	H.R. 3523, the Cyber Intelligence sharing and Protection Act (CISPA) (Rogers-Ruppersberger)	S. 3414, the Cybersecurity Act of 2012 (Lieberman-Collins-Feinstein)	S. 3342, the SECURE IT Act of 2012, (McCain)
WHAT INFORMATION MAY BE SHARED	-Notwithstanding any provision of law, -"Cyber threat information:" information 'directly pertaining' to, -Four types of cyber data, -With the express consent of a protected entity for which such cybersecurity provider is providing goods or services for cybersecurity purposes,-A violation of terms of service may not serve as the sole basis for sharing of information under this law. (Sec. 2(b)(1) and((h)(4))	-Notwithstanding any provision of law, -"Cybersecurity threat indicator:" information that 'is reasonably necessary to 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, -A violation of terms of service may not serve as the sole basis for sharing of information under this law. (Sec. 708(7))	-Notwithstanding any provision of law -"Cyber threat information:" information that ' 'indicates or describes,' -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), 102(a)(3))

	H.R. 3523, CISPA (Rogers-Ruppersberger)	S. 3414, CSA (Lieberman-Collins-Feinstein)	S. 3342, SECURE IT (McCain)
WHO MAY RECEIVE CYBERSECURIT Y RELATED INFORMATION	-Any private or governmental entity if the protected entity gives consent, including military agencies such as the NSA or DoD. (Sec. 2(b)).	- Any private entity (Sec. 702(a)), -DHS approved private exchanges (Sec. 703(e)), -DHS approved government exchanges including one lead exchange (Sec. 703(c)) and possibly additional ones if so approved by DHS (Sec. 703(d)). Government exchanges must be civilian.	- 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	-Private entities may use information collected or shared for any purpose except to gain an unfair competitive advantage (Sec. 2(b)(3)), -Federal government may use for cybersecurity purposes, prosecuting cybersecurity crimes, protecting against or prosecution of crimes that risk life or limb, protecting against and prosecuting crimes against minors and to protect national security (Sec. 2(c)), -Federal government may not use library records, library patriot lists, book sale records, book customer lists, firearms sales records, tax return records, educational records or medical records (Sec. 2(c)),	-Private entities can use, retain or further disclose in order to protect info systems from CS threats or mitigate CS threats (Sec. 701(b),702(b)), -Private and government exchanges 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 further disclose information to law enforcement for cybersecurity purposes or if it appears to pertain to a cybersecurity crime, an imminent threat to life or limb, or serious crimes against minors (Sec.	- Private entities may use information collected or shared for any purpose except to gain an unfair competitive advantage (Sec. 102(e)), 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)(sec. 102(c)); -May be shared with local and state law enforcement for criminal or CS purposes (Sec. 102(c)).

	-Federal government may not affirmatively search cyber threat info except to prosecute cyber crimes (Sec. 2(c)).	704(g)(2)).	

	H.R. 3523, CISPA (Rogers-Ruppersberger)	S. 3414, CSA (Lieberman-Collins-Feinstein)	S. 3342, SECURE IT (McCain)
EXPANSION OF PRIVATE MONITORING/SURVEILLANCE **and** **AUTHORIZATION TO TAKE COUNTERMEASURES**	-'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)).	-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 seven types of indicators, and monitor a 3rd party system for the same if it provides express prior consent (Sec. 701(1)(4)). -Operate countermeausres on own or 3rd party's info systems if it provides express prior consent (Sec. 701(2) and-(5)).	-'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	-For using cybersecurity systems to identify or obtain cyber threat information, -For sharing such information, and -For decisions made based on cyber threat information identified, obtained, or shared under this section (Sec. 2(b)(4)), -For choosing not to participate in information sharing (Sec. 2(g)).	-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 reasonable good faith reliance on Title VII of the bill (706(b)), -But not for knowing or grossly negligent violations of this title or the regs promulgated under this title (Sec. 706(g))	-For use of cybersecurity systems and countermeasures, -For use, receipt or disclosure of cyber threat information -For action or inaction of any lawful recipient of cyber threat information; (102(g)).

	H.R. 3523, CISPA (Rogers-Ruppersberger)	S. 3414, CSA (Lieberman-Collins-Feinstein)	S. 3342, SECURE IT (McCain)
FURTHER GUIDANCE/RULES ON SHARING PRIVATE INFORMATION	-none	-DHS, in consultation with the DNI and AG, 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 and information sharing cannot begin until he does so; policies must be sent to Congress in unclassified form and be made public, but may include a classified annex (Sec. 704(g)(3)), -AG shall establish mandatory program to monitor and oversee compliance with policies and procedures (Sec. 704(g)(4)).	-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, and the Federal government may undertake efforts consistent with this subparagraph to limit the impact on privacy and civil liberties of the sharing of cyber threat information with the Federal government.' (102(d)).

	H.R. 3523, CISPA (Rogers-Ruppersberger)	S. 3414, CSA (Lieberman-Collins-Feinstein)	S. 3342, SECURE IT (McCain)
OVERSIGHT	-Annual Inspector General reports 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 (Sec. 2(e)).	-Annual report to Congress from privacy and civil liberties officers of DOJ, DHS and other appropriate agencies on government exchanges and monitoring, countermeasures and sharing practices of private entities(Sec. 704(g)(5)), -Unclassified PCLOB report to Congress two years after enactment, and every two years thereafter (Sec. 704(g)(5)), -Report on implementation to include discussion on civ libs (Sec. 707(h)). -Annual Inspector General reports from DOJ, IC and DoD to include information on what info is shared, who receives it and how it is used; shall be submitted in unclassified form, but may include classified annex (Sec. 704(g)(5)).	-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 and include classified annex (Sec. 105).

ACCOUNTABILITY MEASURES	-Federal entities are liable for $1,000 or actual damages (whichever is greater) for intentional or willful violations of this title or its regulations (Sec. 2(d)).	-Federal entities are liable for $1,000 or actual damages (whichever is greater) for intentional or willful violations of this title or its regulations (Sec. 704(g)(7)). -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)(4)(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)(6).	-none
EXEMPTION FROM PUBLIC DISCLOSURE LAWS	-FOIA (Sec. 2(b)(5)).	-FOIA (Sec. 704(d)).	-FOIA (Sec. 102(c)(5)).

Miscellaneous	-Five year sunset on CISPA (Sec. 3).	--Nothing in this title shall limit or modify existing information sharing relationships, prohibit a new information sharing relationship or require a new information sharing relationship (Sec. 707(a)(3)). -Nothing in this title may be construed to permit a Federal entity…to condition the award of any Federal grant, contract or purchase on the provision of cybersecurity threat indicators to a Federal entity, if the provision of such indicators does not reasonably relate to the nature of activities, goods or services covered by the award(Sec. 707(e).	--Nothing in this title shall limit or modify existing information sharing relationships, prohibit a new information sharing relationship or require a new information sharing relationship (Sec. 104(a)).