S 1869

Federal Cybersecurity Enhancement Act of 2016

Congress: 114 (2015–2017, Ended)
Chamber: Senate
Policy Area: Government Operations and Politics
Introduced: Jul 27, 2015
Current Status: Placed on Senate Legislative Calendar under General Orders. Calendar No. 673.
Latest Action: Placed on Senate Legislative Calendar under General Orders. Calendar No. 673. (Nov 17, 2016)
Official Text: https://www.congress.gov/bill/114th-congress/senate-bill/1869

Sponsor

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

Cosponsors (1 total)

Cosponsor	Party / State	Role	Date Joined
Sen. Johnson, Ron [R-WI]	R · WI		Jul 27, 2015

Committee Activity

Committee	Chamber	Activity	Date
Homeland Security and Governmental Affairs Committee	Senate	Reported By	Nov 17, 2016

Subjects & Policy Tags

Policy Area:

Government Operations and Politics

Related Bills

Bill	Relationship	Last Action
114 HR 2029	Related bill	**Dec 18, 2015:** Became Public Law No: 114-113.
114 S 754	Related bill	**Oct 28, 2015:** Held at the desk.

Summary (as of Nov 17, 2016)

Federal Cybersecurity Enhancement Act of 2016

(Sec. 3) This bill amends the Homeland Security Act of 2002 to require the Department of Homeland Security (DHS) to coordinate with the Office of Management and Budget (OMB) to implement an intrusion assessment plan to identify and remove intruders in federal agency information systems.

DHS must deploy and operate, for use by other agencies, capabilities to detect and prevent or remove cybersecurity risks in network traffic transiting or traveling to or from agency information systems. DHS may access, and agencies may disclose to DHS, information transiting agency systems, regardless of the location from which the information is accessed, notwithstanding any laws that would otherwise restrict or prevent such disclosures. Agencies must utilize such capabilities and adopt subsequent improvements.

DHS must establish a pilot to test and deploy advanced technologies to improve detection and prevention.

DHS must ensure that: (1) activities are reasonably necessary to protect agency information and systems from cybersecurity risks, (2) information accessed by DHS will be retained no longer than reasonably necessary, (3) notice has been provided to users of agency information systems concerning access to their communications, and (4) activities are implemented pursuant to policies governing the operation of the intrusion detection and prevention capabilities.

Liability protections are provided to private entities authorized to assist DHS with such capabilities. But such liability protections shall not be construed to authorize an Internet service provider to break a user agreement with a customer.

The Department of Justice must ensure that guidelines for such capabilities are consistent with laws governing the acquisition, interception, retention, use, and disclosure of communications.

The OMB and DHS must update government-wide policies and brief Congress regarding the prioritization and use of network security monitoring tools within agency networks.

The Department of Defense and the intelligence community are exempt from this bill's procedures.

(Sec. 4) DHS must include in the Continuous Diagnostics and Mitigation Program advanced network security tools to improve visibility of network activity to detect and mitigate intrusions and anomalous activity. The OMB must implement a plan to ensure that agencies utilize such advanced tools.

DHS must collaborate with the OMB to update government information security metrics to include measures of intrusion and incident detection and response times. The OMB must display additional agency metrics on federal government performance websites.

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

(Sec. 5) DHS must require implementation of best practices for securing agency information systems against intrusion and preventing data exfiltration in the event of an intrusion. Agencies must: (1) identify their stored sensitive and mission critical data, (2) assess data access controls, (3) encrypt data consistent with federal information system standards, (4) implement a single sign-on trusted identity platform for individuals accessing each public website of the agency that requires user authentication, and (5) implement multifactor authentication for remote access to agency systems and for

user accounts with elevated privileges.

(Sec. 6) The Government Accountability Office must report on the effectiveness of the federal government's strategy to secure agency information systems. On an annual basis: (1) DHS must report on the implementation status of intrusion detection and prevention capabilities, and (2) the OMB must report on agency application of such capabilities.

The OMB must submit updated intrusion assessment plans to Congress and report annually on intrusion assessment findings, advanced network security tools, and agency compliance.

(Sec. 7) The authority for operating such federal intrusion detection and prevention capabilities terminates seven years after enactment of this bill.

(Sec. 8) The Office of the Director of National Intelligence (ODNI) must submit to Congress an assessment of: (1) the risks that would result from the breach of unclassified information systems that provide access to information that, when combined with other unclassified information, may comprise classified information; and (2) the cost and impact on the mission carried out by each agency if such systems were subsequently classified.

(Sec. 9) DHS and the ODNI must coordinate with agencies to conduct an ongoing damage and risk assessment relating to data breaches at the Office of Personnel Management (OPM). The ODNI must report on: (1) the extent to which federal data was compromised, exfiltrated, or manipulated by the same entity that caused the OPM data breach; (2) national security impacts; and (3) whether information accessed through the breach has been released or deployed.

(Sec. 10) DHS may issue an emergency directive to an agency to take any lawful action regarding the operation of the agency's information system (including systems owned or operated by another entity on behalf of an agency) in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to information security. DHS must report annually to Congress regarding specific actions taken pursuant to such directives.

If DHS determines that there is an imminent threat for which a directive is unlikely to result in a timely response, DHS may authorize the use of protective capabilities under DHS control for communications or system traffic transiting to or from, or stored on, an agency information system without prior consultation with the affected agency. But DHS must immediately notify the OMB, each affected agency, and Congress of the use of such imminent threat authority and the reasons for, and duration of, the action.

DHS may direct or authorize such lawful action or protective capability only: (1) to protect agency information from unauthorized access, use, disclosure, disruption, modification, or destruction; or (2) to require the remediation of, or to protect against, identified information security risks for information collected or maintained by or on behalf of an agency or that portion of an information system used or operated by an agency or other organization on an agency's behalf.

The OMB must report annually regarding specific actions it has taken to enforce agency compliance and accountability.

Actions Timeline

- **Nov 17, 2016:** Committee on Homeland Security and Governmental Affairs. Reported by Senator Johnson with amendments. With written report No. 114-378.
- **Nov 17, 2016:** Placed on Senate Legislative Calendar under General Orders. Calendar No. 673.
- **Jul 29, 2015:** Committee on Homeland Security and Governmental Affairs. Ordered to be reported with amendments favorably.
- **Jul 27, 2015:** Introduced in Senate
- **Jul 27, 2015:** Read twice and referred to the Committee on Homeland Security and Governmental Affairs.