HR 3402

Federal Information Security Management Reform Act of 2015

Congress: 114 (2015–2017, Ended)
Chamber: House
Policy Area: Government Operations and Politics
Introduced: Jul 29, 2015
Current Status: Referred to the House Committee on Oversight and Government Reform.
Latest Action: Referred to the House Committee on Oversight and Government Reform. (Jul 29, 2015)
Official Text: https://www.congress.gov/bill/114th-congress/house-bill/3402

Sponsor

Name: Rep. Ruppersberger, C. A. Dutch [D-MD-2]
Party: Democratic • **State:** MD • **Chamber:** House

Cosponsors

No cosponsors are listed for this bill.

Committee Activity

Committee	Chamber	Activity	Date
Oversight and Government Reform Committee	House	Referred To	Jul 29, 2015

Subjects & Policy Tags

Policy Area:

Government Operations and Politics

Related Bills

Bill	Relationship	Last Action
114 HR 3313	Related bill	**Aug 11, 2015:** Referred to the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies.
114 S 1828	Identical bill	**Jul 22, 2015:** Read twice and referred to the Committee on Homeland Security and Governmental Affairs. (Sponsor introductory remarks on measure: CR S5456-5458)

Summary (as of Jul 29, 2015)

Federal Information Security Management Reform Act of 2015

Requires the Department of Homeland Security (DHS), in administering federal agencies' implementation of information system security policies, to: (1) operate consolidated intrusion detection, prevention, or protective capabilities and use of associated countermeasures to protect agency information and systems from security threats; (2) provide incident detection, analysis, mitigation, and response information and remote or onsite technical assistance; (3) develop and conduct impact assessments in consultation with other agencies and private entities; (4) foster development of technologies for use across multiple agencies in conjunction with other agencies and the private sector; and (5) coordinate such information security policies with standards for national security systems and policies issued by the Department of Defense (DOD) and the Director of National Intelligence.

Authorizes the DHS Secretary to acquire, intercept, retain, use, and disclose communications and system traffic transiting to or from or stored on agency information systems and deploy countermeasures if the Secretary certifies that: (1) the measures are reasonably necessary to protect agency information systems from security threats; (2) content of communications will not be retained, and traffic will not be subject to countermeasures, unless associated with a known or reasonably suspected information security threat; (3) the information will be used for law enforcement purposes only with the Attorney General's approval when the information is evidence of a crime; (4) system users have been notified of the potential for such an acquisition or disclosure; and (5) the procedures have been approved by the Attorney General.

Allows agency heads to disclose such information to the Secretary notwithstanding any other law that would otherwise restrict or prevent such disclosures. Provides liability protections to private entities authorized to assist the Secretary for such purposes.

Authorizes the Secretary to: (1) issue a directive to an agency to take any lawful action with respect to the operation of a system that maintains agency information in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to an agency's information security; or (2) authorize, without prior consultation with the affected agency, the use of protective capabilities under the Secretary's control if there is an imminent threat and a directive is unlikely to be timely.

Exempts DOD and the intelligence community from such procedures.

Actions Timeline

- **Jul 29, 2015:** Introduced in House
- **Jul 29, 2015:** Referred to the House Committee on Oversight and Government Reform.