HR 1163

Federal Information Security Amendments Act of 2013

Congress: 113 (2013–2015, Ended)
Chamber: House
Policy Area: Government Operations and Politics
Introduced: Mar 14, 2013
Current Status: Received in the Senate and Read twice and referred to the Committee on Homeland Security and Governm
Latest Action: Received in the Senate and Read twice and referred to the Committee on Homeland Security and Governmental Affairs. (Apr 17, 2013)
Official Text: https://www.congress.gov/bill/113th-congress/house-bill/1163

Sponsor

Name: Rep. Issa, Darrell E. [R-CA-49]
Party: Republican • **State:** CA • **Chamber:** House

Cosponsors (5 total)

Cosponsor	Party / State	Role	Date Joined
Rep. Connolly, Gerald E. [D-VA-11]	D · VA		Mar 14, 2013
Rep. Cummings, Elijah E. [D-MD-7]	D · MD		Mar 14, 2013
Rep. Mica, John L. [R-FL-7]	R · FL		Mar 14, 2013
Rep. Chaffetz, Jason [R-UT-3]	R · UT		Mar 21, 2013
Rep. Tierney, John F. [D-MA-6]	D · MA		Mar 21, 2013

Committee Activity

Committee	Chamber	Activity	Date
Homeland Security and Governmental Affairs Committee	Senate	Referred To	Apr 17, 2013
Homeland Security Committee	House	Bills of Interest - Exchange of Letters	Aug 1, 2014
Oversight and Government Reform Committee	House	Reported By	Apr 16, 2013

Subjects & Policy Tags

Policy Area:

Government Operations and Politics

Related Bills

Bill	Relationship	Last Action
113 S 2521	Related bill	**Dec 18, 2014:** Became Public Law No: 113-283.
113 HR 3032	Related bill	**Sep 16, 2013:** Referred to the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies.

Summary (as of Apr 16, 2013)

Federal Information Security Amendments Act of 2013 - (Sec. 2) Amends the Federal Information Security Management Act of 2002 (FISMA) to reestablish the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information and security policies and practices.

Extends the security requirements of federal agencies to include responsibilities for: (1) complying with computer standards developed by the National Institute of Standards and Technology (NIST); (2) ensuring complementary and uniform standards for information systems and national security systems; (3) ensuring that information security management processes are integrated with budget processes; (4) securing facilities for classified information; (5) maintaining sufficient personnel with security clearances; and (6) ensuring that information security performance indicators are included in the annual performance evaluations of all managers, senior managers, senior executive service personnel, and political appointees.

Directs senior agency officials, with a frequency sufficient to support risk-based security decisions, to: (1) test and evaluate information security controls and techniques, and (2) conduct threat assessments by monitoring information systems and identifying potential system vulnerabilities. (Current law requires only periodic testing and evaluation.)

Defines "information system" as a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Includes in such definition: (1) computers and computer networks; (2) ancillary equipment; (3) software, firmware, and related procedures; (4) support services; and (5) related resources and services.

Directs agencies to determine information security levels in accordance with information security classifications and standards promulgated under the National Institute of Standards and Technology Act.

Directs agencies to collaborate with OMB and appropriate public and private sector security operations centers on security incidents that extend beyond the control of an agency. Requires that security incidents be reported, through an automated and continuous monitoring capability, when possible, to the federal information security incident center (the incident center), appropriate security operations centers, and agency Inspector General.

Directs agencies to conduct vulnerability assessments and penetration tests commensurate with the risk posed to agency information systems.

Requires each agency to delegate to its Chief Information Officer the authority and primary responsibility for developing, implementing, and overseeing an agencywide information security (AIS) program.

Directs agencies to implement an OMB-approved AIS program that is consistent with components across and within agencies. Requires that such program include automated and continuous monitoring, when possible, to: (1) mitigate risks associated with security incidents before substantial damage is done; and (2) notify and consult with the incident center, appropriate security operations response centers, law enforcement agencies, Inspectors General, and other entities or as directed by the President.

Directs the OMB Director to review and approve information security policies and procedures to ensure that the incident center has the capability to detect, correlate, and respond to incidents that impair the security of multiple agencies' information systems. Requires the capability, where practicable, to be continuous and technically automated.

(Sec. 4) Specifies that no additional funds are authorized for agencies to carry out their responsibilities under this Act.

Requires agencies to carry out such responsibilities using amounts otherwise authorized or appropriated.

Actions Timeline

- **Apr 17, 2013:** Received in the Senate and Read twice and referred to the Committee on Homeland Security and Governmental Affairs.
- **Apr 16, 2013:** Reported (Amended) by the Committee on Oversight and Government Reform. H. Rept. 113-40.
- **Apr 16, 2013:** Placed on the Union Calendar, Calendar No. 26.
- **Apr 16, 2013:** Mr. Issa moved to suspend the rules and pass the bill, as amended.
- **Apr 16, 2013:** Considered under suspension of the rules. (consideration: CR H2037-2042)
- **Apr 16, 2013:** DEBATE - The House proceeded with forty minutes of debate on H.R. 1163.
- **Apr 16, 2013:** At the conclusion of debate, the Yeas and Nays were demanded and ordered. Pursuant to the provisions of clause 8, rule XX, the Chair announced that further proceedings on the motion would be postponed.
- **Apr 16, 2013:** Considered as unfinished business. (consideration: CR H2053-2054)
- **Apr 16, 2013:** Passed/agreed to in House: On motion to suspend the rules and pass the bill Agreed to by the Yeas and Nays: (2/3 required): 416 - 0 (Roll no. 106).(text: CR H2037-2039)
- **Apr 16, 2013:** On motion to suspend the rules and pass the bill Agreed to by the Yeas and Nays: (2/3 required): 416 - 0 (Roll no. 106). (text: CR H2037-2039)
- **Apr 16, 2013:** Motion to reconsider laid on the table Agreed to without objection.
- **Mar 20, 2013:** Committee Consideration and Mark-up Session Held.
- **Mar 20, 2013:** Ordered to be Reported by Voice Vote.
- **Mar 14, 2013:** Introduced in House
- **Mar 14, 2013:** Referred to the House Committee on Oversight and Government Reform.