S 2105

Cybersecurity Act of 2012

Congress: 112 (2011–2013, Ended)
Chamber: Senate
Policy Area: Government Operations and Politics
Introduced: Feb 14, 2012
Current Status: Committee on Homeland Security and Governmental Affairs. Hearings held. Hearings printed: S.Hrg. 112
Latest Action: Committee on Homeland Security and Governmental Affairs. Hearings held. Hearings printed: S.Hrg. 112-524. (Feb 16, 2012)
Official Text: https://www.congress.gov/bill/112th-congress/senate-bill/2105

Sponsor

Name: Sen. Lieberman, Joseph I. [ID-CT]
Party: Democratic • **State:** CT • **Chamber:** Senate

Cosponsors (4 total)

Cosponsor	Party / State	Role	Date Joined
Sen. Collins, Susan M. [R-ME]	R · ME		Feb 14, 2012
Sen. Feinstein, Dianne [D-CA]	D · CA		Feb 14, 2012
Sen. Rockefeller, John D., IV [D-WV]	D · WV		Feb 14, 2012
Sen. Whitehouse, Sheldon [D-RI]	D · RI		Feb 15, 2012

Committee Activity

Committee	Chamber	Activity	Date
Homeland Security and Governmental Affairs Committee	Senate	Hearings By (full committee)	Feb 16, 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 2151	Related bill	**Mar 1, 2012:** Read twice and referred to the Committee on Commerce, Science, and Transportation.
112 S 2102	Related bill	**Feb 13, 2012:** Read twice and referred to the Committee on Homeland Security and Governmental Affairs.

Summary (as of Feb 14, 2012)

Cybersecurity Act of 2012 - Directs the Secretary of Homeland Security (DHS), in consultation with owners and operators of critical infrastructure, the Critical Infrastructure Partnership Advisory Council, and other federal agencies and private sector entities, to: (1) to conduct a top-level assessment of cybersecurity risks to determine which sectors face the greatest immediate risk, and beginning with the sectors identified as having the highest priority, conduct, on a sector-by-sector basis, cyber risk assessments of the critical infrastructure; (2) establish a procedure for the designation of critical infrastructure; (3) identify or develop risk-based cybersecurity performance requirements; and (4) implement cyber response and restoration plans. Sets forth requirements for securing critical infrastructure, including notification of cyber risks and threats and reporting of significant cyber incidents affecting critical infrastructure.

Defines "critical infrastructure" as systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, or national public health or safety.

Amends the Federal Information Security Management Act of 2002 (FISMA) to revise information security requirements for federal agencies and provide for continuous monitoring of, and streamlined reporting of, cybersecurity risks.

Amends the Homeland Security Act of 2002 to consolidate existing DHS resources for cybersecurity within a National Center for Cybersecurity and Communications. Sets forth the duties of the Center, including managing efforts to secure, protect, and ensure the resiliency of the federal information infrastructure, supporting private sector efforts to protect such infrastructure, prioritizing efforts to address the most significant risks to the information infrastructure, and ensuring privacy protections.

Requires: (1) the DHS Secretary to implement outreach and awareness programs on cybersecurity; (2) the DHS Secretary and the Secretary of Commerce to establish a program to identify, develop, and recruit talented individuals to work in cybersecurity; (3) the Director of the National Science Foundation (NSF) to establish a program to stimulate innovation in basic cybersecurity research and development and to recruit and train cybersecurity professionals; and (4) the Director of the Office of Personnel Management (OPM) to assess the readiness and capacity of the federal workforce to meet cybersecurity needs and to establish a cybersecurity awareness and education curriculum for all federal employees and contractors.

Requires the Secretary of Education to develop model curriculum standards to address cybersecurity issues for elementary school students and for students in institutions of higher education and career and technical institutions.

Requires federal agencies to adopt OPM best practices for motivating employees to demonstrate leadership in cybersecurity.

Requires the Director of the Office of Science and Technology Policy to develop a national cybersecurity research and development plan to advance the development of new technologies to protect against evolving cyberthreats.

Requires the DHS Secretary to coordinate with private sector and academic experts, the Secretaries of Defense (DOD), Commerce, and State, the Director of National Intelligence (DNI), and other federal agencies to develop and periodically update an acquisition risk management strategy to ensure the security of the federal information infrastructure.

Authorizes private entities to disclose or receive lawfully obtained cybersecurity threat information to protect an information system. Establishes a process to designate cybersecurity exchanges for distributing, receiving, and

exchanging cybersecurity threat information. Allows a non-federal entity to disclose lawfully obtained cybersecurity threat information to an exchange. Provides legal protections for entities engaged in cybersecurity monitoring activities, including a good faith defense.

Directs the DHS Secretary and the Secretary of Defense (DOD) to report to Congress annually on major cyber incidents involving networks of executive agencies and military departments. Requires the Attorney General and the Director of the Federal Bureau of Investigation (FBI) to report on investigations and prosecutions of cybercrimes. Requires the Attorney General to report on the ability of federal courts to grant timely relief in matters relating to cybercrime.

Requires the DHS Secretary to report on: (1) available technical options to enhance the security of critical infrastructure, (2) legal or other impediments to public awareness of cybersecurity threats, and (3) the national security implications of a disruption of the U.S. electric grid caused by a cyber attack.

Expresses the sense of Congress with respect to engaging in international cooperation to advance U.S. cyberspace objectives and combat cybercrime. Authorizes the Secretary of State to designate a senior State Department official to coordinate diplomatic efforts on the full range of international cyber issues. Requires the Secretary to assess and report on significant global issues, trends, and actors with respect to cybercrime and to give priority in foreign assistance to programs designed to combat cybercrime.

Actions Timeline

- **Feb 16, 2012:** Committee on Homeland Security and Governmental Affairs. Hearings held. Hearings printed: S.Hrg. 112-524.
- **Feb 15, 2012:** Read the second time. Placed on Senate Legislative Calendar under General Orders. Calendar No. 323.
- **Feb 14, 2012:** Introduced in Senate
- **Feb 14, 2012:** Sponsor introductory remarks on measure. (CR S616-618)
- **Feb 14, 2012:** Introduced in the Senate. Read the first time. Placed on Senate Legislative Calendar under Read the First Time.