and Use Permissions Threaten to Turn This Cybersecurity Bill Into a Cyber Surveillance Bill. The bill permits companies to share "cyber threat indicators" notwithstanding any law -- including all of the privacy laws. However CTIs are far broader than technical data and threat signatures. In order to cover the information that needs to be shared, the CTIs are defined broadly enough to include, for example:

- Medical records, financial records, keying materials, passwords, and trade secrets stolen in a cyber attack because they show the actual harm caused by the incident;
- Web browsing activity of innocent users who visit a website that is subjected to a DDOS attack, because their visits to the website are difficult to separate from the visits associated with the DDOS attack; and
- The text of communications associated with spear fishing attacks, because that text constitutes a method of defeating a security control.

---

[9] *See*, The Center for Democracy & Technology, *Letter to Senate Select Committee on Intelligence regarding CISA* (March 2, 2015), *available at* https://cdt.org/insight/letter-to-senate-select-cmte-on-cisa/.

[10] *See*, *Letter From Civil Society Organizations, Security Experts, and Academics to President Obama* (July 27, 2015), *available at* https://static.newamerica.org/attachments/4459-pr-massive-coalition-of-security-experts-companies-and-civil-society-groups-urge-obama-to-veto-cisa/Final_Coalition Ltr Urging Pres. to Veto CISA.8b33e2d86dc14780b35c9cde44a41797.pdf.

[11] S*ee*, United States. Senate. Committee on Homeland Security and Governmental Affairs. *Hearing on Protecting America From Cyber Attacks: The Importance of Information Sharing*. January 28, 2015. 114th Cong. 1st sess (*statement of Greg Nojeim, Director of the Freedom, Security, and Technology Project, The Center for Democracy & Technology*), available at https://cdt.org/files/2015/01/HSGAC-Cybersec-tes-1-28-15-final-TEH.pdf.

The sharing of some of this information is necessary for cybersecurity. However, because of the breadth of the information that can shared is quite wide, the purpose of the information sharing and use of the information shared should be narrow, and focused on cybersecurity.

Instead, the bill permits companies to share any data that meet the broad definition of cyber threat indicators not just for cybersecurity purposes, but for any purpose permitted under the bill, including broad law enforcement purposes. Section 4(c)(1). Once shared, such information could be pooled and mined repeatedly over time not for cybersecurity reasons, but rather for preventing, investigating, mitigating, or prosecuting terrorism suspects, fraud and ID theft, espionage, censorship, theft of trade secrets, and a host of felonies that include running drugs with a gun, kidnapping, and car jacking. Section 5(d)(5).

(2) "Insta-Sharing" Mandate and Overbroad Info Sharing Permission Harms Privacy and Security. Instead of requiring that cyber threat indicators be shared only with DHS, the bill permits companies to share cyber threat indicators with any agency of the federal government, including the NSA, Department of Justice, and DOD's Cyber Command. This permission operates "notwithstanding any law" and regardless of whether the indicator is shared for cybersecurity or law enforcement purposes. Section 4(c). Thus, disclosure of user communications information that could be done under current law only based a warrant or court order can be volunteered to the government under the bill.

To encourage companies to share CTIs with DHS as opposed to other governmental agencies, companies are given liability protection when they share CTIs with DHS, or when they share under certain exceptions in the bill. Section 6(b). However, DHS must share in real time the CTIs it receives in electronic form with all "appropriate government agencies" including the NSA, the FBI, the Commerce Department and many others. Section 5(a)(3)(A) and Section 2(3). Thus, while the bill establishes a "civilian portal" through which CTIs received from the private sector in electronic form could be shared, the broad "insta-sharing" mandate directs everything shared with DHS right to the NSA. The bill requires privacy guidelines that govern the sharing of CTIs within the Federal government, but the guidelines must reflect the insta-sharing mandate, and they need not even be in place before insta-sharing begins.

Even for CTI's that are shared by private entities with the government in other than electronic form, the sharing mandate is excessive: no restriction on sharing, including any privacy-related restriction that takes time, can subject sharing to any "action that could impede receipt by all appropriate government agencies." That is, if a CTI shared with the government need not be shared with the NSA because it is irrelevant to the NSA's mission, or if the analysis required to decide whether it should be shared takes any time, it must be shared anyway because holding it back would "impede receipt" by an "appropriate government agency." Section 5(a)(3)(B).

Insta-sharing harms both privacy and security. First, it funnels cyber threat indicators containing personal information directly to the NSA even when the NSA does not need the CTI's for its mission. This is unnecessary. Second, it does not permit privacy measures – including data minimization, if they take any time. Speed is often a crucial part of cyber response, but sometimes, the need to be careful to share only information necessary to describe a threat should be permitted to trump the need for speed. Third, it undermines security by discouraging companies from voluntarily sharing cyber threat indicators. Companies want to assure users that they aren't sharing private data with the NSA; after the

revelation of PRISM many companies affirmatively stated they would not do so.[12] Because CISA mandates insta-sharing with the NSA, companies might opt not to share CTIs at all, undercutting the key goal of the legislation. Fourth, it undermines security by requiring insta-sharing with a large number of federal agencies regardless of whether they have the technical capabilities to store and adequately protect sensitive data. In the wake of the OPM hacks, and with many agencies facing similar security problems,[13] this is a concern that should not go ignored.[14]

(3) Authorization for Countermeasures Undermines Cybersecurity. The federal anti-hacking law, the Computer Fraud and Abuse Act ("CFAA") subjects to criminal and civil liability anyone who intentionally accesses another person's computer without authorization and as a result of such conduct, recklessly causes damage. 18 USC 1030(a)(5)(B). If the damage caused exceeds $5,000 or effects 10 or more computers, the perpetrator faces a hefty fine and up to 5 years in prison. For certain countermeasures, CISA removes this potential liability, thus giving a green light to conduct that would otherwise constitute hacking.

Under the bill, a company may employ a countermeasure notwithstanding any law. A countermeasure (euphemistically re-named at mark up as a "defensive measure") is any action, device, technique, procedure or other measure applied to on one's own information system (or the system of a consenting party) or to information on such system, which detects, prevents, or mitigates a known or suspected cybersecurity threat. Countermeasures cannot include a measure that "destroys, renders unusable, or substantially harms an information system or data on an information system" other than one's own or that of a consenting party.

As a result, countermeasures that are deployed for legitimate reasons on one network that damage data on another network, or damage the network itself, would become lawful under the bill so long as the damage is not "substantial," which is undefined in the bill, leaving private actors to decide how much damage they may be authorized to cause. Countermeasures deployed on one network that slow another or impede access to data on another network, would also become lawful. Countermeasures deployed on one network that render unusable a physical device attached to another network, but do not cause substantial harm *to information or to an information system* also become lawful. Specific examples of permissible conduct are outlined here. Despite the CFAA, such conduct would not result in criminal liability and prospects for any civil liability in tort are unclear at best. This could do real harm to the Internet.

A cybersecurity bill should not authorize conduct prohibited by the federal anti-hacking statute. This one does.

(4) Protection of Personal Information Falls Short. The bill requires companies to review CTI's before sharing them and to strip out personal information that the company "knows at the time of sharing to be … not directly related to a cybersecurity threat" before sharing. The

---

[12] *See*, Chenda Ngak, *Apple, Google, Facebook, Yahoo, Microsoft, Paltalk, AOL issue statements of denial in NSA data mining*, CBS News (June 7, 2013), *available at* http://www.cbsnews.com/news/apple-google-facebook-yahoo-microsoft-paltalk-aol-issue-statements-of- denial-in-nsa-data-mining/.

[13] *See*, Office of Management and Budget, *Annual Report to Congress: Federal Information and Security Management Act* (February 27, 2015), *available at* https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy14_fisma_report_02_27_2015.pdf.

[14] See, Jake Laperruque, How the OPM Hack Demonstrates the Need to Improve CISA, The Center for Democracy & Technology (June 24, 2015), available at https://cdt.org/blog/how-the-opm-hack-demonstrates-the-need-to-improve-cisa/.

2014 version of the bill did not require *any* proactive review, so this is an improvement. However, the bill sets no standard for this review: Even a cursory review that simply "goes through the motions" would suffice. Moreover, a company could still share personal information it suspects or even *strongly believes* is irrelevant to a cybersecurity threat as long as it does not definitely *know* such. Such a standard could lead companies to share all information by default. Finally, the bill only requires removal of information that is not related to a threat, which leaves victims' information that is unnecessary to counter a threat but still *related to* the threat unprotected. A better approach would be to require a company to make reasonable efforts to strip out personal information it does not reasonably believe to be necessary to describe or mitigate a cybersecurity threat, based on guidelines DHS would issue.

(5) NSA Anti-Cybersecurity Activity Is Ignored. It would be tragic if the Congressional response to revelations that the NSA may be engaging in activity that diminishes, rather than enhances, cybersecurity, was to ignore them. In particular, revealed documents suggest that the NSA may be stockpiling "zero day" vulnerabilities in software so it can later exploit them for espionage. A zero day vulnerability is one not previously disclosed to the software maker so the vulnerability can be patched. The vulnerabilities can be exploited by hackers and foreign intelligence agencies to the detriment of cybersecurity worldwide. The President's Review Group on Intelligence and Communications Technologies recommended that such vulnerabilities be quickly disclosed to software companies with rare exception.[15] Congress should use the occasion of consideration of cybersecurity information sharing legislation to require this disclosure.

III. Conclusion

While cybersecurity threats continue to be a significant problem warranting Congressional action, CISA goes well beyond authorizing necessary conduct, to authorizing dangerous conduct, and unnecessarily harming privacy. Its broad use permissions suggest that the legislation is as much about surveillance as it is about cybersecurity. We urge Senators to oppose the bill, support amendments to improve it, and for the President to veto the bill should it come to his desk.

[15] *The President's Review Group on Intelligence and Communications Technologies, Liberty and Security in a Changing World*, (Dec. 12, 2013), 219, *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.