S 2521

Federal Information Security Modernization Act of 2014

Congress: 113 (2013–2015, Ended)
Chamber: Senate
Policy Area: Government Operations and Politics
Introduced: Jun 24, 2014
Current Status: Became Public Law No: 113-283.
Latest Action: Became Public Law No: 113-283. (Dec 18, 2014)
Law: 113-283 (Enacted Dec 18, 2014)
Official Text: https://www.congress.gov/bill/113th-congress/senate-bill/2521

Sponsor

Name: Sen. Carper, Thomas R. [D-DE]
Party: Democratic • **State:** DE • **Chamber:** Senate

Cosponsors (1 total)

Cosponsor	Party / State	Role	Date Joined
Sen. Coburn, Tom [R-OK]	R · OK		Jun 24, 2014

Committee Activity

Committee	Chamber	Activity	Date
Homeland Security and Governmental Affairs Committee	Senate	Reported By	Sep 15, 2014
Homeland Security Committee	House	Bills of Interest - Exchange of Letters	Aug 1, 2014

Subjects & Policy Tags

Policy Area:

Government Operations and Politics

Related Bills

Bill	Relationship	Last Action
113 HR 1163	Related bill	**Apr 17, 2013:** Received in the Senate and Read twice and referred to the Committee on Homeland Security and Governmental Affairs.

Summary (as of Dec 18, 2014)

(This measure has not been amended since it was passed by the Senate on December 8, 2014. The summary of that version is repeated here.)

Federal Information Security Modernization Act of 2014 - Amends the Federal Information Security Management Act of 2002 (FISMA) to: (1) reestablish the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices, and (2) set forth authority for the Secretary of Homeland Security (DHS) to administer the implementation of such policies and practices for information systems.

Requires the Secretary to develop and oversee implementation of operational directives requiring agencies to implement the Director's standards and guidelines for safeguarding federal information and systems from a known or reasonably suspected information security threat, vulnerability, or risk. Authorizes the Director to revise or repeal operational directives that are not in accordance with the Director's policies.

Requires the Secretary (currently, the Director) to ensure the operation of the federal information security incident center (FISIC).

Directs the Secretary to administer procedures to deploy technology, upon request by an agency, to assist the agency to continuously diagnose and mitigate against cyber threats and vulnerabilities.

Requires the Director's annual report to Congress regarding the effectiveness of information security policies to assess agency compliance with OMB data breach notification procedures.

Provides for OMB's information security authorities to be delegated to the Director of National Intelligence (DNI) for certain systems operated by an element of the intelligence community.

Directs the Secretary to consult with and consider guidance developed by the National Institute of Standards and Technology (NIST) to ensure that operational directives do not conflict with NIST information security standards.

Directs agency heads to ensure that: (1) information security management processes are integrated with budgetary planning; (2) senior agency officials, including chief information officers, carry out their information security responsibilities; and (3) all personnel are held accountable for complying with the agency-wide information security program.

Provides for the use of automated tools in agencies' information security programs, including for periodic risk assessments, testing of security procedures, and detecting, reporting, and responding to security incidents.

Requires agencies to include offices of general counsel as recipients of security incident notices. Requires agencies to notify Congress of major security incidents within seven days after there is a reasonable basis to conclude that a major incident has occurred.

Directs agencies to submit an annual report regarding major incidents to OMB, DHS, Congress, and the Comptroller General (GAO). Requires such reports to include: (1) threats and threat actors, vulnerabilities, and impacts; (2) risk assessments of affected systems before, and the status of compliance of the systems at the time of, major incidents; (3) detection, response, and remediation actions; (4) the total number of incidents; and (5) a description of the number of individuals affected by, and the information exposed by, major incidents involving a breach of personally identifiable information.

Authorizes GAO to provide technical assistance to agencies and inspectors general, including by testing information security controls and procedures.

Requires OMB to ensure the development of guidance for: (1) evaluating the effectiveness of information security programs and practices, and (2) determining what constitutes a major incident.

Directs FISIC to provide agencies with intelligence about cyber threats, vulnerabilities, and incidents for risk assessments.

Directs OMB, during the two-year period after enactment of this Act, to include in an annual report to Congress an assessment of the adoption by agencies of continuous diagnostics technologies and other advanced security tools.

Requires OMB to ensure that data breach notification policies require agencies, after discovering an unauthorized acquisition or access, to notify: (1) Congress within 30 days, and (2) affected individuals as expeditiously as practicable. Allows the Attorney General, heads of elements of the intelligence community, or the DHS Secretary to delay notice to affected individuals for purposes of law enforcement investigations, national security, or security remediation actions.

Requires OMB to amend or revise OMB Circular A-130 to eliminate inefficient and wasteful reporting.

Directs the Information Security and Privacy Advisory Board to advise and provide annual reports to DHS.

Actions Timeline

- **Dec 18, 2014:** Signed by President.
- **Dec 18, 2014:** Became Public Law No: 113-283.
- **Dec 12, 2014:** Presented to President.
- **Dec 10, 2014:** Mr. Meadows asked unanimous consent to take from the Speaker's table and consider.
- **Dec 10, 2014:** Considered by unanimous consent. (consideration: CR H8994-8998)
- **Dec 10, 2014:** Passed/agreed to in House: On passage Passed without objection.(text: CR H8994-8998)
- **Dec 10, 2014:** On passage Passed without objection. (text: CR H8994-8998)
- **Dec 10, 2014:** Motion to reconsider laid on the table Agreed to without objection.
- **Dec 9, 2014:** Received in the House.
- **Dec 9, 2014:** Message on Senate action sent to the House.
- **Dec 9, 2014:** Held at the desk.
- **Dec 8, 2014:** Measure laid before Senate by unanimous consent. (consideration: CR S6395)
- **Dec 8, 2014:** Passed/agreed to in Senate: Passed Senate with an amendment by Voice Vote.
- **Dec 8, 2014:** Passed Senate with an amendment by Voice Vote.
- **Sep 15, 2014:** Committee on Homeland Security and Governmental Affairs. Reported by Senator Carper without amendment. With written report No. 113-256.
- **Sep 15, 2014:** Placed on Senate Legislative Calendar under General Orders. Calendar No. 564.
- **Jun 25, 2014:** Committee on Homeland Security and Governmental Affairs. Ordered to be reported without amendment favorably.
- **Jun 24, 2014:** Introduced in Senate
- **Jun 24, 2014:** Read twice and referred to the Committee on Homeland Security and Governmental Affairs.