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

CYBERSECURITY INFORMATION SHARING BILLS FALL SHORT ON PRIVACY PROTECTIONS

April 22, 2015

The Center for Democracy and Technology opposes the two cybersecurity information sharing bills that are coming to the floor of the House of Representatives today, April 22. The Protecting Cyber Networks Act, reported by the House Permanent Select Committee on Intelligence (H.R. 1560, the "HPSCI Bill") and the National Cybersecurity Protection Advancement Act reported by the House Homeland Security Committee (H.R. 1731, the "Homeland Bill"), were both overwhelmingly approved in committee and are expected to pass in the House.

While the two bills have much in common, ***with respect to virtually every civil liberties issue on which the two bills differ, the Homeland Bill comes out on top.*** Both bills authorize companies in the private sector to share among themselves and with the Federal government cyber threat indicators (CTIs) derived from Internet communications. This information sharing is authorized notwithstanding any law – an approach sure to have unintended consequences. Both bills authorize, notwithstanding any law, countermeasures (euphemistically called "defensive measures") that can harm external systems and that amount to "hacking back." Neither bill requires adequate scrubbing of personally identifiable information unnecessary to describe or mitigate a cybersecurity threat or risk. Neither bill affirmatively addresses the cybersecurity-related conduct of the National Security Agency (NSA) that undermines cybersecurity.

However, the ***HPSCI Bill*** has particularly egregious provisions that make it look as much like ***a surveillance bill*** as a cybersecurity bill. The HPSCI bill:

- Requires that any cyber threat indicator shared with the federal government be immediately shared with the National Security Agency and other elements of the Department of Defense, thereby discouraging the very information sharing it would be enacted to foster;
- Permits cyber threat indicators shared by the private sector with the federal government to be re-purposed to investigate crimes that have nothing to do with cybersecurity, thus turning the cybersecurity program the bill creates into a surveillance program; and
- Includes no mechanism to encourage companies in the private sector to abide by the information sharing rules the bill establishes.

This analysis will begin with background information about cybersecurity and about how the bills would work. It will then point out problems in particular provisions of the bills, starting in each case with the HPSCI Bill and contrasting it to the Homeland 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. 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. 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.

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. Privacy groups have also registered their opposition.

Moreover, current law provides substantial authority to communications service providers to monitor their own networks and to share communications that traverse them for cybersecurity reasons. 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 bills take is not narrow.

The bills operate by authorizing companies to monitor information systems (or conduct "network awareness") for "cybersecurity threats" or for "cybersecurity risks" or "incidents." Information that qualifies as a "cyber threat indicator" can be shared with the federal government or among private entities. The indicators are defined using broad, functional language, rather than technical language, because of concerns that technical language would become outdated quickly. To compensate, partially, for the breadth of the information that can be shared, the bills impose some restrictions on the use of cyber-threat indicators and some obligations to strip out personal information before they are shared. The bills also authorize countermeasures against cybersecurity threats, risks, or incidents. 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

A. Expansive Use Permissions Threaten to Turn The HPSCI Bill Into a Cyber Surveillance Bill

This is perhaps the biggest fixable problem in the HPSCI Bill, but it will go unfixed. The HPSCI Bill permits companies to share "cyber threat indicators" notwithstanding any law, including all of the privacy laws. In order to cover the information that needs to be shared, the CTIs are defined broadly enough to include, for example:

- Web browsing activity of innocent users who visit a website that is subjected to a Distributed Denial of Service ("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.

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

Instead, the HPSCI Bill permits information shared for cybersecurity reason to be pooled and mined repeatedly over time not for cybersecurity, but rather for preventing, investigating, mitigating, or prosecuting fraud and ID theft, espionage, censorship, theft of trade secrets, and a host of felonies that range from running drugs with a gun, to kidnapping and carjacking.

In contrast, the Homeland Bill permits information shared for cybersecurity reasons to be used only for cybersecurity purposes, but defines them too broadly. In response to concerns CDT raised about the scope of those purposes, the Homeland Bill will be amended on the House floor to limit use of CTIs to true cybersecurity. (Amendment 33, Sponsored by Reps. Katko (R-NY), Lofrgen (D-CA), Eshoo (D-CA) and McClintock (R-CA)).

B. "Insta-Sharing" Mandate Harms Privacy and Security

Instead of requiring that cyber threat indicators be shared only with Department of Homeland Security (DHS), the HPSCI Bill permits companies to share cyber threat indicators with a wide range of federal agencies, excluding the Department of Defense and the NSA. This permission operates "notwithstanding any law" and companies are given sweeping liability protection for this information sharing. Thus, disclosure of user communications information that could be compelled under current law only based a warrant or court order can be volunteered to the government under the bill.

The HPSCI bill then requires, under policies and procedures the President would issue, that the CTIs shared with a civilian agency be shared in real-time with all "appropriate Federal agencies" including the NSA, the FBI, the Commerce Department, and many others. Sections 4(b)(2) and 11(2). Thus, while the HPSCI Bill establishes a "civilian portal" through which CTIs from the private sector would be shared, the broad "insta-sharing" mandate directs everything shared with a civilian agency right to the NSA. This sharing of cyber threat indicators may not be subject to delay, and no indicator can be modified, without "good cause." The HPSCI bill does not indicate whether application of a privacy protective technique, such as stripping out personal information unrelated to cybersecurity threat, constitutes "good cause."

Insta-sharing harms both privacy and security. First, it funnels all cyber threat indicators, including those 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 may 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 or mitigate a threat should be permitted to trump the need for speed. Third, it undermines security by discouraging companies from voluntarily sharing cyber threat indicators with the government. 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. Because the HPSCI Bill mandates insta-sharing with the NSA, companies might opt not to share CTIs at all, undercutting the key goal of the legislation.

The Homeland Bill takes a different, superior approach. It channels CTIs a private entity would like to share with the federal government to the DHS National Cybersecurity and Communications Integration Center (NCCIC), a civilian entity established for the purpose of cybersecurity information sharing. It adds a new paragraph (g) to the second Section 226 of the Homeland Security Act that requires development and implementation of automated mechanisms for the timely sharing of CTIs with many government agencies including the NSA and DOD, but it does not require insta-sharing and it does not require that every CTI shared with the NCCIC be shared with NSA and many other agencies. If information erroneously shared as a CTI is not in fact a CTI, it need not be immediately shared with a host of federal agencies, as would happen in the HPSCI bill. Privacy procedures that take a moment may be applied.

C. 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. Merely accessing another's computer without authorization is also outlawed. For certain countermeasures (euphemistically called "defense measures"), both bills remove this potential liability, thus giving a green light to conduct that would otherwise constitute malicious hacking.

Under the HPSCI Bill, a company may operate a countermeasure on its own network or on the network of a consenting entity notwithstanding any law. "Defensive measures" are defined as any action, device, technique or procedure executed on an information system that prevents or mitigates a known or suspected cybersecurity threat or security vulnerability. Section 11(6). A countermeasure placed on one information system can cause harm to another information system or to data on such other system. The Manager's Amendment removes the requirement that a countermeasure be limited to the system on which it is placed, underlining the possibility of risk to others. The provision, as amended,

- Allows countermeasures that harm other information systems or data (so long as the harm is not "substantial" – a term left undefined);
- Allows countermeasures that initiate new actions, processes, and/or procedures on another's information system;
- Allows unauthorized access to another's information system and information; and
- Allows conduct that damages or slows another's information system, so long as it does not "destroy" it, or render it "unusable or inaccessible" in whole or in part.

All of this illegal conduct that the CFAA prohibits would become lawful under these bills if done to protect one's own information system or that of a consenting entity.

Countermeasures that initiate new actions, processes or procedures, which are specifically authorized by the Manager's Amendment to the HPSCI Bill, can be quite pernicious even if they do not cause "substantial harm" to data or to an information system. For example, a company could employ a honeypot -- an attractive target on its own network -- that infects unauthorized visitors with an attribution-oriented virus or worm. The virus or worm could spread from the supposed malicious visitor to other systems that it has the ability to infect. As long as this "defensive" malware does not substantially harm, or render unusable or inaccessible the external information system, it would be permitted and could be quite invasive. It could, for example, act like the network address verification tools that the FBI uses for surveillance (the Computer Internet Protocol Address Verifiers (CIPAVs)), which can report back sensitive information about infected devices (IP addresses and persistent device identifiers such as MAC addresses), as well as information such as precise geolocation coordinates. It could even record and report back images from infected computers, and audio as well.

The Homeland Bill uses different language, but authorizes these same problematic countermeasures. Further, while the HPSCI bill prohibits countermeasures that render an external system "unusable or inaccessible (in whole or in part)," the Homeland Bill only prohibits countermeasures that render a system "unusable." This means the Homeland Bill would authorize countermeasures that render another system inaccessible, which is what ransomware does.

A cybersecurity bill should not authorize conduct prohibited by the federal anti-hacking statute. Both of these bills do. Last night, the Rules Committee ruled as "out of order" two amendments from Rep. Connelly (D-VA) that would have prevented this by making it clear that no authorized countermeasure can violate the Computer Fraud and Abuse Act. It's hard to imagine an amendment to a cybersecurity bill more "in order" than that.

D. Protection of Personal Information Falls Short

The HPSCI Bill requires the Director of National Intelligence to adopt procedures that govern information sharing. Those procedures must require that prior to sharing a cyber threat indicator, a Federal agency must remove information it *knows* at the time of sharing to be "personal information of or information identifying a specific person" not "directly" related to a cybersecurity threat. Proposed Section 111(a)(2)(E) of the National Security Act. This is insufficient because it will result in the sharing of personal information even if reasonably believed to be, but not known to be, unrelated to threat.

The HPSCI bill has also requires *companies* and state and local governmental entities to remove personal information, but under a different standard. Section 3(d). They must make reasonable efforts to review cyber threat indicators before they share them, and to remove information they "reasonably believe" to be personal information of or identifying a specific person not directly related to a cybersecurity threat. The "reasonable belief" standard is reasonable and ought to apply to Federal agency sharing as well. The House Homeland bill takes that approach. It requires that both governmental and private entities make reasonable efforts to remove or exclude information that can be used to identify specific persons that is reasonably believed at the time of sharing to be unrelated to a cybersecurity risk or incident. Proposed Section 226(i) of the Homeland Security Act.

However, standards for all sharing should have been tightened in both bills to bar the sharing of personal information not necessary to describe or mitigate a cybersecurity threat, risk, or incident, such as information about a victim of a botnet that is *related to* but not necessary to *respond to* a threat. The Rules Committee prevented votes on amendments that would have strengthened the requirement to strip out such personal information prior to sharing cyber threat indicators.

E. Absence of Mechanisms To Ensure Company Compliance

Both bills impose obligations on companies to use cyber threat indicators shared under the legislation only for cybersecurity purposes. As indicated above, both bills require companies to make some effort to strip out personal information that is unrelated to a cybersecurity threat, incident, or risk before they share a cyber threat indicator. However, neither bill includes a mechanism sufficient to adequately police or enforce these obligations. This is particularly problematic for the company-to-company information sharing that the bills authorize: governmental entities – and internet users whose information is being shared – may never learn that information shared among companies is being used for commercial purposes unrelated to cybersecurity. (CDT does not object to – and indeed, encourages – commercial use of cyber threat indicators for cybersecurity purposes.)

Both bills create a limited private right of action for people who are harmed by the federal government's intentional or willful violation of privacy rules the bills establish. This encourages governmental compliance. However, neither bill creates such a private right for individuals who are harmed by company non-compliance. Instead, both bills establish liability protection that extends to some level of non-compliance. While this will encourage voluntary information sharing, it does not sufficiently encourage compliance with privacy restrictions on voluntary information sharing. Neither bill creates a mechanism to audit company compliance with the information sharing rules.

However, the Homeland Bill does include a mechanism that could be useful to promote company compliance with information sharing rules when the company shares information with the Federal government, through the DHS NCCIC. Proposed Section 226(i) of the Homeland Security Act authorizes the NCCIC to enter into standard and negotiated information sharing agreements with private entities. Those agreements can, and should, incorporate the obligations the bill imposes to strip out personal information and to use shared information only for cybersecurity purposes. Proposed Section 226(i) also specifically authorizes the NCCIC to terminate an information sharing relationship with an entity that repeatedly and intentionally violates the information sharing rules after repeated notice of such violations

F. 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 is 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. NSA may stockpile these vulnerabilities so they can be later used in its own espionage efforts. The President's Review Group on Intelligence and Communications Technologies recommended that such vulnerabilities be quickly disclosed to software companies with rare exception. Congress should have used the

occasion of consideration of cybersecurity information sharing legislation to require this disclosure, but neither bill addresses it.

III. Conclusion

While cybersecurity threats continue to be a significant problem warranting Congressional action, the cybersecurity information sharing bills the House is considering go well beyond authorizing necessary conduct and in fact, authorize dangerous conduct harmful to both security and privacy. The broad use permissions in the HPSCI bill suggest that the legislation is as much about surveillance as it is about cybersecurity. We urge members to oppose both bills.