KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE
www.cdt.org
CENTER FOR DEMOCRACY
& TECHNOLOGY

Cyber-Surveillance Bill to Move Forward, Secretly

March 4, 2015

The Senate Intelligence Committee is expected to consider the Cybersecurity Information Sharing Act (CISA) in a closed Committee meeting as soon as the week of March 9. While it will mark up the bill in secret and thereby deny the public an opportunity to better understand the risks the legislation poses, to its credit, the Committee has circulated for comment a discussion draft of the bill, and the draft has been publicly posted to the Internet, including on the Politico website. This document analyzes the discussion draft, as does a sign-on letter issued by prominent security experts, and CDT and other civil society groups. CDT will release a more comprehensive analysis after the secret mark up of CISA.

Though CISA includes some improvements from last year's version of the legislation, every major concern we expressed about the 2014 version of the bill is also a major concern with the 2015 version. 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 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 overly broad anti-terrorism and law enforcement purposes;

- 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 reckless conduct that runs counter to the cybersecurity purpose of the bill; and

- Fails to affirmatively address the cybersecurity-related conduct of the NSA that actually undermines cybersecurity.

Rather than move forward with legislation that could actually worsen the very problems it was drafted to solve, CDT believes that Congress should focus on reining in NSA surveillance. We outline below five major concerns with the legislation:

I. Expansive 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. 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
- 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 the breadth of information that can be shared is quite wide, the purpose of the information sharing and use of the information shared should be narrow, and specifically focused on cybersecurity.

Instead, the bill permits companies to share these cyber threat indicators not just for cybersecurity purposes, but for any purpose permitted under the bill, including broad law enforcement and anti-terrorism 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, many felonies, fraud and ID theft, espionage, censorship and theft of trade secrets. Section 5(d)(5). The government views all Americans' communications metadata as relevant to counter terrorism investigations (as evidenced by the ongoing telephone metadata program and the now abandoned Internet metadata bulk collection program). Communications metadata collected under this bill would be viewed the same problematic way.

II. "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, anti-terrorism, or crime fighting purposes. Section 4(c). Thus, disclosure of user communications information that could be done previously (under current law) only based on a warrant or court order could now 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 the share CTIs with DHS, or when they share under certain exceptions in the bill. Section 4(c). However, DHS must share immediately or in real time the CTIs it receives with all "appropriate government agencies" including the NSA, the FBI, the Commerce Department and many others. Section 2(3). Thus, while the bill establishes a "civilian portal" through which CTIs from the private sector would 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 it the guidelines must reflect the insta-sharing mandate, and they need not even be in place before insta-sharing begins.

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. Because CISA mandates insta-sharing with the NSA, companies might opt not to share CTIs at all, undercutting the key goal of the legislation.

III. 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" is any action, device, technique or procedure used on one's own information system or on information on such system, which prevents or mitigates a suspected cybersecurity threat. As a result, countermeasures that are deployed for legitimate reasons on one network that damage or destroy data on another's network, or damage or destroy another's network itself, would become lawful under the bill. CISA protects the deployment of such countermeasures so long as they are deployed without intent to harm another's information system. Thus, a person who recklessly deploys such a countermeasure on his own network that destroys another's information system is acting lawfully. A person who deploys a countermeasure on his own network *intending* that it destroys data on another's network, as opposed to the network itself, is also acting lawfully under the bill. Despite the CFAA, neither would 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.

IV. Protection of Personal Information Falls Short:

The bill requires companies to review CTI's before sharing them, and to strip out

before sharing personal information that the company "knows at the time of sharing to be … not directly related to a cybersecurity threat." The 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. 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 identify or describe cyber threats, based on guidelines DHS would issue.

V. Pro 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 world wide. 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 use this opportunity, while considering cybersecurity information sharing legislation, to require this disclosure.

Improvements In the Bill Are Insufficient

Because CISA broadly expands the collection and use of personal information for anti-terrorism and criminal investigative activities, it has overall moved backwards in terms of privacy and civil liberties protections as compared to last year. However, some important improvements have been made and should not be ignored:

- The bill now excludes mere violations of terms of service and licensing agreements from the definition of cybersecurity threats. This will largely prevent CFAA prosecutions of terms of service violations based solely on information shared under the bill. The bill should similarly exclude violation of net neutrality rules from conduct that constitutes a cybersecurity threat.

- The bill tightens the definition of cyber threat indicator by limiting it to information "necessary to describe or identify" a particular activity that may pose a threat. Last year, CISA permitted CTIs that merely "indicate" a threat.

- Unlike last year's bill, CISA requires a company to review CTIs for irrelevant personal information prior to sharing the CTI (though, as noted above, the review can be cursory).

- Unlike last year's legislation, the bill does not expand surveillance by granting companies blanket liability protection for sharing CTIs with the FBI for malware

analysis.

- The bill requires the government to notify companies when the government later determines that information shared as a CTI was in fact not a CTI and was shared in error. This will diminish further errant information sharing.
- CISA now bars the government from conditioning federal grants and contracts on sharing of CTIs.

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 harm to privacy that is not necessary. Its broad use permissions suggest that the legislation is as much about surveillance as it is about cybersecurity. We urge the Senate Intelligence Committee to make significant improvements before reporting the bill.