LegiList
Congress, Made Clear.

Bill Fact Sheet – January 8, 2026
https://legilist.com
Bill page: https://legilist.com/bill/113/s/2588

S 2588

Cybersecurity Information Sharing Act of 2014

Congress: 113 (2013–2015, Ended)
Chamber: Senate
Policy Area: Government Operations and Politics
Introduced: Jul 10, 2014
Current Status: Placed on Senate Legislative Calendar under General Orders. Calendar No. 462.
Latest Action: Placed on Senate Legislative Calendar under General Orders. Calendar No. 462. (Jul 10, 2014)
Official Text: https://www.congress.gov/bill/113th-congress/senate-bill/2588

Sponsor

Name: Sen. Feinstein, Dianne [D-CA]
Party: Democratic • **State:** CA • **Chamber:** Senate

Cosponsors

No cosponsors are listed for this bill.

Committee Activity

Committee	Chamber	Activity	Date
Intelligence (Select) Committee	Senate	Reported Original Measure	Jul 10, 2014

Subjects & Policy Tags

Policy Area:

Government Operations and Politics

Related Bills

No related bills are listed.

Summary (as of Jul 10, 2014)

Cybersecurity Information Sharing Act of 2014 - Requires the Director of National Intelligence (DNI), the Secretary of Homeland Security (DHS), the Secretary of Defense (DOD), and the Attorney General (DOJ) to develop and promulgate procedures for classified and declassified cyber threat indicators in possession of the federal government to be shared in real time with private entities; non-federal government agencies; or state, tribal, or local governments. Provides for the public availability of unclassified indicators.

Permits private entities to monitor and operate countermeasures to prevent or mitigate cybersecurity threats or security vulnerabilities on their own information systems and, with written consent, the information systems of other entities and federal entities. Authorizes such entities to monitor information that is stored on, processed by, or transiting such monitored systems.

Allows entities to share and receive indicators and countermeasures with other entities or the federal government.

Permits state, tribal, or local agencies to use shared indicators (with the consent of the agency sharing the indicators) to prevent, investigate, or prosecute computer crimes.

Directs the Attorney General to: (1) promulgate procedures relating to the receipt of indicators and countermeasures by the federal government; and (2) develop privacy and civil liberties guidelines to limit receipt, retention, use, and dissemination of personal or identifying information.

Directs the DHS Secretary to develop a process for the federal government to: (1) accept cyber threat indicators and countermeasures from entities in an electronic format; and (2) distribute such indicators and countermeasures to appropriate federal entities in real time, simultaneous with receipt. Requires the DHS Secretary to certify to Congress that such capability is fully operational before the process is implemented.

Requires the Federal Bureau of Investigation (FBI) and the DHS Secretary to report to Congress regarding implementation of an automated malware analysis capability, including an assessment of the advisability of transferring the operation of such capability to DHS.

Authorizes indicators and countermeasures to be disclosed to, retained by, and used by, consistent with otherwise applicable federal law, any federal agency or federal government agent solely for: (1) protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability; (2) responding to, or otherwise preventing or mitigating, an imminent threat of death or serious bodily harm or threat to a minor; or (3) investigating or prosecuting an offense arising out of a threat of death or serious bodily harm, as well as offenses relating to fraud and identity theft, espionage and censorship, and trade secrets.

Prohibits government agencies from using indicators and countermeasures provided to the federal government to regulate the lawful activities of an entity.

Provides liability protections to entities acting in accordance with this Act that: (1) monitor information systems, and (2) share and receive indicators and countermeasures. Makes an entity's good faith reliance that conduct was permitted under this Act a complete defense to a cause of action based on such monitoring and sharing activities.

Actions Timeline

- **Jul 10, 2014:** Introduced in Senate
- **Jul 10, 2014:** Select Committee on Intelligence. Original measure reported to Senate by Senator Feinstein. Without written report.
- **Jul 10, 2014:** Placed on Senate Legislative Calendar under General Orders. Calendar No. 462.