UPDATED – Analysis of the Cybersecurity Information Sharing Act of 2014: A Major Step Back on Privacy

Robyn Greene, Policy Counsel

The Cybersecurity Information Sharing Act of 2014 (CISA) (S. 2588)[i] takes a significant step back from the privacy protections that were included in the last cybersecurity information-sharing bill considered by the Senate, the Cybersecurity Act of 2012 (S. 3414).[ii] It also fails to address the significant concerns that have been raised over the last year as Americans have learned about the scope and breadth of the government's surveillance and cyber operations.

In its current form, this legislation would, among other things, create an expansive new information-sharing program that would give the National Security Agency (NSA) access to vast quantities of personal information, authorize private entities to engage in an array of countermeasures that could potentially harm average Internet users, fail to adequately protect individuals' personal information, and absolve companies of all liability for harms resulting from negligent or improper information-sharing, and legitimate the NSA's practice of stockpiling known vulnerabilities for its own use rather than responsibly disclosing them.

CISA's Information-Sharing Procedures Allow Direct Military Involvement in Civilian Cybersecurity Programs: CISA would authorize automatic information-sharing with the NSA, because under its information-sharing provisions, the Department of Homeland Security (DHS) is required to establish procedures for receiving cyber threat indicators that enable entities within the Department of Defense (DOD), such as the NSA and the Office of the Director of National Intelligence, to access the information simultaneous with receipt by DHS (CISA, Sec. 5(c)(1)(C)). Additionally, the government's procedures prohibit any delay or interference with the dissemination of cyber threat indicators (CISA, Sec. 5(a)(3)(ii)).

Thus, DHS would serve merely as a portal through which DOD entities receive cyber threat indicators, and there would be no functional distinction between sharing with a civilian agency and sharing directly with the NSA. Additionally, the procedures require that companies share information in an "electronic format," which is vaguely defined to include "a real time, automated process between information systems" (CISA, Sec. 2(8), *and* Sec. 5(c)(1)(A)). This may be interpreted to authorize the government to gain direct access to a company's information systems to receive cyber threat indicators. Finally, DHS and DOJ lack independence in establishing their procedures and must coordinate with, rather than merely consult, military and intelligence agencies.

Instead, a civilian agency should be in charge of receiving cyber threat indicators, and only share them with military or intelligence agencies when those indicators are necessary to address a significant cyber threat. The Cybersecurity Act of 2012 (CSA 2012) had a much more civilian-centric process for information-sharing from the private sector to government. It would have created a cybersecurity exchange, either within a civilian federal entity or a non-federal entity, to receive and distribute threat indicators, with procedures to share threat indicators in "as close to real time as possible with appropriate" federal and non-federal entities (CSA 2012, Sec. 703(a)).

CISA Authorizes Excessive Information-Sharing and Countermeasures: CISA would authorize an overly expansive new information-sharing program because it fails to reasonably limit the instances in which information can be shared, what kinds of information can be shared, and what can be done to mitigate a cybersecurity threat, based on overbroad definitions of the terms "cybersecurity threat," "cyber threat indicator," and "countermeasure."

CISA authorizes information-sharing with the government about any "cybersecurity threat," which is defined as any action that "may result in an unauthorized effort to adversely impact" a system (CISA, Sec. 2(6)). This extremely permissive standard for likelihood of an attack requires only that there is a vague possibility that an action will pose a threat. Additionally, the concept of "adverse impact" is too broad, and could cover a wide variety of inconsequential impacts that would not pose serious threats to an entity's network or system. In contrast, the Cybersecurity Act of 2012 more tightly defined "cybersecurity threat" as "any action that may result in unauthorized access to, exfiltration of, manipulation of, harm of, or impairment to the integrity, confidentiality, or availability of an information system or information that is stored on, processed by, or transiting an information system," except all actions protected by the First Amendment and terms of service violations (CSA 2012, Sec. 708(6)). That narrower definition, when combined with the other privacy protections included in the 2012 bill, posed far less of a threat to privacy.

Additionally, the types of information that can be shared with the government, "cyber threat indicators," are defined too broadly, and include anything that is "necessary to indicate, describe, or identify" a cyber threat, or "any other attribute" of the threat (CISA Sec. 2(7)). Therefore any and every part of a communication that falls within the bill's overbroad definition of "cybersecurity threat"—including the content of that communication, or any metadata associated with it—could be shared with the government, since it could be considered to "indicate" or "describe" the threat, or fit into the catchall "any other attribute" category. Instead, the bill should allow sharing only of cyber threat indicators that are reasonably necessary to identify or respond to a narrowly defined cybersecurity threat, and from which "reasonable efforts were made" to remove personally identifiable information, as was the case in the Cybersecurity Act of 2012 (CSA 2012, Sec. 708(7)).

Finally, once an entity identifies a cyber threat, CISA would allow that entity to respond to that threat with an overbroad set of countermeasures, including any "action, device, procedure, technique, or other measure" that prevents or mitigates a known, or even just a suspected, threat or vulnerability (CISA, Sec. 2(4)). Terms like "procedure," "device," and any "other measure" are so broad that they may be interpreted to authorize any possible countermeasure, including inserting malware or spyware on someone else's computer, including even before they have attacked, as a means of "prevention." The bill exempts companies from all other provisions of law that would prohibit such hack-back activities, and requires only that these countermeasures be "applied to" information systems of the countering entity or those of parties who have consented to the countermeasures – there is no requirement that the effects of the countermeasures be contained within those systems (CISA, Sec. 4(b)). Thus, the impact of countermeasures authorized under this bill could be far reaching, and could inadvertently affect countless innocent Internet users who are wholly unrelated to the cybersecurity threat. This provision should be substantially narrowed or removed entirely.

CISA Authorizes Sharing of Unnecessary Personally Identifiable Information (PII): CISA requires only that private sector and federal entities sharing cyber threat indicators must, before sharing, "remove any information contained within such indicators 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" (CISA, Sec. 4(d)(2)). However, because this provision only requires stripping out PII that the sharing entity "knows" is PII at the time of sharing, it creates no affirmative duty on the party of the sharing entity to establish a process or review to try to identify and remove unnecessary personal information, and could result in a significant amount of personal information being unnecessarily shared. Thus, it provides insufficient protection — especially when compared to the Cybersecurity Act of 2012, which included in its definition of "cyber threat indicator" a requirement to make reasonable efforts to strip all PII (CSA 2012, Sec. 708(7)), whether initially known or not, and whether belonging to a US person or not.

CISA Inadequately Limits Government Use of Information It Receives: CISA authorizes the federal government to use cyber threat indicators it receives in investigations and prosecutions that are far outside the scope of cyber crimes. The federal government may use that information to prevent, investigate, or prosecute not just violations of the Computer Fraud and Abuse Act but also ID document and authentication feature fraud, aggravated ID theft, access device fraud, economic espionage, theft of trade secrets, and violation the Espionage Act, which could have serious implications for whistleblowers who are seeking to disclose abusive or illegal activity or journalists reporting on those abuses (Sec. 5(d)(5)(A)). Use authorizations for state, local and tribal governments were narrowed from the original bill such that they can use information they receive for the prevention investigation, or prosecution of any computer crime, so long as they obtain the consent of the entity that provided the information, where before, they could use the information for any law enforcement purpose (Sec. 4(d)(4)(A)).

Instead and at most, CISA should only allow law enforcement uses of cyber threat indicators to protect information systems from cybersecurity threats, and for investigations and prosecutions that pertain to cybersecurity crimes, the imminent threat of death or bodily injury, or a serious threat to minors, as was the case in the Cybersecurity Act of 2012 (CSA 2012, Sec. 704(g)(2)(B)).

CISA Authorizes Companies to Monitor Their Customers' Activities: The Electronic Communications Privacy Act (ECPA) already allows private entities to intercept communications made over their networks in order to protect their right and property or combat trespassers, and to access the data that they store. CISA undermines the reasonable privacy protections included in those authorities, as well as any other law that protects electronic privacy, by creating a vague new authority for private entities to "monitor" any information "stored on, processed by or transiting" their information systems. (The verb "monitor", a new term in the law of electronic privacy, is circularly defined as the act of "obtain[ing], identify[ing], or otherwise possess[ing] information that is stored on, processed by, or transiting an information system." (CISA, Sec. 2(15)). This authority is redundant if read reasonably and dangerous if read unreasonably, and should be cut (CISA, Sec. 4(a)).

CISA's Liability Protections Leave Customers No Recourse If They Are Wrongly Harmed by Information-Sharing: CISA absolves companies of any liability associated with sharing or monitoring of information pursuant to the Act, except for actions that constitute gross negligence. A good faith reliance that a company's conduct was authorized under this Act constitutes a complete defense (CISA, Sec. 6). This provision would preclude causes of action for violations of the

Computer Fraud and Abuse Act as well as privacy statutes such as the Stored Communications Act and Wiretap Act portions of ECPA. CISA's liability protections should be narrowed to ensure that there is reasonable recourse for those harmed in the event that a company unnecessarily monitors or shares their personal information.

Stockpiling of Vulnerabilities and Internet Security: CISA includes a rule of construction that nothing in the bill can be interpreted to modify the authority of the Federal Government "to protect sources and methods and the security of the United States" (CISA, Sec. 8(c)(3)). This language highlights a significant problem that was not contemplated in the Cybersecurity Act of 2012 – that the government is stockpiling vulnerabilities for its own investigative use rather than responsibly disclosing them. The government may interpret this language to authorize it to stockpile vulnerabilities discovered or purchased by the NSA that it would otherwise disclose to companies under the information-sharing procedures required under this bill. These procedures, developed by the DNI, DHS Secretary, and Attorney General, in consultation with the heads of appropriate agencies, are also required to be established consistent with protection of sources and methods and national security (CISA, Sec. 3(a)).

This type of stockpiling can have substantial negative consequences for Internet security, as the President's Review Group noted in its final report: "In almost all instances, for widely used code, it is in the national interest to eliminate software vulnerabilities rather than to use them for US intelligence collection.... Eliminating the vulnerabilities – 'patching' them – strengthens the security of US Government, critical infrastructure, and other computer systems."[iii] When news of the Heartbleed vulnerability broke, the Administration responded to allegations that the NSA knew about the Heartbleed vulnerability by indicating that it already has an interagency process called the "vulnerabilities equities process," which establishes when to disclose vulnerabilities.[iv] However, this process is almost completely opaque, and the Administration indicated that it had "reinvigorated" the process in response to the President's Review Group's report, suggesting that it hadn't been strongly implemented or consistently followed before the report was released.

The White House and the Intelligence Community have both stated that it is already U.S. policy to disclose vulnerabilities except in the narrowest of cases. This is a policy that the President's Review Group strongly supported, and that should be codified in any information-sharing bill in order to ensure that it is followed.

---

[i] Cybersecurity Information Sharing Act of 2014, 113th Cong. (2014), *available at* http://www.feinstein.senate.gov/public/index.cfm/files/serve/?File_id=7aa01948-f9a5-45e0-ae00-60e1606e5f5f.

[ii] S. 3414, Cybersecurity Act of 2012, 112th Cong. (2012), *available at* https://beta.congress.gov/112/bills/s3414/BILLS-112s3414pcs.pdf.

[iii] President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World* 220(Dec. 2013), http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf [hereinafter President's Review Group Report].

[iv] Michael Daniel, Special Assistant to the President and Cybersecurity Coordinator, *Heartbleed: Understanding When We Disclose Cyber Vulnerabilities*, April 28, 2014, http://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities. *See also* Press Release, Office of the Director of National Intelligence Public Affairs Office, Statement on Bloomberg News story that NSA knew about the "Heartbleed bug" flaw and regularly used it to gather critical intelligence" (April 11, 2014)(on file with author), *available at* http://icontherecord.tumblr.com/post/82416436703/statement-on-bloomberg-news-story-that-nsa-knew; *and* David E. Sanger, *Obama Lets N.S.A. Exploit Some Internet Flaws, Officials Say*, N.Y. TIMES, April 12, 2014, http://www.nytimes.com/2014/04/13/us/politics/obama-lets-nsa-exploit-some-internet-flaws-officials-say.html?_r=0.