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

1634 Eye Street, NW
Suite 1100
Washington, DC 20006

July 29, 2012

Comparison of Information Sharing, Monitoring and Countermeasures Provisions in the Cybersecurity Bills

The chart below compares on civil liberties grounds three bills that seek to promote cybersecurity and it updates a similar chart we issued on April 4, 2012 based on prior versions of all three bills. The Senate is set to consider the Cybersecurity Act, S. 3414 ("Lieberman-Collins" bill), introduced on July 19. The chart shows that the Lieberman bill better protects privacy than do either of the competing bills, and that it should be further improved by dropping monitoring and countermeasures language. The leading alternative Senate bill, SECURE IT, S. 3342, was re-introduced by Senator McCain and other co-sponsors on June 27 ("SECURE IT"). Despite a White House veto threat, the House passed the Cyber Intelligence Sharing and Protection Act, H.R. 3523 ("CISPA") on April 26 on a vote of 248-168. It will be reconciled with cybersecurity legislation that the Senate passes. (Lieberman-Collins and SECURE IT include cybersecurity measures unrelated to information sharing that are not reflected in this chart.) For more information, contact CDT's Gregory T. Nojeim (gnojeim@cdt.org) or Kendall C. Burman (kburman@cdt.org), 202/637-9800.

	CISPA, H.R. 3523 (House Bill)	**Lieberman-Collins, S. 3414**	**SECURE IT, S. 3342**
Does the bill confer overly broad authority for providers to monitor Internet users' communications?	Yes. Bill permits ISPs to use "cybersecurity systems" on their networks and permits cybersecurity providers to do so as well to monitor the networks of companies they protect, to identify and obtain "cyber threat information," which the bill defines somewhat narrowly. The bill makes clear that companies are not authorized to use the government's EINSTEIN devices on private sector networks. Proposed Nat'l Security Act Secs. 1104(b)(1), (g)(4)	Yes. Also authorizes ISPs and others to monitor their networks, and the computers of consumers and companies who give permission, for specific categories of threat indicators. Sec. 701	Yes. Authorizes ISPs and others to use on their networks, and the networks of those who give permission, "cybersecurity systems" to obtain "cyber threat information," which is more broadly defined than in Lieberman-Collins. Sec. 102(a)

	CISPA, H.R. 3523 (House Bill)	Lieberman-Collins, S. 3414	SECURE IT, S. 3342
Do private companies receive overly-broad authority to employ countermeasures against Internet users, including their customers?	The bill does not explicitly grant new authority to use countermeasures, but such authority is arguably included in the authority to use "cybersecurity systems" to identify and obtain cyber threat information to protect rights and property. Sec. 1104(b)(1)	Yes. The bill gives companies power to modify or block traffic to protect rights or property from cybersecurity threats extremely broadly defined to include "any action" that may result in unauthorized access to, theft of, or manipulation of data that is stored on or transiting an info system. Countermeasures cannot violate net neutrality rules. Secs. 707(10), 701, 708(2) and (6)	Yes. The bill gives the same broad and problematic authority to interfere with traffic as does Lieberman-Collins, but with no protections for net neutrality. Bill compounds the problem by immunizing countermeasures conduct against any legal liability. Secs. 102(a), (g)
Does the bill protect privacy by narrowly defining the cyber threat information that can be shared? (Bill language defining the info that can be shared is so critically important we set it forth for each bill in the appendix.)	Somewhat. "Cyber threat information" is limited to "information directly pertaining to" a vulnerability, a threat, an effort to degrade, disrupt, or destroy a system or network or an effort to gain unauthorized access to a system or network. Unlike the bill as introduced, this definition should preclude companies from sharing entire communications streams with the government. Does not require any effort to strip out irrelevant personal information. Sec. 1104(h)(4)	Yes. Entities can disclose eight specific categories of information called "cyber threat indicators." Importantly, information must be "reasonably necessary to describe" those categories of information. Bill helpfully requires reasonable efforts to strip out irrelevant information on specific persons. Secs. 702, 704	No. "Cyber threat information" includes information that "indicates or describes" nine categories of information, including that which "may signify malicious cyber intent" or "fosters situational awareness of US cybersecurity." Does not require any effort to strip out irrelevant personal information. Sec. 101(4)

	CISPA, H.R. 3523 (House Bill)	Lieberman-Collins, S. 3414	SECURE IT, S. 3342
Method of sharing?	Companies and governmental agencies can share cyber threat information directly for any cybersecurity purpose. Companies would choose the agency with which they would share information. Agencies are permitted to share with each other so long as such sharing does not "undermine the purpose for which such information is shared." Secs. 1104(b)(1), (b)(2)(B), and (b)(3)(B)(iv)	Cyber threat indicators may be shared through DHS-designated federal or non-federal exchanges or directly among companies. Since complete liability protection for private companies only applies for information shared with an exchange, companies will be disinclined to share strictly with each other. Secs. 702, 703	Allows for private companies to exchange information with each other and with existing cybersecurity centers. Sec. 102(a)(2). Cybersecurity centers *must immediately* share that information with each other (Sec. 102(d)(1)(b)) and with other federal entities. Information can also be shared with local governments, private companies, and international partners, with the permission of the disclosing entity. Secs. 102(c) and 103(d). In certain circumstances, federal contractors providing IT services would be required to inform the contracting agency of a significant cyber incidents involving government information. Sec. 102(b)
Does the bill promote transfer of cybersecurity authority from civilian to military control by permitting private civilian entities to share communications info with NSA?	Yes. The bill permits companies to share directly with military agencies, such as the NSA, but it also requires the NSA (and any other agency) to share that information with DHS. Though this flow of information will grow NSA's cyber authorities, the bill disclaims this outcome. Secs. 1104(b)(2)(A), and (g)(2)	No. All federal exchanges with which companies can share information must be within civilian agencies. The bill requires DHS, the AG, ODNI, and DOD create a process for designating cyber exchanges. Secs. 703(c) and (d)	Yes. The bill permits cyber information to be shared by civilian private entities with a host of government cybersecurity centers, the majority of which are military.[i]

	CISPA, H.R. 3523 (House Bill)	Lieberman-Collins, S. 3414	SECURE IT, S. 3342
Does the bill protect privacy by requiring that information shared with a private company for cybersecurity purposes be used only for cybersecurity purposes?	No. No use restriction protects consumers. Other than a prohibition against using information to gain an unfair competitive advantage, bill leaves all restrictions on recipient company use up to the companies who share this information. Also exempts companies from liability for abuses of sharing information if they act in good faith. Secs. 1104(b)(2) and (3)	Yes. Companies that receive information can use it only for cybersecurity purposes, must make reasonable efforts to safeguard information that identifies individuals, must agree to any lawful restrictions placed on the disclosure of the info by the disclosing entity or exchange, and must not use the information to gain an unfair competitive advantage. Secs. 702(b) and 704(c). Companies cannot disclose information to an entity that they know has violated these requirements if the company also knows it is reasonably likely that the entity will violate them again. Secs. 702(c) and 704(d). While there is no immunity for breach of info sharing rules, companies have a good faith defense in any civil or criminal action. Sec. 706(b)	No. No use restriction protects consumers. Other than a prohibition against using information to gain an unfair competitive advantage, bill leaves all restrictions on recipient company use up to the companies who share this information. Sec. 102(e). Provides civil and criminal liability protection for the use or disclosure of information under the Act, undermining even this use restriction. Sec. 102(g)

	CISPA, H.R. 3523 (House Bill)	Lieberman-Collins, S. 3414	SECURE IT, S. 3342
Does the bill protect privacy by limiting government use of shared information to cybersecurity purposes?	Somewhat. Information shared with the government can be used not only for cybersecurity purposes (which includes prosecution of cyber crimes), but also for any national security purpose, and certain law enforcement purposes involving serious bodily harm or for the protection of minors. It can be searched only for prosecution of cybersecurity crimes. Sec. 1104(c)	Yes. The bill restricts disclosure of cybersecurity threat indicators to law enforcement unless it "reasonably appears" that information pertains to a cybersecurity crime, to an imminent threat of death or serious bodily harm, or to a serious threat to minors. Sec. 704(g)(2).	No. The bill puts fewer limits on government use than do the other bills, permitting cyber threat information the government receives to be used for "a cybersecurity purpose, a national security purpose, or in order to prevent, investigate, or prosecute" the many crimes listed under the Wiretap Act. Sec. 102(c)(1)

	CISPA, H.R. 3523 (House Bill)	Lieberman-Collins, S. 3414	SECURE IT, S. 3342
Does the bill include strong measures to ensure that entities authorized to share and receive info are held accountable?	No. The bill authorizes the Inspector General of the Intelligence Community to submit an annual report to Congress on the exchange and use of cyber threat information. Bill requires the government to notify a company if the company shares information that is not cyber threat information. Sec. 1104(c)(5), (e). Creates private right of action against the gov't if it intentionally violates use, disclosure or search restrictions. Sec. 1104(d)	Yes. Requires private companies to agree by contract with disclosing federal agency that they will not misuse the cyber threat information they receive. Sec. 704(g)(2)(b). Requires non-federal exchanges to commission an annual audit and federal exchanges are subject to an annual IG investigation. Every two years PCLOB is required to report to Congress on practices of private entities under the bill and the impact on civil liberties of actions by federal entities. Creates private right of action against the government for any intentional violation of the info sharing title of the bill, not just those that directly govern use and disclosure of information. Sec. 704(g)(7)	No. Because the bill imposes such limited use restrictions, there isn't much for a company or agency to be held accountable for. Companies can only disclose their customers' information if the customer has an opportunity to prevent such disclosure. Sec. 102(a)(3). Requires cybersecurity centers to develop procedures on their receipt and handling of information, including consideration of privacy and civil liberties, and requires those centers along with PCLOB to issue a report to Congress that includes an assessment of whether info sharing goes beyond that which is authorized. Secs. 102(d)(1)(C) and 105. Also authorizes compliance review of government activities by the Council of the Inspectors General on Integrity and Efficiency. Sec. 106. Creates no new private right of action against the government for violations of info sharing rules.

Appendix - Defining What Information Can Be Shared

Each of the three bills analyzed in this chart permits companies to share cybersecurity information "notwithstanding any law." This means that information sharing is authorized even if a federal or state privacy law, or another law, would protect the information against disclosure. As a result, it is critically important that the bills narrowly describe the information that can be shared. This is so critically important that this appendix quotes the description of the information that can be shared under each bill.

- CISPA defines "cyber threat information" that can be shared notwithstanding any law (see Sec. 1104(h)) as "information directly pertaining to (i) a vulnerability of a system or network of a government or private entity; (ii) a threat to the integrity, confidentiality, or availability of a system or network of a government or private entity or any information stored on, processed on, or transiting such a system or network; (iii) efforts to deny access to or degrade, disrupt, or destroy a system or network of a government or private entity; or (iv) efforts to gain unauthorized access to a system or network of a government or private entity, including to a system or network of a government or private entity, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting a system or network of a government or private entity." The definition expressly excludes "information pertaining to efforts to gain unauthorized access to a system or network of a government or private entity that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute authorized access." Sec. 1104(g)(4)

- The Lieberman-Collins bill defines "cybersecurity threat indicators" that can be shared notwithstanding any law (see Secs. 702(a), 704(a), and 705(b)) as information that (A) is reasonably necessary to describe (1) malicious reconnaissance, including anomalous patterns of communications that reasonably appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat; (2) a method of defeating a technical control; (3) a technical vulnerability; (4) a method of defeating an operational control; (5) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a technical control or an operational control; (6) malicious cyber command and control; (7) the actual or potential harm caused by an incident, including information exfiltrated as a result of subverting a technical control when it is necessary in order to identify or describe a cybersecurity threat; (8) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or (9) any combination thereof; and (B) from which reasonable efforts have been made to remove information that can be used to identify specific persons unrelated to the cybersecurity threat. Sec. 708(7)

- SECURE IT defines "cyber threat information" that can be shared notwithstanding any law (see Sec. 102(f)) as information that indicates or describes: (A) a technical or operation vulnerability or a cyber threat mitigation measure; (B) an action or operation to mitigate a cyber threat; (C) malicious reconnaissance, including anomalous patterns of network activity that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat; (D) a method of defeating a technical control; (E) a method of defeating an operational control; (F) network activity or protocols known to be associated with a malicious cyber actor or that signify malicious cyber intent; (G) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to inadvertently enable the defeat of a technical or operational control; (H) any other attribute of a

cybersecurity threat or cyber defense information that would foster the situational awareness of the United States cybersecurity posture, if disclosure of such attribute or information is not otherwise prohibited by law; (I) the actual or potential harm caused by a cyber incident, including information exfiltrated when it is necessary in order to identify or describe a security threat; or (J) any combination thereof. Sec. 101(4).

---

[i] SECURE IT defines "cybersecurity center" as the Department of Defense Cyber Crime Center, the Intelligence Community Incident Response Center, the United States Cyber Command Joint Operations Center, the National Cyber Investigative Joint Task Force, the National Security Agency/Central Security Service Threat Operations Center, the National Cybersecurity and Communications Integration Center, and any successor center. Sec. 101(5)