	H.R. 3674, the PRECISE Act of 2011, as reported from HHSC Subcmte on Cybersecurity (Lungren)	H.R. 3523, the Cyber Intelligence sharing and Protection Act of 2011, as reported from HPSCI (Rogers-Ruppersberger)	S. 2105, the Cybersecurity Act of 2012, as introduced (Lieberman-Feinstein)	S. 2151, the SECURE IT Act of 2012, as introduced (McCain)
WHAT INFORMATION MAY BE SHARED	-Notwithstanding any provision of law, -"Cyber threat information:" information 'necessary to identify or describe,' -six types of cyber data, -From which reasonable efforts have been made to remove info that can be used to identify specific persons unrelated to a cyber-attack. (Sec. 248(f)(6) at p. 44)	-Notwithstanding any provision of law, -"Cyber threat information:" information 'directly pertaining' to, -Vulnerability or threat to system or network of government or private entity including (A) efforts to degrade, disrupt, or destroy such system or network; or (B) theft or misappropriation of private or government info, intellectual property or personally identifiable info, -With the express consent of a protected entity for which such cybersecurity provider is providing goods or services for cybersecurity purposes. (Sec. 6 at p. 10; Sec. 2 at p. 4)	-Notwithstanding any provision of law, -"Cybersecurity threat indicator:" information that 'may be indicative or describe,' -Eight types of cyber data, -From which reasonable efforts have been made to remove info that can be used to identify specific persons unrelated to the cybersecurity threat. (Sec. 708(6))	-Notwithstanding any provision of law -"Cyber threat information:" information that 'may be indicative or describe,' -Nine types of cyber data, -"If the CTI described in paragraph (1) is obtained, in the course of services to another entity, that entity shall, at any time prior to disclosure of such information, be given a reasonable opportunity to authorize or prevent such disclosure or to request anonymization of such information." (Sec. 101(4))

	H.R. 3674, the PRECISE Act of 2011 (Lungren)	H.R. 3523, the CISPA of 2011 (Rogers-Ruppersberger)	S. 2105, the CSA of 2012 (Lieberman-Feinstein)	S. 2151, the SECURE IT Act of 2012 (McCain)
WHO MAY RECEIVE CYBERSECURIT Y RELATED INFORMATION	-New semi-private entity called the National Information Sharing Organization (NISO), which will be overseen by a board of government and private sector officials, and include a membership of cyber related companies federal agencies. The NISO will be responsible for distributing cyber info amongst its members and to the public. (Sec. 248(a)(2) and(3)).	-Any private or governmental entity if the protected entity gives consent, including military agencies such as the NSA or DoD. (Sec. 2(b) at p. 4-5).	- Any private entity (Sec. 3(a)), -DHS approved private exchanges (Sec. 4(e)), -DHS approved government exchanges including one lead exchange (Sec. 4(c)) and possibly additional ones if so approved by DHS (Sec. 4(d)).	- Six existing federal 'cybersecurity centers' including the NSA, and offices at DHS, DoD, DNI, and the FBI(Sec. 101(5)), -'Any other entity in order to assist with preventing, investigating, or otherwise mitigating threats to info security.' (Sec. 102(a)(2).
HOW MAY INFORMATION BE USED / REDISTRIBUTED	-Federal government and private entities may use for CS purposes (Sec. 248(b)(3-4) at p. 38-39), -Federal government may additionally use 1) to further investigation or the prosecution of a cybersecurity related criminal act as defined at 248(f)(2)on p. 43; or 2) to disclose the info to the appropriate congressional committee, -Note: stripping unnecessary PII before dissemination listed in mission and activities (Sec. 242(1)(A) at p. 27).	-Federal government may use for any lawful purpose only if (A) not for regulatory purposes; and B) at least one significant purpose is cybersecurity or national security (Rogers/Ruppersberger amdt, available at HPSCI website).	-Private entities can use, retain or further disclose in order to protect info systems from CS threats or mitigate CS threats (Sec. 702(b)), -Exchanges and government can use, retain or further disclose in order to protect info systems from CS threats or mitigate CS threats (Sec. 704(b) and (c)), -Government can disclose to law enforcement if information appears to pertain to a crime which has been, is being or is about to be committed (Sec. 704(g)(2)).	-CTI given to a cybersecurity center may be disclosed to and used by the government for cybersecurity or national security purposes or to prosecute any of the offenses listed in 18 USC 2516 (wiretapping predicates); may also be used by communication or cybersecurity provider for 'purposes related to such services' (Sec. 102(c)), -May be shared with local and state law enforcement for criminal or CS purposes (Sec. 102(c)).

	H.R. 3674, the PRECISE Act of 2011 (Lungren)	H.R. 3523, the CISPA of 2011 (Rogers-Ruppersberger)	S. 2105, the CSA of 2012 (Lieberman-Feinstein)	S. 2151, the SECURE IT Act of 2012 (McCain)
EXPANSION OF PRIVATE MONITORING/SURVEILLANCE **and** **AUTHORIZATION TO TAKE COUNTERMEASURES**	-Notwithstanding any other provision of law, CS providers with the express consent of a protected entity and self-protected entities may use 'CS systems to identify and obtain cyber threat information to protect the rights and property of such protected entity'(Sec 248(a) at p.36-37).	-'Notwithstanding any other provision of law, a CS provider, with the express consent of a protected entity for which such CS provider is providing goods or services for CS purposes, or self-protected entity may use 'CS systems to identify and obtain cyber threat information to protect the rights and property of such protected entity' (Sec 2(b) at p. 4-5).	-Notwithstanding ECPA, FISA, or the Communications Act, any private entity may monitor its info systems and info that is stored on, processed by or transiting such info for cyber threats, and monitor 3rd party if it lawfully authorizes such monitoring(701(1-2)); or operate countermeausres on own or 3rd party's info systems if it lawfully authorizes such monitoring (701(3-4)).	-'Notwithstanding any other provision of law, a private entity may, 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, employ countermeasures and use cybersecurity systems in order to obtain, identify or otherwise possess cyber threat information' (Sec. 102(a)(1)).
LIABILITY PROTECTION / IMMUNITY	-Provided against tort or criminal right of action in Fed or State court for failure to warn or disclose, provided the info is shared with NISO (sec. 248(b)(7) at p. 39), -Private right of action to sue private entity if it uses info for any purpose other than a cybersecurity purpose; subject to good faith defense (Keating amdt; available on HHSC website).	-Against a CS provider or protected entity acting in good faith for 'using cybersecurity systems or sharing info' or 'for not acting on information obtained or shared in accordance with this section' (Sec. 2(b)(3) at p. 6).	-For monitoring (706(a)(1)), -For sharing with exchange, CI operators, customers of CS services or any other entity if an exchange is notified (706(a)(2)), -Complete bar for 'good faith' reliance on Title VII of the bill (706(b)).	-For any entity for use, receipt or disclosure of cyber threat information or subsequent action or inaction of any lawful recipient of cyber threat information; (102(g)), -Additionally for private entities for taking countermeasures (102(g)).

	H.R. 3674, the PRECISE Act of 2011 (Lungren)	H.R. 3523, the CISPA of 2011 (Rogers-Ruppersberger)	S. 2105, the CSA of 2012 (Lieberman-Feinstein)	S. 2151, the SECURE IT Act of 2012 (McCain)
FURTHER GUIDANCE/RULES ON SHARING PRIVATE INFORMATION	-NISO charter shall include protections of privacy and civil liberties including A) transparency and oversight, B) ensure only CTI is shared with NISO, C) omit PII not necessary describe a cyber threat from info shared with and by the NISO (Sec 244(9) at p. 33), --Within 90 days, board of NISO shall issue procedures including protection of privacy rights and civ libs (Sec. 248(d) at p. 40), --Mission includes 'ensuring that the information exchanged shall be stripped of all information identifying the submitted and of any unnecessary personally identifiable information' (Sec. 242 (1)(A) at p. 27).	-none	-DHS shall issue policies on privacy and civil liberties for government receipt, retention, use and disclosure of CTI under bill; must be approved by AG within one year of passage of this act; policies must be sent to Congress (704(g)(4)), -AG shall establish mandatory program to monitor and oversee compliance with policies and procedures (704(g)(5)).	-The head of each of the six named cybersecurity centers shall submit procedures to congress within 60 days that shall ensure CTI 'is handled by the federal government in a reasonable manner, including consideration of the need to protect the privacy and civil liberties of individuals through anonymization or other appropriate methods, while fully accomplishing the objectives of this title.' (102(d)).

	H.R. 3674, the PRECISE Act of 2011 (Lungren)	H.R. 3523, the CISPA of 2011 (Rogers-Ruppersberger)	S. 2105, the CSA of 2012 (Lieberman-Feinstein)	S. 2151, the SECURE IT Act of 2012 (McCain)
OVERSIGHT	-Annual independent audits by a private firm to be appointed by NISO and approved by DHS. Shall be shared with DHS, the Homeland Security Committees, shall be made public with appropriate redactions, and may include a classified annex (Sec. 249 at p. 46).	-Annual audits by DNI IG on type and use of information shared under the program, including a review of actions taken by the Federal government and impacts on privacy and civil liberties; shall be submitted in unclassified form, but may include a classified annex (Rep. Mike Thompson amdt, available on HPSCI website).	-Annual report to Congress from privacy and civil liberties officers of DOJ, DHS and other appropriate agencies on government exchanges (Sec. 704(g)(5)(C)), -PCLOB report to Congress two years after enactment (Sec. 704(g)(6)), -Report on implementation to include discussion on civ libs (Sec. 707(h)).	-One year after enactment then every two years thereafter, the heads of the six cybersecurity centers, in consultation with their civil liberties officers, shall report to congress concerning the implementation of this title. It shall include a review of the type of information shared, impacts on privacy, government use of information and a description of any violations by the Federal government. Shall be unclassified by may include classified annex (Sec. 104).
ACCOUNTABILITY MEASURES	-Government, NISO and member entities may not knowingly publish, divulge, disclose or make known in any manner… any CTI protected from disclosure by this title; Violations shall be fined under Title 18, imprisoned for not more than one year, or both, and shall be removed from office or employment (Sec. 250(a) and (b) at p. 47-48).	-none	-The heads of federal entities that receive information shall inform AG of significant violations of the privacy and civil liberties policies required by the bill (704(g)(5)(B), -The heads of federal entities shall develop and enforce sanctions for officers employees, or agents who conduct activities under this title in violation of their duties or the policies required by this bill. (704(g)(7).	-none
EXEMPTION FROM PUBLIC DISCLOSURE LAWS	-FOIA -FACA	-FOIA	-FOIA	-FOIA