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

	-'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)). -'No civil or criminal cause of actin shall lie…for decisions made based on cyber threat information identified, obtained, or shared under this section' (Sec 4(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 system 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)).
	-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. (Sec. 102(g))

	-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).

	-Five year sunset on CISPA (Sec. 3).	-Nothing in this title shall limit or modify existing information sharing relationships, prohibit a new information s	