S 2102

Cybersecurity Information Sharing Act of 2012

Congress: 112 (2011–2013, Ended)
Chamber: Senate
Policy Area: Government Operations and Politics
Introduced: Feb 13, 2012
Current Status: Read twice and referred to the Committee on Homeland Security and Governmental Affairs.
Latest Action: Read twice and referred to the Committee on Homeland Security and Governmental Affairs. (Feb 13, 2012)
Official Text: https://www.congress.gov/bill/112th-congress/senate-bill/2102

Sponsor

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

Cosponsors (1 total)

Cosponsor	Party / State	Role	Date Joined
Sen. Mikulski, Barbara A. [D-MD]	D · MD		Feb 13, 2012

Committee Activity

Committee	Chamber	Activity	Date
Homeland Security and Governmental Affairs Committee	Senate	Referred To	Feb 14, 2012

Subjects & Policy Tags

Policy Area:

Government Operations and Politics

Related Bills

Bill	Relationship	Last Action
112 S 3414	Related bill	**Nov 14, 2012:** Upon reconsideration, cloture on the bill not invoked in Senate by Yea-Nay Vote. 51 - 47. Record Vote Number: 202. (consideration: CR S6784; text: CR S6784)
112 S 2105	Related bill	**Feb 16, 2012:** Committee on Homeland Security and Governmental Affairs. Hearings held. Hearings printed: S.Hrg. 112-524.

Summary (as of Feb 13, 2012)

Cybersecurity Information Sharing Act of 2012 - Authorizes private entities to monitor information systems for cybersecurity threats and operate countermeasures for protection, including the information systems of third parties authorizing such measures.

Allows private entities to disclose lawfully obtained cybersecurity threat indicators to any other private entity, provided that the entities: (1) make efforts to safeguard information that can be used to identify specific persons, (2) comply with lawful use or disclosure restrictions, (3) not use the indicators to gain an unfair competitive advantage, and (4) use the indicators only for the purpose of protecting against or mitigating cybersecurity threats.

Directs the Secretary of Homeland Security (DHS) to establish processes and procedures for: (1) designating appropriate federal and non-federal entities as cybersecurity exchanges, (2) sharing classified and unclassified cybersecurity threat information with designated cybersecurity exchanges and other appropriate entities, and (3) identifying certified entities to receive such classified information.

Directs the Secretary to designate a federal entity as the lead cybersecurity exchange for cybersecurity information sharing among federal entities and with non-federal entities.

Allows a non-federal entity to disclose lawfully obtained cybersecurity threat information to an exchange.

Requires the Secretary to develop policies and procedures that govern a federal entity's receipt, retention, use, and disclosure of cybersecurity threat information in a manner that minimizes the impact on privacy and civil liberties. Directs: (1) the Secretary and the Attorney General (DOJ) to establish a mandatory program to oversee compliance with such policies and procedures, and (2) the heads of federal entities to develop and enforce appropriate sanctions for officers, employees, or agents of the federal entities who conduct prohibited activities.

Provides legal protections for entities engaged in cybersecurity monitoring activities, including a good faith defense.

Actions Timeline

- **Feb 13, 2012:** Introduced in Senate
- **Feb 13, 2012:** Sponsor introductory remarks on measure. (CR S568-569)
- **Feb 13, 2012:** Read twice and referred to the Committee on Homeland Security and Governmental Affairs.