

## HR 4257

### Federal Information Security Amendments Act of 2012

**Congress:** 112 (2011–2013, Ended)

**Chamber:** House

**Policy Area:** Government Operations and Politics

**Introduced:** Mar 26, 2012

**Current Status:** Received in the Senate and Read twice and referred to the Committee on Homeland Security and Government

**Latest Action:** Received in the Senate and Read twice and referred to the Committee on Homeland Security and Governmental Affairs. (May 7, 2012)

**Official Text:** <https://www.congress.gov/bill/112th-congress/house-bill/4257>

### Sponsor

**Name:** Rep. Issa, Darrell E. [R-CA-49]

**Party:** Republican • **State:** CA • **Chamber:** House

### Cosponsors (2 total)

Cosponsor	Party / State	Role	Date Joined
Rep. Cummings, Elijah E. [D-MD-7]	D · MD		Mar 26, 2012
Rep. Van Hollen, Chris [D-MD-8]	D · MD		Apr 26, 2012

### Committee Activity

Committee	Chamber	Activity	Date
Homeland Security and Governmental Affairs Committee	Senate	Referred To	May 7, 2012
Oversight and Government Reform Committee	House	Reported By	Apr 26, 2012

### Subjects & Policy Tags

#### Policy Area:

Government Operations and Politics

### Related Bills

Bill	Relationship	Last Action
112 S 413	Related bill	May 23, 2011: Committee on Homeland Security and Governmental Affairs. Hearings held. Hearings printed: S.Hrg. 112-221.
112 HR 1136	Related bill	Apr 1, 2011: Referred to the Subcommittee on Government Organization, Efficiency, and Financial Management.

Federal Information Security Amendments Act of 2012 - (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**

---

- **May 7, 2012:** Received in the Senate and Read twice and referred to the Committee on Homeland Security and Governmental Affairs.
- **Apr 26, 2012:** Reported (Amended) by the Committee on Oversight and Government Reform. H. Rept. 112-455.
- **Apr 26, 2012:** Placed on the Union Calendar, Calendar No. 318.
- **Apr 26, 2012:** Mr. Issa moved to suspend the rules and pass the bill, as amended.
- **Apr 26, 2012:** Considered under suspension of the rules. (consideration: CR H2187-2189)
- **Apr 26, 2012:** DEBATE - The House proceeded with forty minutes of debate on H.R. 4257.
- **Apr 26, 2012:** Passed/agreed to in House: On motion to suspend the rules and pass the bill, as amended Agreed to by voice vote.(text: CR H2187-2189)
- **Apr 26, 2012:** On motion to suspend the rules and pass the bill, as amended Agreed to by voice vote. (text: CR H2187-2189)
- **Apr 26, 2012:** Motion to reconsider laid on the table Agreed to without objection.
- **Apr 18, 2012:** Committee Consideration and Mark-up Session Held.
- **Apr 18, 2012:** Ordered to be Reported (Amended).
- **Mar 26, 2012:** Introduced in House
- **Mar 26, 2012:** Referred to the House Committee on Oversight and Government Reform.