HR 3313

Cyber Defense of Federal Networks 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 Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies.
Latest Action: Referred to the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies. (Aug 11, 2015)
Official Text: https://www.congress.gov/bill/114th-congress/house-bill/3313

Sponsor

Name: Rep. McCaul, Michael T. [R-TX-10]
Party: Republican • **State:** TX • **Chamber:** House

Cosponsors (1 total)

Cosponsor	Party / State	Role	Date Joined
Rep. Ratcliffe, John [R-TX-4]	R · TX		Jul 29, 2015

Committee Activity

Committee	Chamber	Activity	Date
Homeland Security Committee	House	Referred to	Aug 11, 2015
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 3402	Related bill	**Jul 29, 2015:** Referred to the House Committee on Oversight and Government Reform.
114 S 1828	Related 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)

Cyber Defense of Federal Networks Act of 2015

Amends the Homeland Security Act of 2002 to require the Department of Homeland Security (DHS), in coordination with the Office of Management and Budget (OMB), to implement plans to: (1) detect, identify, and remove intruders in federal agencies' information systems; and (2) make advanced network security tools available for agencies to improve visibility of network activity to detect and mitigate intrusions and anomalous activity.

Directs DHS to coordinate with the OMB to: (1) update government information security metrics to include measures of intrusion and incident detection and response times, and (2) display additional metrics about agency cybersecurity postures on federal government performance websites.

Authorizes DHS, upon an agency's request, to operate and maintain technology that is deployed to agencies to diagnose and mitigate cyber threats and vulnerabilities.

Requires DHS to regularly assess and require implementation of best practices for securing agency information systems and preventing data exfiltration.

Redefines for purposes of DHS's national cybersecurity and communications integration center: (1) "cybersecurity risk" to exclude actions that solely involve a violation of a consumer term of service or a consumer licensing agreement; and (2) "incident" to include occurrences that actually or imminently jeopardize, without lawful authority, an information system, thereby replacing a standard that currently includes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

Requires DHS to assist agencies in implementing information security practices by: (1) providing incident detection, analysis, mitigation, and response information, disseminating related homeland security information, and providing remote or onsite technical assistance; (2) developing and conducting impact assessments in consultation with other governmental and private entities; (3) assessing and fostering technologies for use across multiple agencies; and (4) ensuring that policies are coordinated with standards for national security systems and policies of the Department of Defense (DOD) and the Director of National Intelligence.

Authorizes the DHS Secretary to: (1) issue a directive to an agency to take any lawful action with respect to the operation of an agency's information system in response to a known or reasonably suspected information security threat, vulnerability, risk, or incident, including an act of terrorism, that represents a substantial threat to information security; or (2) authorize, without prior consultation with the affected agency, the use of protective capabilities under the Secretary's control for communications or system traffic transiting to or from or stored on an agency information system 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

- **Aug 11, 2015:** Referred to the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies.
- **Jul 29, 2015:** Introduced in House
- **Jul 29, 2015:** Referred to the Committee on Oversight and Government Reform, and in addition to the Committee on Homeland Security, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned.