KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 Eye Street, NW
Suite 1100
Washington, DC 20006

Information Sharing, Monitoring, and Countermeasures in the Cybersecurity Act, S. 2105, and the SECURE IT Act, S. 2151

March 28, 2012

The Cybersecurity Act of 2012, S. 2105 ("Lieberman-Collins"), and SECURE IT, S. 2151 ("McCain"), both have broadly written provisions that would authorize ISPs and other companies to:

(i) share private communications with the National Security Agency and other federal entities, or with any other agency of the federal government designated by the Department of Homeland Security;
(ii) monitor private communications passing over their networks; and
(iii) employ countermeasures against Internet traffic.

The new authorities would trump existing privacy laws.[1]

Cybersecurity is important to all Internet users because it can make the Internet a safer place to shop, conduct business, communicate with others and find information. While CDT believes that legislation is necessary to help companies and governmental agencies share cybersecurity information, we oppose the information sharing provisions of both bills because they permit too much information to flow to the NSA.[2] In addition, we oppose the monitoring and countermeasures provisions of the Cybersecurity Act and SECURE IT.

The information sharing provisions of both bills should be narrowed to protect privacy and to ensure that the NSA does not come to dominate federal cybersecurity efforts directed at the private sector. The information sharing language in the McCain bill is particularly problematic: it expressly allows sharing with the NSA, and it expressly allows ISPs to monitor for, and share with the NSA, any "information that would foster situational awareness of the United States security posture."

The ill-defined authorities to monitor communications and employ countermeasures have been examined too late in the legislative process to be adequately considered before

---

[1] In Lieberman-Collins, the new authorities to monitor and employ countermeasures would trump existing electronic surveillance statutes that would otherwise prohibit this conduct to protect privacy. In the McCain bill, the monitoring and countermeasures provisions would trump all laws without exception. In both Lieberman-Collins and McCain, the information sharing authority trumps the surveillance privacy laws and all others without exception.

[2] In the House, Reps. Bono Mack and Blackburn have introduced their version of SECURE IT, H.R. 4262, and there are two other House bills on information sharing as well -- the bill sponsored by Chairman Rogers, H.R. 3523, has equally broad language on monitoring and even broader language on information sharing, but the bill sponsored by Rep. Lungren, H.R. 3674, avoids such missteps by taking a more carefully targeted approach.

these important bills move to the Senate floor. While multiple congressional hearings have focused on information sharing, there has been precious little public discussion of any need to dramatically expand the already substantial authorities companies already have to monitor Internet activity and operate countermeasures against Internet users' traffic. The new monitoring and countermeasures authorities could disrupt existing cybersecurity initiatives in the private sector. They could be used by government agencies to push industry in a direction that would be desirable from neither a security nor a civil liberties standpoint. They are especially troubling in light of the campaign by the NSA to acquire more access to private sector communications streams.[3] The monitoring and countermeasures provisions ought to be dropped entirely. They constitute only a small part of either bill, but leaving them in could drag down the entire package.

Below, we analyze each of these provisions of both bills, starting in each case with the Lieberman-Collins Cybersecurity Act because it is the bill that Senate leadership is most likely to bring to the Senate floor.

I. Information Sharing

Top line: The Cybersecurity Act and SECURE IT permit more private communications information to be shared than is necessary; permit information to be shared with military and intelligence agencies – thus inviting a shift from civilian to military control of government cybersecurity efforts aimed at the private sector; allow the information shared to be used for general law enforcement purposes rather than just cybersecurity; and have insufficient accountability measures to ensure that the information sharing rules are followed. Substantial changes are needed. By each of these measures, the SECURE IT Act is worse than the Cybersecurity Act. In particular, SECURE IT permits information shared for cybersecurity reasons to be used broadly for national security reasons, effectively establishing a new intelligence surveillance program.

CDT has long supported a narrow, targeted amendment to the electronic surveillance statutes to facilitate the sharing of cyber attack information among private entities and between the government and the private sector. An amendment to existing law is appropriate, for example, because a network operator may benefit from receiving information about a cyber attack on another operator's network and current law may not allow such sharing. However, because cybersecurity information sharing involves the sharing of information derived from private communications, it must be carefully controlled. Controls circle around these key questions:

- What information can be shared?
- With whom?
- For what purpose can the information be shared?

[3] Ellen Nakashima, "White House, NSA Weigh Cybersecurity, Personal Privacy," The Washington Post (February 27, 2012) http://www.washingtonpost.com/world/national-security/white-house-nsa-weigh-cyber-security-personal-privacy/2012/02/07/gIQA8HmKeR_story.html; and James Bamford, "The NSA IS Building the Country's Biggest Spy Center (Watch What You Say)," Wired (Mar. 15, 2012) http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1.

- For what purpose can it be used?
- What accountability measures tend to ensure that these information sharing rules are followed?

The answers to these questions are particularly important because the information sharing language of each of the major cybersecurity bills permits information sharing "notwithstanding any law." This means the bills trump all privacy laws – including the Electronic Communications Privacy Act, the Wiretap Act, the Foreign Intelligence Surveillance Act, and the Privacy Act – and all other laws without exception.

A. What Information Can Be Shared?

The Cybersecurity Act defines the "cybersecurity threat indicators" that can be shared fairly well[4] by listing specific categories of threat data that companies, IT professionals and others have said need to be shared. In this respect, it is a substantial improvement over other approaches that describe in broad, general terms the threat information that can be shared.[5] However, the Cybersecurity Act creates a large loophole by permitting information to be shared if it "may be indicative" of a defined threat. This loose standard would be difficult to apply and is likely to result in the unnecessary sharing of private communications information that does not describe a cybersecurity threat. A better formulation would permit the sharing of only information "reasonably believed to be necessary to describe" the threat. The bill includes a helpful minimization provision: it requires that companies sharing cyber threat information make reasonable efforts to remove from the information they share personally identifiable information unrelated to the cybersecurity threat.

SECURE IT also permits threat information to be shared if it merely "may be indicative" of a threat, and it goes further by authorizing companies to share with the government two unnecessarily broad categories of threat information. It allows companies to share information that may be indicative of "network activity" that "may signify malicious intent." "Malicious intent" is left undefined. SECURE IT also permits companies to share with the government and each other any information that "may be indicative" of information that would "foster situational awareness of the United States security posture," unless a law specifically bars disclosure. This is far too broad. Finally, SECURE IT omits the minimization requirement that the Cybersecurity Act imposes.

B. With Whom Can Information Be Shared?

1. Information sharing from the private sector to the government

The answer to this question – with whom can information be shared – will in large part determine whether the National Security Agency or DOD's Cyber Command will displace the Department of Homeland Security as the lead federal agency for cybersecurity for

[4] Cybersecurity Act, Section 708(6).

[5] For example, the threat information that the Rogers bill authorizes companies to share with the NSA and other agencies could include all of the information passing over their network that they examine for cybersecurity reasons. See, https://www.cdt.org/blogs/greg-nojeim/112cyber-intelligence-bill-threatens-privacy-and-civilian-control

the private sector. The NSA has been lobbying for a bigger role in cybersecurity, including more access to private communications. Information is power: the entity that becomes the governmental hub for cybersecurity information sharing will gain substantial power over cybersecurity policy and practices. The NSA and Cyber Command are far more secretive than DHS, and they have intelligence missions that go beyond cybersecurity. Civilian control of cybersecurity helps promote transparency and accountability to the public for failure and abuse, and it gives companies asked to share information more confidence that they will know how the information they share is used.

Unfortunately, Section 703 of the Cybersecurity Act punts the question of who is in charge of cybersecurity information sharing with the private sector to the Department of Homeland Security. Under the bill, after consulting with the Director of National Intelligence, the Secretary of Defense, and the Attorney General, DHS will designate a lead federal cybersecurity exchange and may designate additional federal and non-federal cybersecurity exchanges. The lead federal exchange has significant authority: it receives and disseminates "cyber security threat indicators" among governmental, private, and international entities and coordinates information security collaboration among these entities. While the current Administration has signaled its intent to keep DHS in charge, a future Administration could designate NSA or another element of the Department of Defense as the lead federal exchange or as an additional exchange through which significant amounts of consumers' communications traffic might flow.

Congress should not leave this critical question open. Instead, Congress should designate a DHS entity (most likely the National Cybersecurity and Communications Integration Center or "NCCIC") as the lead cybersecurity exchange and require that any additional federal information exchanges be civilian, unless they deal primarily with elements of the Defense Industrial Base.

The McCain bill, SECURE IT, goes in the opposite direction: it expressly designates three DOD entities, including the National Security Agency, as "cybersecurity centers"[6] to receive cyber threat information from the private sector notwithstanding any law and with blanket immunity. This means that ISPs and other communication service providers could "voluntarily" share a very broad range of communications data with the National Security Agency. Moreover, even if a company chooses to share cyber security threat indicators only with DHS, SECURE IT subverts that choice: it requires the receiving cybersecurity center to immediately re-disclose the information to the NSA.[7]

2. Company-to-company information sharing

A government-centric information sharing hub will likely not be able to act quickly enough to share in real time the cyber threat information that needs to be shared to protect networks. For this reason, and because the flow of private information to intelligence and law enforcement entities poses severe civil liberties risks, CDT has always favored private-to-private information sharing, with controls, instead of government-centric information sharing models. Both the Cybersecurity Act (Section 702(a)) and SECURE

[6] SECURE IT, Section 101(5).

[7] SECURE IT, Section 102(d)(1)(B).

IT (Section 102(a)(2)) permit companies to share threat information with each other, but the Cybersecurity Act discourages company-to-company sharing because it does not sufficiently limit liability for such information sharing.[8] This makes it less likely that companies would take the risk of voluntarily sharing cyber threat information, except through the cybersecurity exchanges the bill authorizes. SECURE IT takes a better approach by granting immunity for information sharing regardless of whether it occurs through an information sharing hub (Section 102(g)(1)), but as indicated below, fails to ensure that information shared for cybersecurity reasons is used exclusively for those reasons.

C. For What Purposes May Information Be Shared and Used?

Properly constructed cybersecurity legislation would require that cyber security threat information be shared and used only for cybersecurity purposes. Without this limitation, cybersecurity information sharing can become a back door wiretap: communications that the government could receive only with a warrant or other legal process are made available to it under the cybersecurity information sharing umbrella and can then be used for criminal prosecution, to target additional intelligence or criminal surveillance, and for other governmental purposes.

1. Law enforcement use of cybersecurity disclosures

The Cybersecurity Act permits information disclosed for cybersecurity purposes to be used for other law enforcement purposes, thus creating the backdoor wiretap risk a strong use restriction would preclude. Under the Cybersecurity Act, private entities are authorized to disclose lawfully obtained cybersecurity threat indicators directly to any entity that operates a cybersecurity exchange. It then permits federal entities that operate cybersecurity exchanges to disclose those indicators to federal, state and local law enforcement agencies.[9] The standard for disclosure is very low: information "that appears to relate to a crime" can be disclosed to law enforcement. The Cybersecurity Act also permits federal entities that receive cybersecurity threat indicators from any exchange to disclose the indicators to federal, state, and local law enforcement agencies under the same low standard.[10]

To both protect civil liberties and promote information sharing, the bill should be amended to require that the information it enables to be shared for cybersecurity purposes be used exclusively for those purposes. Such purposes may include prosecution of cybersecurity crimes.[11]

---

[8] Cybersecurity Act Section 706(a)(2)(D). Private-to-private information sharing in the Cybersecurity Act is immunized only if the information is shared with an entity that manages critical infrastructure, or if it is also shared with a designated cybersecurity exchange.

[9] Cybersecurity Act Section 704(g)(2).

[10] Cybersecurity Act, Section 704(g)(3)(A).

[11] The House Homeland Security Committee's PRECISE Act, H.R. 3674, introduced by Rep. Dan Lungren, appropriately permits information shared for cybersecurity purposes to be used to prosecute cybersecurity crimes but not other crimes. Sections 248(b)(3)(A) and 248(f)(2).

While we have very strong reservations about the uses to which the government could put cyber threat information shared in the Cybersecurity Act, SECURE IT is worse: it would permit information disclosed for cybersecurity purposes to be used for law enforcement purposes[12] as well as for "national security" purposes unrelated to cybersecurity. Thus, SECURE IT effectively turns cybersecurity information sharing into an intelligence surveillance program.

Moreover, SECURE IT *requires* companies to disclose cyber threat information they encounter that is directly related to a contract they have with a governmental agency to provide the agency with communication or cybersecurity services.[13] These federal contractors would be required to disclose the cyber threat information to the federal entity with which they have a contract, and that entity would be required to disclose the threat information to a federal cybersecurity center, and the center could disclose it further, even before the company that made the product with the vulnerability is notified. This undermines cybersecurity by putting the cart before the horse: the vulnerability is disclosed before the fix is fashioned. It also threatens the public-private partnership essential to the success of the cybersecurity program. This section should be dropped.

2. Disclosures to private entities

The Cybersecurity Act permits private entities to disclose lawfully obtained cybersecurity threat indicators to any other private entity for any purpose, but private entities receiving those threat indicators can retain, use, or further disclose them only for cybersecurity purposes.[14] Disclosing companies can place restrictions on the disclosure or use of the cybersecurity threat indicators they disclose to other companies, and have the option of requiring that personally identifiable information be removed from such indicators before they are re-disclosed to others. Companies that fail to abide by the use or disclosure rules imposed by the bill or by the disclosing party can be held liable for those failures only if a law or contract currently imposes liability.[15] The bill creates no private right of action. Instead, if a company is otherwise obligated to safeguard, use or disclose cyber threat information in a particular way, failure to abide by that obligation is not immunized. This section could improved by permitting the initial disclosure of threat information only for cybersecurity purposes, and, as indicated below, by providing for a private right of action for those aggrieved by a failure to abide by the information sharing rules it imposes, or another equally effective compliance mechanism.

---

[12] While the Cybersecurity Act permits law enforcement to prosecute any crime based on cybersecurity threat information shared under the bill, SECURE IT permits such information to be used to prosecute only the hundreds of crimes that are wiretap predicates. This is still a large universe of crimes and significant loophole.

[13] SECURE IT, Section 102(b).

[14] Cybersecurity Act, Section 702(b)(4) provides that a recipient "may only use, retain, or further disclose the cybersecurity threat indicators for the purpose of protecting an information system or information stored on, processed by, or transiting and information system from cybersecurity threats or mitigating the threats."

[15] Cybersecurity Act, Section 706(g) provides that there is no limit on liability for failure to abide by use and disclosure rules in Section 702(b).

SECURE IT imposes no requirement that companies that receive cyber threat information use it only for cybersecurity purposes. It permits disclosing companies to impose use restrictions, but leaves consumers without this important protection.

D. What Promotes Compliance with Information Sharing Rules?

The Cybersecurity Act lacks sufficient accountability measures to ensure that companies abide by limits placed on information sharing, and SECURE IT is even more lacking because it omits even the use limitations in the Cybersecurity Act.

The Cybersecurity Act provides that companies may only use, retain and further disclose cyber threat indicators for cybersecurity purposes and failure to abide by this limitation is not immunized against liability.[16] This promotes compliance with disclosure and use requirements. SECURE IT does not even require companies that receive cyber threat information to use, retain and disclose the information only for cybersecurity purposes. The Cybersecurity Act also requires federal entities to extract contractual commitments from the entities with which they share cybersecurity threat indicators that limit use of that information to cybersecurity purposes.[17] SECURE IT includes no such requirement. While the Cybersecurity Act clearly has superior accountability measures, to ensure cyber threat indicator information is not misused, the legislation should create either a private right of action for any person aggrieved by the use of cybersecurity threat indicators for any purpose other than cybersecurity, or another equally effective accountability measure.

II. Monitoring

Top line: The monitoring provisions of the Cybersecurity Act and SECURE IT should be dropped. They have not received any serious public scrutiny to date. The conduct that would be permitted has not been adequately delineated. Current law already authorizes network operators and other companies to monitor their systems for cybersecurity purposes and already provides immunity for such monitoring. It is not clear what additional authority is needed, nor is it clear what additional authority is being conferred. The impact on companies and on Internet users could be enormous. The risk of abuse is too great, especially when the information sharing provisions in both bills allow any information that is intercepted to flow to the super-secret NSA.

Section 701 of the Cybersecurity Act authorizes ISPs and other companies to monitor their information systems and any information stored on, processed by, or transiting their systems for "cybersecurity threats." A cybersecurity threat is defined as "any action that may result in unauthorized access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality, or availability of an information system or information that is

[16] Cybersecurity Act, Sections 702(b)(4) and 706(a). However, reliance in good faith that the bill permitted the use, retention or disclosure in question is a complete defense against a claim based on such use, retention or disclosure.

[17] Cybersecurity Act, Section 704(g)(3)(B).

stored on, processed by, or transiting an information system."[18] In addition, any private entity could monitor the system of any third party if the third party lawfully authorizes the monitoring. To "monitor" is to wiretap communications in real time or to acquire communications from storage.[19] Companies that engage in this monitoring would enjoy broad immunity from any liability for doing so.[20]

This grant of authority to monitor information systems and information stored on, processed by or transiting such systems for any action that might result in compromise of that system or of any other system, or any information stored on, processed by or transiting any other system is overbroad, largely because the definitions of cybersecurity threat and cybersecurity threat is so broad.[21] Sharing the password to your Facebook account is an "action" that may result in unauthorized access in the future and thus constitutes a cybersecurity threat. Sharing a link to a file-sharing site may result in "unauthorized access" to information. Since any email attachment may contain a virus or a worm, forwarding any email attachment is "an action" that may result in impairment of an information system.

The McCain bill, SECURE IT, permits any ISP or any other entity, notwithstanding any law, to use on its networks "cybersecurity systems" to obtain "cyber threat information," which in turn is defined to include "information that may be indicative of … network activity … that may signify malicious intent." Since cybersecurity threats can be embedded in any seemingly innocent communication, this could allow the monitoring of all communications. The McCain bill goes on to allow any such information, plus information "that would foster situational awareness of the United States security posture" to be shared with the US government. It also requires any information shared with one government entity to be immediately shared with the NSA.

In authorizing any ISP to monitor any communication on its system for any activity that would compromise any information, the Cybersecurity Act would, among other things, appear to authorize ISP monitoring of subscribers' traffic streams to identify copyright violations, a highly controversial issue with major privacy implications.[22] The McCain bill

---

[18] Cybersecurity Act, Section 708(5). An "information system" is "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information …" Cybersecurity Act, Section 708(10). It seems that, under this definition, every computer and smart phone is an "information system," as is every website. In fact, it would seem that every student term paper with a list of references is a "discrete set of information resources organized for the … sharing … of information."

[19] Cybersecurity Act, Section 708(13) defines "monitor" as "the interception, acquisition, or collection of information that is stored on, processed by or transiting an information system for the purpose of identifying cybersecurity threats."

[20] Cybersecurity Act, Section 706(a)(1).

[21] The language allows monitoring of a system "for cybersecurity threats." It does not say that the monitoring must be limited to threats to the system that is being monitored. Instead, it seems to allow ISPs and other to monitor their systems for threats to other systems, and to some degree that is appropriate.

[22] As CDT described in comments to the Department of Commerce, "[u]sers quite simply do not expect such surveillance. If consumers come to learn that their ISPs are monitoring and perhaps recording every step they take online, [such monitoring] runs the risk of damaging consumer confidence in the medium. This could have a chilling effect on the use of the Internet for beneficial purposes, including academic, financial,

is explicit on this point: the monitoring it authorizes is to be done by "cybersecurity systems," which it defines to include "measures intended to protect a system … from … misappropriations of … intellectual property."

But the monitoring authority goes even further. The Cybersecurity Act authorizes any private entity to monitor a third party's information system (that is, a computer) if the third party lawfully authorizes the monitoring. Likewise, the McCain bill authorizes any private entity to monitor another entity's networks "as authorized" by that other entity. CDT would strenuously argue that such monitoring could not be authorized in the terms of service associated with the purchase of software, the purchase of a computer, the use of a website or the subscribing to Internet service, but the fact is that courts have upheld so-called "click-wrap" contracts.[23] (On this issue, the Cybersecurity Act is the broader of the two Senate bills, stating that any computer user may authorize any private entity to access his or her computer to acquire any information stored there.)

The monitoring authority granted in these bills is of particular concern because communication service providers already enjoy broad authority under the surveillance statutes to monitor their networks.[24] So far, explanation as to why the broad monitoring authorization in the Cybersecurity Act or SECURE IT is necessary has been wholly inadequate. Moreover, there has been no explanation as to how the authority granted under the bills would differ from existing authority. Specific clarifications in existing authority may be needed, for example, to permit detection of botnets, but with Senate floor action looming, its seems impossible to publicly vet language on such a topic and get all affected stakeholders to publicly agree on any specific language and to be sure that the language is not capable of multiple interpretations. The monitoring provisions should be dropped.

---

and health services." Comments of CDT in Response to the Department of Commerce Internet Policy Task Force's Inquiry on Copyright, Creativity, and Innovation in the Internet Economy (Nov. 19, 2010) https://www.cdt.org/files/pdfs/CDT%20Comments%20to%20NTIA%20Copyright%20Task%20Force.pdf at 8. In Europe, the European Court of Justice recently concluded that requiring ISPs to monitor for copyright infringement would be inconsistent with EU laws regarding privacy and freedom of information. Court of Justice of the European Union, Press Release No 126/11 (Nov. 24, 2011). http://curia.europa.eu/jcms/upload/docs/application/pdf/2011-11/cp110126en.pdf.

[23] See CDT, "An Overview of the Federal Wiretap Act, Electronic Communications Privacy Act, and State Two-Party Consent Laws of Relevance to the NebuAd System and Other Uses of Internet Traffic Content from ISPs for Behavioral Advertising" (July 8, 2010) http://www.cdt.org/privacy/20080708ISPtraffic.pdf; EFF, "The Clicks That Bind: Ways Users 'Agree' to Online Terms of Service," (Nov. 2009) https://www.eff.org/wp/clicks-bind-ways-users-agree-online-terms-service. The Justice Department argues that consumers can implicitly surrender any Constitutional right they have against government access to their communications.

[24] The Wiretap Act has several provisions allowing communication service providers to monitor their own networks. To begin with, the Wiretap Act's definition of "intercept" excludes monitoring by service providers using their own equipment "in the ordinary course of business." 18 U.S.C. Section 2510(4) and (5). The Wiretap Act goes on to state that it is lawful for any provider of electronic communication service, or an agent of such provider, to intercept, disclose or use communications passing over its network while engaged in any activity that is a necessary incident to the rendition of the service or to the protection of the rights and property of the provider.18 U.S.C. Section 2511(2)(a)(i). The same authority is available to any other entity that operates a network.

III. Countermeasures

Top line: In addition to authorizing monitoring, the Cybersecurity Act authorizes companies to operate "countermeasures" to protect their own information systems and data and to protect the information systems and data of third parties who have given lawful authorization. SECURE IT would authorize any private entity to employ countermeasures on its networks or, as authorized by another entity, on such entity's networks. In both bills, the countermeasures language, like the monitoring language, is too broad and too risky. It should be dropped.

A "countermeasure" is defined in the Cybersecurity Act as any action to modify or block data packets on one's own information system or, with lawful authorization by a third party, the information system of that third party to protect against any action that may result in compromise of the network or data stored on it.[25] Countermeasures may be undertaken even if they would otherwise violate the surveillance statutes or the Communications Act of 1934.[26] A good faith belief that the Cybersecurity Act authorizes a countermeasure is an affirmative defense in any civil or criminal action brought on the basis of that countermeasure under any other law.[27]

The countermeasures language is far too broad. It would potentially authorize a provider to violate the FCC's Net Neutrality rules[28] by selectively throttling, as a cybersecurity measure, legitimate Internet traffic that is not malicious but happens to be bandwith-intensive -- on a theory that high bandwidth usage could impair network availability. Creating such an exception to the FCC's Net Neutrality rules is entirely unnecessary, since the rules already provide ample leeway for companies to engage in "reasonable network management" to ensure network security. The countermeasures language in the Cybersecurity Act would also appear to authorize a provider cut off its own customers' Internet access, for example as a protective measure when the customer has been victimized by a botnet, without defining any procedures for notice to the customer. It would even permit ISPs to reach into the computers of their customers to modify data packets in the name of protecting those consumers, if the consumer "lawfully authorizes" the countermeasures.

The questions of when ISPs should cut off customers infected by bots or reach into their computers are very sensitive and nuanced. The Cybersecurity Act's countermeasures provisions would brush aside all those sensitivities. Botnet best practices are already

---

[25] "Countermeasure" is defined as "automated or manual actions with defensive intent to modify or block data packets associated with electronic or wire communications, internet traffic, program code or other system traffic transiting to or from or stored on an information system for the purpose of protecting the information system from cybersecurity threats, conducted on an information system owned or operated by or on behalf of the party to be protected or operated by a private entity acting as a provider of electronic communications services, remote computing services or cybersecurity services." Cybersecurity Act, Section 708(2).

[26] Cybersecurity Act, Section 701.

[27] Cybersecurity Act, Section 706(b).

[28] Open Internet Rules, 47 CFR Sections 8.1 - 8.11.

being considered through two industry-led processes,[29] and this broad grant of authority could short circuit the significant progress that has already been made. There is no need for Congress to open this can of worms: providers already have authority to protect their networks from harm and to hire others to do so as their agents.[30] There has been no public explanation of why the current authority is inadequate. This provision, which has not been the subject of any substantial public debate but has far reaching implications, should be dropped.

Senator McCain's bill, SECURE IT, is even more troubling, if only because it is even vaguer: It combines monitoring and countermeasures into one broad authorization, permitting any private entity, notwithstanding any law, "for the purpose of preventing, investigating, or otherwise mitigating threats to information security, on its own networks, or as authorized by another entity, on such entity's networks," to "employ countermeasures and use cybersecurity systems in order to obtain, identify, or otherwise possess cyber threat information." In SECURE IT, "countermeasure" is defined as "an automated or a manual action with defensive intent to mitigate cyber threats." That covers all of the ground in the Lieberman-Collins bill, and more. "Cyber threat" is not defined. Unlike the Cybersecurity Act, SECURE IT immunizes countermeasures conduct from any legal liability, making the vague countermeasures provision even more problematic.[31]

IV. Information Sharing in FISMA Reform Sections

In addition to the provisions allowing private sector entities to share with each other and with the government, the Cybersecurity Act includes provisions allowing federal agencies to share information with DHS. This intra-government sharing authority is included in the provisions of the Act that would reform the Federal Information Security Management Act (FISMA). The intra-governmental information sharing provisions raise privacy challenges that need to be addressed. SECURE IT's FISMA reform provisions[32] do not raise these concerns because they do not authorize overly-broad information sharing by federal agencies.

The FISMA reform provisions in the Cybersecurity Act authorize federal agencies to share sensitive personally identifiable information with the Department of Homeland Security and authorize DHS to disclose that information for law enforcement purposes.

---

[29] A working group of the FCC Communications Security, Reliability and Interoperability Council (CSRIC) issued an Anti-Bot Code of Conduct for ISPs earlier this month https://otalliance.org/resources/botnets/20120322%20WG7%20Final%20Report%20for%20CSRIC%20III.pdf.At the same time, a Commerce Department/DHS Request for Information https://www.federalregister.gov/articles/2011/09/21/2011-24180/models-to-advance-voluntary-corporate-notification-to-consumers-regarding-the-illicit-use-of has inspired another industry-led effort to develop a voluntary botnet code of conduct for a broader segment of industry. CDT has applauded this effort. http://www.nist.gov/itl/upload/CDT-Comments-on-BotNet-FRN-11-14-11.pdf.

[30] 18 U.S.C. 2511(2)(i).

[31] SECURE IT Act, Section 102(g)(1)(A)(i) grants companies that monitor or employ "countermeasures" legal immunity for doing so.

[32] SECURE IT Section 201.

These provisions may be intended to facilitate operation of the Einstein intrusion detection and prevention system,[33] but they go substantially beyond what would be necessary and could have unintended consequences.

For example, proposed Section 44 U.S.C. 3554(c) would authorize the head of any agency to allow DHS (or any entity assisting it) to acquire, intercept, retain, use and disclose communications and other information stored in or transiting to or from such agency's information systems for information security reasons, even if disclosure of the information would otherwise be illegal.[34] The bill authorizes DHS to order other agency heads to take any lawful action with respect to the operation of information system for the purposes of protecting it.[35] It also authorizes DHS to "acquire, intercept, retain, use and disclose" communications stored on or transiting an agency information system when DHS deems it reasonably necessary to protect it from information security threats, to collect and retain content "associated" with a reasonably suspected information security threat, and to disclose that content for law enforcement purposes when it may be evidence of any crime.[36]

Taken together, these provisions mean that sensitive information a person submits or has submitted to the one government agency under a promise of privacy and limited use may be disclosed to DHS, and may be used to prosecute the person if it relates to a crime. For example, the Department of Health and Human Services collects substance abuse treatment records that include personally identifiable evidence of drug crimes. 42 C.F.R. 2 imposes strict confidentiality rules on this information. Subverting those rules threatens treatment goals. If DHS deems disclosure to DHS of information in this HHS database necessary to protect the database from an information security threat, it can order the HHS to make this disclosure. The bill then authorizes DHS to share evidence of the drug abuse crimes revealed by that data with the FBI and local law enforcement. The check on this power: approval by the head of the department that would prosecute – the Attorney General.

There are plenty of other examples because many agencies – the Census Bureau, the Internal Revenue Service and many others – maintain personally identifiable information confidentially in order to provide a service or conduct a government function. The Cybersecurity Act opens this data up to DHS for cybersecurity purposes, and authorizes it to be used for criminal enforcement purposes. These provisions should be narrowed so that only cybersecurity threat indicators defined in Section 708(6) may be disclosed to DHS and to ensure that these indicators are used only for cybersecurity purposes. The bill should also be clarified to entitle agency heads to withhold disclosure to DHS of personally identifiable information in their databases when such disclosure is contrary to the public interest.

---

[33] DHS uses Einstein, with NSA assistance, to protect federal agency information systems. See this Privacy Impact Assessment of an Einstein 3 exercise http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_initiative3exercise.pdf for a description of the program.

[34] Cybersecurity Act Section 201, proposed 44 U.S.C. Section 3554(d) (p. 76).

[35] Cybersecurity Act Section 201, proposed 44 U.S.C. Section 3553(e).

[36] Cybersecurity Act Section 201, proposed 44 U.S.C. Section 3553(d)(2).

Conclusion

The information sharing provisions in the cybersecurity bills as drafted would allow far too much information to flow to the government and far too much to flow to the National Security Agency. In the process, the bills would undermine the ongoing efforts to improve information sharing within a framework of trust and accountability. The information sharing provisions should be amended to –

- limit sharing of information to that which is "reasonably believed to be necessary to describe" a specific category of cybersecurity threat indicator;
- incentivize sharing company-to-company;
- delete the authorization to share any information that would "foster situational awareness of the US security posture;"
- designate DHS as the lead federal agency to receive information from the private sector for cybersecurity purposes; and
- limit the uses of cybersecurity information to cybersecurity (including the prosecution of cybercrimes).

In addition, the overbroad, far reaching monitoring and countermeasures provisions should be dropped. They have not been justified, they could have very serious implications for Internet users, and they have not been adequately explored.
CDT looks forward to working with the sponsors of the Senate bills and with industry stakeholders to address the concerns set forth above while developing an effective response to the critical issue of cybersecurity.

For more information, please contact CDT's James X. Dempsey, (jdempsey@cdt.org), Gregory T. Nojeim (gnojeim@cdt.org), or Kendall C. Burman (kburman@cdt.org) and at 202/637-9800.