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

1634 Eye Street, NW
Suite 1100
Washington, DC 20006

April 4, 2012

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

The chart below compares on civil liberties grounds four bills that seek to promote cybersecurity . The PRECISE Act, H.R. 3674 ("Lungren" bill) is scheduled for mark-up the week of April 16 at the House Homeland Security Committee. The Cyber Intelligence Sharing and Protection Act, H.R. 3523 ("Rogers" bill) was marked up in December by the House Permanent Select Committee on Intelligence. The Cybersecurity Act, S. 2105 ("Lieberman" bill) was introduced on February 14. The SECURE IT Act, S. 2151 ("McCain" bill) was introduced on March 1. The Lieberman, McCain and Lungren bills all include cybersecurity measures unrelated to information sharing that are not reflected in this chart. For more information, please contact CDT's Gregory T. Nojeim (gnojeim@cdt.org) or Kendall C. Burman (kburman@cdt.org), 202/637-9800.

	Lungren, H.R. 3674	**Rogers, H.R. 3523**	**Lieberman, S. 2105**	**McCain, S. 2151**
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.)	Yes. Authorizes the sharing only of information that is "necessary to identify or describe" one of six carefully defined categories of information related to cyber attacks, and requires reasonable efforts to strip irrelevant information on specific persons. Sec. 248	No. Very broadly defines the information that can be shared as "information directly pertaining to a vulnerability of, or threat to a system or network," including information pertaining to protecting a system or network from an attack or theft of information, with no requirement to strip personal information. Sec. 1104(b)(f)(6)	Somewhat. Like the Lungren bill, authorizes entities to disclose eight specific categories of information called "cyber threat indicators," although information need only "indicative of" those categories in order to be shared. Also requires reasonable efforts to strip irrelevant information on specific persons. Secs. 702, 704	No. "Cyber threat information" includes information that is "indicative of or describes" nine categories of information, including that which "may signify malicious intent" or "fosters situational awareness of US security." Does not require any effort to strip personal information. Sec. 101(4)

	Lungren, H.R. 3674	Rogers, H.R. 3523	Lieberman, S. 2105	McCain, S. 2151
Method of sharing?	Establishes a non-profit, quasi-governmental entity – the National Information Sharing Organization (NISO) -- that would serve as a clearinghouse for the exchange of cyber threat information. NISO's board of directors would be dominated by industry, with government and privacy interests also at the table. Sec. 241	Allows for private companies and government agencies to exchange information directly for any cybersecurity purpose. Companies would choose the agency or agencies with which they would share information and could also share information directly with each other. The bill creates no clearinghouse. Sec. 1104(b)(1)	Cyber threat indicators may be shared through DHS-designated federal or non-federal exchanges or directly among companies. Since 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.[1] Sec. 102(a)(2). Federal contractors providing certain IT services to the government would be *required* to disclose 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?	No. Wisely cements DHS, a civilian agency, as the lead federal agency for cybersecurity. Information sharing authorized in the bill would go through a primarily private entity.	Yes. The bill creates a real possibility that a military agency, such as NSA or DOD's Cyber Command, would take the lead. Information sharing is authorized through amendment to Title 50 of National Security Act, rather than through amendment of civilian homeland security authorities.	Unclear. The bill requires DHS, the AG, ODNI, and DOD create a process for designating cyber exchanges. The lead federal cyber exchange could be NSA, Cyber Command, or a DHS entity, but DHS is the lead exchange for up to 60 days until this designation. Other federal exchanges could be civilian or military. Sec. 703(c) and (d)	Yes. Goes beyond even Rogers by allowing cyber information to be shared by civilian private entities with a host of government cybersecurity centers, the majority of which are military.

[1] The McCain bill 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, [and] the National Cybersecurity and Communications Integration Center, and any successor center." Sec. 101(5)

	Lungren, H.R. 3674	Rogers, H.R. 3523	Lieberman, S. 2105	McCain, S. 2151
Does the bill protect privacy by requiring that information shared with a private company for cybersecurity purposes be used only for cybersecurity purposes?	Yes. Private companies can only use information for a cybersecurity purpose. Sec. 248(b)(5).	No. No use restriction protects consumers. Other than a prohibition against using information to gain an unfair competitive advantage, bill leaves all restrictions on 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. Sec. 1104 (b)(2) and (3)	Yes. Companies that receive information can use it only for cybersecurity. Secs. 702(b)(4) and 704(c)(4). Companies must agree to any lawful restrictions placed on the disclosure of the info by the disclosing entity or exchange. Secs. 702(b)(2), 704(c)(2), 704(g)(1)(B). They are also prohibited from using info to gain an unfair competitive advantage. Sec. 702(b); 704(c). 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. Private entities to place restrictions on the use or further sharing of information by the receiving entity. 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)

	Lungren, H.R. 3674	Rogers, H.R. 3523	Lieberman, S. 2105	McCain, S. 2151
Does the bill protect privacy by limiting government use of shared information to cybersecurity purposes?	Yes. Properly restricts the government from using shared information for anything other than a cybersecurity purpose, which includes the prosecution of cybersecurity crimes. Sec. 248(b)(3)	No. As amended, information shared with the government for cybersecurity purposes can be used by the government for any non-regulatory purpose whatsoever, including intelligence surveillance. It can also be used in any criminal prosecution if also used for a significant national security or cybersecurity purpose.	No. Like Rogers, bill provides no real restriction on law enforcement use. Law enforcement can receive cyber threat indicators from federal cyber exchanges and only restriction is that information must "appear[] to relate to a crime." Sec. 704(g)(2) and (3)	No. Bill puts even fewer limits on government use than in the other bills, permitting cyber threat information the Fed. Gov't 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)
Does the bill include strong measures to ensure that entities authorized to share and receive info are held accountable?	Yes. Requires NISO to commission an independent audit to review compliance of NISO and its members with information sharing rules. Creates limited private right of action for willful violations of obligation to use information only for cybersecurity purposes, and makes good faith compliance with information sharing rules a complete defense. Sec. 249 and Sec. 251 as amended	No. Because the bill imposes such limited use restrictions, there isn't much for a private or governmental entity to be held accountable for. As amended, authorizes the Inspector General of the Intelligence Community to submit an annual report to Congress on the exchange and use of cyber threat information. No accountability mechanism designed to ensure that private companies do not use information received for non-cybersecurity purposes or that they abide by use and disclosure restrictions.	Somewhat. Requires private companies to agree by contract with disclosing federal agency that they will not misuse the cyber threat information they receive, but creates no private right of action. Sec. 704(g)(2)(b). DHS given wide discretion to develop policies that balance cybersecurity needs with civil liberties interests for Federal entities. Compliance program for cyber policies set by DHS and DOJ who will also issue report to Congress. Sec. 704(g)	

	Lungren, H.R. 3674	Rogers, H.R. 3523	Lieberman, S. 2105	McCain, S. 2151
Does the bill confer overly broad authority for providers to monitor internet users' communications?	Somewhat. Permits ISPs to use "cybersecurity systems" on their networks and permits cybersecurity providers to do so as well in order to monitor the networks of companies they protect, to identify and obtain only narrowly defined cyber threat information. Proposed Homeland Security Act Sec 248(a)	Yes. Permits ISPs to use "cybersecurity systems" on their networks and permits cybersecurity providers to do so as well in order to monitor the networks of companies they protect, to identify and obtain much more broadly defined cyber threat information, which includes information pertaining to the misappropriation of intellectual property. Proposed National Security Act Sec. 1104(b)(1)	Yes. Also authorizes ISPs and others to monitor their networks, and the computers of consumers and companies who give permission, for "cybersecurity threats" which are 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 any system. 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 broadly defined to include any information that "may be indicative of" any information that would "foster situational awareness of the US security posture." Sec. 102(a)
Do private companies receive overly-broad authority to employ countermeasures against Internet users, including their customers?	Unclear. The bill vaguely gives cybersecurity providers and self-protected entities authority to use "cybersecurity systems" to protect rights and property which may be roughly equivalent of authority to employ countermeasures. Sec. 248(a)	Unclear. Similar to Lungren, the Rogers bill includes authority to use "cybersecurity systems" to protect rights and property, which may authorize overly-broad countermeasures. Sec. 1104(b)(1)	Yes. The bill gives companies broad power to modify or block traffic to protect against "any action" that might result in compromise of an information system. Exercise of this authority could violate net neutrality. Sec. 701	Yes. McCain gives the same broad and problematic authority to interfere with traffic as does Lieberman, and compounds the problem by immunizing countermeasures conduct against any legal liability. Secs. 102(a), (g)

Appendix - Defining What Information Can Be Shared

Each of the four 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. Of the four bills, only the Lungren bill has a sufficiently narrow description.

- The Lungren bill defines the term "cyber threat information" that can be shared notwithstanding any law (see Sec. 248) as the information that is (A) necessary to identify or describe-- (1) a method of defeating a technical or operational control that corresponds to a cyber attack; (2) a method of causing a person with authorized access to an information system or to information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a technical control; (3) information exfiltrated in a cyber attack when such information necessary to identify or describe the attack; (4) anomalous patterns of communications that appear to be transmitted in connection with a cyber attack, but does not include other communications content, or dialing, routing, addressing and signaling information not necessary to describe such attack; (5) anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information to be used in a cyber attack; or (6) a method for remote identification of, access to, or use of an information system or information that is stored on, processed by, or transiting an information system associated with a known or suspected cyber attack; and (B) from which reasonable efforts have been made to remove information that can be used to identify specific persons unrelated to a cyber attack. Sec. 248 (f)(6)

- The Rogers bill defines "cyber threat information" that can be shared notwithstanding any law (see Secs. 1104(b) and 9d)) as "information directly pertaining to a vulnerability of, or threat to a system or network of a government or private entity, including information pertaining to the protection of a system or network from-- (A) efforts to degrade, disrupt or destroy such system or network; or (B) theft or misappropriation of private or government information, intellectual property, or personally identifiable information." Sec. 1104(b)(f)(6)

- The Lieberman defines "cybersecurity threat indicators" that can be shared notwithstanding any law (see Secs. 702(a), 704(a), and 707(b)) as information that (A) may be indicative of or 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(6)

- The McCain bill defines "cyber threat information" that can be shared notwithstanding any law (see Sec. 102(f)) as information that may be indicative or describe: (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 may signify malicious 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 information that would foster the situational awareness of the United States security 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).