Cybersecurity Information Sharing Act (CISA, S. 754) Amendment Analysis

Sponsor	Amendment No.	Issue	Summary	OTI Position
Whitehouse	2626	Computer Crime Authority	Authorizes the court to issue an order compelling private sector entities to hack into people's computers and networks: -Immunizes companies from liability for helping government hack, regardless of harm, and establishes authority to reimburse companies for expenses incurred Significantly expands violations and penalties for violating CFAA in relation to critical infrastructure (CI): -Establishes penalty of up to 20 years in prison for harm to computers connected to CI that do not actually harm or interfere with operation of CI -Overbroad definition of CI that could include shopping malls, sports stadiums, and other places the public gathers	Strongly Oppose
Cotton	2581	Operation: Sharing	Incentivizes direct sharing with FBI by extending liability protections: -Reduces operational effectiveness; it undermines DHS's situational awareness -Harms privacy and civil liberties because FBI is not subject to privacy guidelines	Strongly Oppose
Burr/Feinstein	Manager's Amendment	Operation: Sharing Privacy and Civil Liberties: Government Uses Cybersecurity: Defensive Measures Oversight: Transparency	Sharing Authorization: Improves an operational and privacy concern by only allowing sharing for cybersecurity purposes -Does not address many outstanding operational and privacy issues Law Enforcement Uses: Removes authorization to use information in investigations into 18 USC 3559 violent felonies -Law enforcement would still be authorized to use information for many investigations unrelated to cyber threats Resolves concern that defensive measures would undermine cybersecurity by authorizing companies to violate the federal anti-hacking statute FOIA: Removes the new and unnecessary (b)(10) FOIA exemption	Strongly Support

FOR MORE INFORMATION, CONTACT ROBYN GREENE, POLICY COUNSEL,
NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE at greene@opentechinstitute.org.

Sponsor	Amendment No.	Issue	Summary	OTI Position
Franken	2612	Operation and Privacy: Definitions	Clarifies definition of Cybersecurity Threat: -Increases operational effectiveness and reduces sharing of information on false positives by ensuring companies only share information about events that are reasonably likely to result in harm Clarifies definition of Cyber Threat Indicator: -Ensures that more of the information shared is actionable by reducing sharing of unnecessary user content and PII	Strongly Support
Wyden	2621	Operation and Privacy: Protection of PII	Significant operational and privacy improvement - requirement to remove PII: -Protects PII by requiring as much of it as is feasible be removed unless it's necessary to describe or identify a threat -Would significantly increase how actionable the shared threat data is since PII is not actionable for security experts	Strongly Support
Heller	2548	Operation and Privacy: Protection of PII	Minimal improvement: Requirement to remove PII: -Requires PII removal if there is reasonable belief it isn't directly related to threat -Does not establish standard for efficacy of review for PII -Would still allow sharing of unnecessary victim information and other PII	Neutral
Coons	2552	Privacy: Second PII Scrub	Ensures DHS can remove unnecessary PII before disseminating indicators throughout government: -Incomplete fix because it does not require companies to share through DHS	Strongly Support
Carper	2615	Privacy: Second PII Scrub	Ensures DHS can remove unnecessary PII before disseminating indicators throughout government, and establishes standard for stripping PII: -Incomplete fix because it does not require companies to share through DHS	Strongly Support
Flake/Franken	2582	Oversight: Sunset	Establishes a six year sunset: -Improves oversight by ensuring Congress reviews effectiveness of authorities -Preserves liability protection for actions taken during authorization period	Strongly Support
Tester	2632	Oversight: Government Reporting	Enhances transparency by requiring government reporting on the efficacy of information sharing, how much person data is shared, and how often that data is used for purposes unrelated to cybersecurity	Strongly Support
Wyden	2622	Oversight: Notification of Improper Sharing	Requires the federal government to notify people if their PII was improperly shared	Support
Leahy	2587	Oversight: FOIA	Removes unnecessary de facto FOIA exemptions of all information shared: -Most information would already be protected under standing FOIA exemptions	Support
Vitter	2578	Oversight: Staff Security Clearances	Enhances oversight by requiring review and update of procedures to ensure one staffer for each member of relevant Committees can obtain security clearances	Support
Vitter	2579	Cybersecurity: Small Business Support	Bolsters DHS's resources to help small businesses enhance their cybersecurity: -Establishes a new DHS Small Business Cyber Security Operations Center -Appropriates funds to stand up Center for 3 year pilot program	Support
Coats	2604	Cybersecurity: Mobile Devices	Commissions DHS to study and issue a report on security threats to mobile devices	Support

FOR MORE INFORMATION, CONTACT ROBYN GREENE, POLICY COUNSEL,
NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE at greene@opentechinstitute.org.

Sponsor	Amendment No.	Issue	Summary	OTI Position
Mikulski	2557	Cybersecurity: Appropriations	Enhances cybersecurity by appropriating $37M for OPM emergency response to cyber attacks	Support
Gardner	2631	Cybersecurity: Report on Cyberspace Policy	Requires the Secretary of State to publically produce a strategy on elements of international cyberspace policy	Neutral
Carper	2627	Cybersecurity: Einstein Authorization	Authorizes DHS to make Einstein intrusion detection system available to deploy on federal networks -Includes emergency authorization for DHS to deploy intrusion detection and response capabilities	Neutral
Kirk	2603	Cybersecurity: Apprehension of International Cybercriminals	Requires the Secretary of State to consult with countries with whom the US doesn't have an MLAT or extradition treaty to: -Apprehend and prosecute people accused of committing cybercrimes or intellectual property crimes; -Work to prevent further commission of those crimes	Neutral
Paul	2564	Business Rights: Contracts	Protects the right to contract by ensuring liability protections don't override user agreements	Support
Flake	2580	Business Rights: Clarifies Voluntary Sharing	Restates that private sector to private sector sharing is voluntary	Neutral
Murphy	2589	Privacy: Human Rights and International Relations	Extends Privacy Act protections and ability to pursue a remedy for violations to non-U.S. persons	Support