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

ANALYSIS OF FEINSTEIN-CHAMBLISS CYBERSECURITY INFORMATION SHARING ACT OF 2014 DISCUSSION DRAFT RELEASED JUNE 17, 2014

June 24, 2014

This is an analysis of the Cybersecurity Information Sharing Act of 2014, which was released to the public as a discussion draft on June 17, 2014. As compared to the Cybersecurity Act the Senate considered in July, 2012, the bill would dismantle many hard-fought privacy protections that had improved that legislation as it moved to the Senate floor. Indeed, the bill seems to disregard the revelations about surveillance conducted by the National Security Agency both within the U.S. and includes no new civil liberties protections responsive to those disclosures. As we explain more fully below, the bill:

- Fails to address recently-disclosed cybersecurity-related conduct of the National Security Agency (NSA), some of which undermines cybersecurity;
- Requires that any cyber threat indicators a company shares with many federal agencies will be immediately shared with multiple other federal agencies, including elements of the Department of Defense ("DOD"), which includes the NSA, thereby discouraging the very information sharing it would be enacted to permit;
- Risks turning the cybersecurity program it creates into a back door wiretap by authorizing use of cyber threat indicators for overly broad law enforcement purposes;
- Does not effectively require that personally identifiable information irrelevant to a cyber threat indicator be removed before information about the threat indicator is shared; and
- Authorizes broadly-defined cybersecurity countermeasures and provides a good faith defense against claims that a countermeasure unlawfully damaged a network or stored information, encouraging reckless conduct that runs counter to the cybersecurity purpose of the bill.

The leading co-sponsors of the bill, Senator Diane Feinstein (D-CA) and Senator Saxby Chambliss (R-GA) are the Chair and Vice-Chair of the Senate Intelligence Committee. It held a hearing on the bill on June 19, 2014 and is expected to mark up the bill on June 26.

Snowden Revelations Ignored in the Bill

As best we can tell, the bill addresses none of the Snowden revelations about NSA surveillance, and addressing them should be a pre-requisite to advancing cybersecurity legislation. Instead, it would funnel more private communications

communications and communications information to the NSA. The bill borrows from the 2012 Cybersecurity Act, S. 3414 (before the July, 2012 privacy amendments that were adopted as the bill moved to the Senate floor), the McCain-Chambliss SECURE IT Act, S. 3342, as reintroduced on June 27, 2012, and the House cybersecurity bill, CISPA, H.R. 624, as passed by the House on April 17, 2013.

Since those bills were considered, the public has learned much about the extent to which the NSA and other governmental agencies have stretched the meaning of statutory provisions in order to gather information in ways that in our view, the law did not permit. This calls for corrective actions to rein in the NSA that do not appear in this draft. In particular, any cybersecurity legislation should adopt a number of reforms, outlined below, that pertain directly to NSA's cybersecurity activities, most of which are drawn from recommendations of the President's Review Group (http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf):

- There should be a statutory prohibition on stockpiling of zero days (with a narrow safety valve exception) so a software maker can be promptly notified and the security vulnerability can be patched (Review Group Recommendation 30 on p. 219);
- In order to restore trust, the bill should begin the process of removing the information assurance function from NSA and putting it at DHS, which is already building an information assurance capability (Review Group also recommended removing information assurance from NSA, but they would have put it at another DOD element. Recommendation 25 on p. 191)
- Repeal the statutory provision that requires the National Institute of Standards ("NIST") to consult with NSA in the encryption standards setting process (Rep. Grayson's amendment, described and linked to here: https://cdt.org/blog/house-committee-moves-to-break-statutory-link-between-nsa-and-nist/); and
- Create a statutory bar to inserting vulnerabilities into any generally available commercial software (Review Group recommendation 29, p. 216).
-

These measures should be added to the cybersecurity legislation. We now turn to an analysis of the provisions of the bill.

I. Information Sharing on Automatic

The bill requires that cyber threat indicators a company shares voluntarily and in an electronic format with the Department of Homeland Security will automatically and immediately be shared with the NSA and Cybercommand, with other elements of the Department of Defense, with the Department of Energy, the Department of Commerce, the Department of Treasury, and the Office of the Director of National Intelligence. This in our view is a non-starter. We do not object to the automated sharing of cyber threat indicators, but rather, the entities with which they are shared and the circumstances under which they are shared should be carefully thought out and either spelled out in the bill or spelled out in subsequently issued policies and procedures designed to protect privacy and civil liberties.

Automatic sharing of cyber threat indicators – many of which will contain communications content and personally identifiable information – is bad for privacy because the recipients include a military intelligence agency with a recently exposed track record of unlawful use of

Section 215 to conduct surveillance in the U.S. It is particularly problematic in the context of continuous monitoring [https://cdt.org/blog/continuous-monitoring-big-data-and-concerns-with-cispa/]: companies will continuously monitor their networks and can, under the bill, share information automatically with the government. Requiring the governmental entity that receives that information to automatically share it with NSA and other elements of the DOD may discourage some companies from voluntarily participating in the information sharing regime the bill is intended to encourage. U.S. cloud providers are being asked by their clients in Europe for assurance that data the customers store in the cloud will not be shared with the NSA. This provision would make it impossible for a company to share cyber threat indicators with the government and make that promise to its customers.

Instead, companies in the private civilian sector should be encouraged to share cyber threat indicators with DHS, which would then adopt privacy protective policies and procedures about what information should be shared with DOD elements, DOJ and other federal entities. The bill does enhance the role of DHS in the civilian cybersecurity program. It gives DHS 90 days to develop a capability and process to receive cyber threat indicators in electronic format. This is a step in the right direction because it affirms a central role in cybersecurity for DHS. The auto-sharing provision, however, works against this, requiring DHS to share whatever it receives immediately with NSA and other elements of DOD.

II. Policies and Procedures for Information Sharing

The bill requires the U.S. Attorney General, in coordination with the head of DOD, DHS, DOE, ODNI, and DOC, to develop interim and final policies and procedures for sharing cyber threat indicators and countermeasures within the government. The policies and procedures provision needs substantial changes.

- The policies and procedures should include the civil liberties policies and procedures that the Attorney General is separately required to adopt. Having separate guidelines for privacy risks confusion or ignorance of the privacy requirements.
- The policies and procedures ought to require that information sharing under the bill better comport with principles of fair information practices as articulated by DHS Privacy Office under the Bush Administration. http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf. The July, 2012 Cybersecurity Act made a good start at this and the language from that bill could be used as the starting point.
- As mentioned above, the information sharing policies and procedures should be issued by DHS in coordination with the other federal entities.
- The policies and procedures should require timely destruction of information that is not known to be related to a cyber security threat and should require such assessment by a date certain. The current draft has a different default: it permits indefinite retention of information unless it becomes known that it is not directly related to a use authorized in the Act.
- The policies and procedures should be enforceable by those who suffer harm as a result of violation of the policies and procedures. The draft requires that cyber threat indicators and countermeasures be used and shared by the federal government in accordance with the policies and procedures that govern such dissemination and use, but it does not establish a remedy for those who suffer damage from unlawful use or dissemination.

The July 2012 Cybersecurity Act created a private right of action against the government if it violates the information dissemination and use restrictions.

While it is sometimes critically import that cyber threat information be shared quickly, sometimes being careful is more important than being quick. The bill does not allow for that. Instead, for cyber threat indicators and countermeasures DHS receives in electronic format, the policies and procedures that govern the sharing of that information must ensure that they are shared without any delay or interference "or any action that could impede real-time receipt" by the NSA and other elements of the federal government. This means a privacy-protective procedure, such as stripping out personally identifiable information that is not necessary to describe threat, cannot be part of the procedures if they take any time at all. While we believe that much of this can be automated, the guidelines should allow for the possibility or protective procedures that are not immediate. Nor, under the draft bill, can human review be permitted even to ensure the quality of the data flow. For information shared in other than an electronic format, any delay or interference cannot be "unreasonable." We would suggest, instead, a requirement of "prompt" information sharing, in real time or in as reasonably close to real time as is feasible.

III. Removal of Personal Information is Insufficient

Removal from cyber threat indicators and countermeasures, before dissemination, of personally identifiable information not relevant to a cyber security threat is critical to the effort to protect privacy in the context of this legislation. The bill should require any entity, including federal entities, to remove personally identifiable information from any cyber threat indicator or countermeasure before sharing the indicator or countermeasure, except when the PII is ***necessary*** to describe the threat or countermeasure. For example, IP address plus port number may be personally identifiable information; it can be shared in the cybersecurity context when it is necessary to describe the cybersecurity threat, as it often is.

The July, 2012 Cybersecurity Act had good language in this regard. It built the requirement to make reasonable efforts to remove PII right into the definition of cyber threat indicator so a sharing entity would not obtain the benefits of bill (such as the ability to share notwithstanding any law, and liability protection) unless it made reasonable efforts to remove irrelevant PII from the cyber threat indicators it shared. Likewise, the requirement to make reasonable efforts to remove irrelevant PII from a countermeasure before it is shared could be built right into the definition of countermeasure.

The draft bill takes a different approach that in practice will offer little protection.
It adopts a willful blindness approach: if the sharing entity does not know whether a cyber threat indicator includes "personal information" irrelevant to the threat, the sharing entity need not look for it, and can share the cyber threat indicator with the irrelevant personal information it would have found had it looked. "Personal information" is left undefined. Moreover, for the provision to offer any protection, the sharing entity would have to "know" that the personal information pertains to a US citizen or lawful permanent resident (a "U.S. person"). In most contexts, the sharing entity, even if it knows there is personal information, will not "know" whose personal information it is, and in particular, whether the personal information pertains to a U.S. person.

The provision is also inconsistent with the spirit of Section 4(a) of Presidential Policy Directive 28 ("PPD-28"), which requires, in the context of gathering signals intelligence, that to the

maximum extent feasible consistent with the national security, non-US persons should enjoy the benefits of the same restrictions on dissemination of PII about them that that US persons enjoy.

Finally, The provision about removing PII does not even extend to the cyber threat indicators that the federal government shares. It only extends to an "entity" which is defined to exclude federal entities. This appears to be a minor drafting error that is easy to correct.

IV. Overbroad Use Permissions

Information shared, notwithstanding any law, for cybersecurity purposes should be used only for those purposes. Use for law enforcement or national security or counterintelligence reasons that are unrelated to cybersecurity purposes risks of turning the cybersecurity information sharing program that the bill authorizes into a backdoor wiretap.

The July, 2012 Cybersecurity Act had reasonable use restrictions. Under Section 704 of that bill, cyber threat indicators could be disclosed to federal, state and local law enforcement agencies, and be used by them, to protect information systems from cybersecurity threats, to prosecute (defined) cybersecurity crimes, to protect individuals from imminent threat of death or serious bodily harm and to protect minors from any serious threat, including sexual exploitation. The draft bill, in contrast, permits state and local law enforcement entities to use the cyber threat information shared with them to investigate and prosecute *any crime*.

It permits federal law enforcement use for cybersecurity purposes and to protect against imminent threat of death or serious bodily harm, but also to prosecute violations of the Computer Fraud and Abuse Act (18 USC Section 1030), ID fraud (18 USC Section 1028), fraudulently producing and using and sharing passwords, account numbers and personal identification numbers (18 USC 1029), espionage and censorship (18 USC Chapter 37) and theft, copying and trafficking in trade secrets (18 USC Chapter 90).

The draft bill bars private entities that receive cyber threat indicators from using them for purposes not authorized in the draft bill. However, the bill provides no remedy for a party injured by such unauthorized use of cyber threat indicators. To ensure that this proscription is followed, the bill should provide a right of action to parties injured by unauthorized use.

V. Monitoring and Countermeasures

It is not clear that a broad exception for monitoring and countermeasures is necessary and creating one could be unwise. The Electronic Communications Privacy Act and the Wiretap Act already permit providers and their agents to intercept, use and disclose communications (including content) in order to protect their networks. An amendment to permit such interception use and disclosure to protect the networks of others is all this is needed.

"Countermeasure" is defined overly broadly in the bill: any action, device, measure or procedure applied to an information system or to information, that prevents or mitigates a cybersecurity threat or security vulnerability, fits the bill. The bill authorizes the application of countermeasures notwithstanding any other law. The definition of countermeasure in the July 2012 Cybersecurity Act was much tighter and less likely to unintended results. It limited the countermeasures to actions to modify, redirect or block on networks in order to protect them.

The bill wisely limits the countermeasures it authorizes to those that are applied to the information systems of a private entity, or of another party with express consent. However, this still leaves the scope of the countermeasures authorization unclear. A countermeasure employed on one network can have effects on another, and they can be extreme, and include destruction of valuable data. To avoid authorizing such conduct and extending liability protection to such conduct, the bill ought to employ an effects test: countermeasures are not protected if, though applied to one network, have effect on another or on information stored on another network.

Even if an effects test is used, the provision still raises serious questions. It shifts responsibility for employment of reckless and careless countermeasures from the security vendor who employs them to the party who hired the vendor to provide protection. For example, if a security vendor employs a countermeasure device or process that errantly destroys or renders useless a $10 million database that its client hired the vendor to protect, the broad liability protections mean that the client cannot effectively pursue a remedy in court, even if the contract between them makes it clear that the vendor should pay. The vendor would have a good faith defense to the claim that would result in dismissal of the case seeking damages.
This encourages careless and reckless countermeasures, which is counterproductive.
Finally, the provision could be read to invite Internet Service Providers to extract in terms of service user consent to the use of countermeasures on the users' own computers. Under the draft, an individual is a "private entity" and such entities can give consent to the operation by third parties of countermeasures on the private entity's computer. This is not to say that users should never be able to grant such consent; rather, such consent in the case of individual users should be granted knowingly, on a case-by-case basis, after the user is fully informed and specifically assents to the use of such countermeasures, rather than permitting blanket consent to be buried in lengthy terms of service.

VI. Net Neutrality and Terms of Service Implications

The draft bill's definition of cybersecurity threat is overbroad and includes "any action" that may result in an unauthorized effort to adversely impact the security, confidentiality and availability of an information system or of information stored on such system. Countermeasures can be employed against such threats. This would appear, for example, to permit an operator to slow down some traffic to make other information is processes more available to users, raising serious net neutrality issues. A contractual commitment not to do so would be unenforceable under the liability protection provisions of the bill. The July 2012 Cybersecurity Act included language designed to prevent this result and it should be incorporated. In addition, language from the July 2012 Cybersecurity Act that was designed to ensure that mere violations of terms of service that result in unauthorized access are not considered cyber security threats should also be built in.

VII. Cyber Threat Indicator

A tight definition of cyber threat indicators helps address other issues in the bill, such as concerns about the lax use restrictions and overbroad liability protection.
A cyber threat indicator should include only information "reasonably necessary" to describe a threat, rather than the more amorphous language in the bill about "indicating" a threat. The July

2012 Cybersecurity used this narrower language and it should be adopted here. We have continuing objections to the catch all cyber threat indicator "any other attribute of a cybersecurity threat" unless disclosure is prohibited by law because it could have unintended results.

Conclusion

Because the bill raises significant privacy concerns, could have unintended effects including discouraging the information sharing it should encourage, the Center for Democracy & Technology opposes the bill in its current form. We urge, and have suggested, significant changes that would address these concerns. Many of those changes can be lifted directly from the July, 2012 Cybersecurity Act. In addition, the bill fails to address the disclosures by NSA cybersecurity practices that the President's Review Group recommended; those changes should also be incorporated before the bill moves forward.

For further information, please contact CDT's Gregory T. Nojeim, Director of the Project on Freedom, Security and Technology (gnojeim@cdt.org, 202/637-9800) or Jake Laperruque, Fellow on Privacy, Surveillance and Security (jake@cdt.org).