**Calendar No. 673**

| 114TH CONGRESS *2d Session* | SENATE | REPORT 114–378 |
|---|---|---|

# FEDERAL CYBERSECURITY ENHANCEMENT ACT OF 2015

---

## R E P O R T

OF THE

## COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

## S. 1869

TO IMPROVE FEDERAL NETWORK SECURITY AND AUTHORIZE AND ENHANCE AN EXISTING INTRUSION DETECTION AND PREVENTION SYSTEM FOR CIVILIAN FEDERAL NETWORKS

NOVEMBER 17, 2016.—Ordered to be printed

---

U.S. GOVERNMENT PUBLISHING OFFICE

69–010 WASHINGTON : 2016

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

RON JOHNSON, Wisconsin, *Chairman*

JOHN MCCAIN, Arizona
ROB PORTMAN, Ohio
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MICHAEL B. ENZI, Wyoming
KELLY AYOTTE, New Hampshire
JONI ERNST, Iowa
BEN SASSE, Nebraska

THOMAS R. CARPER, Delaware
CLAIRE MCCASKILL, Missouri
JON TESTER, Montana
TAMMY BALDWIN, Wisconsin
HEIDI HEITKAMP, North Dakota
CORY A. BOOKER, New Jersey
GARY C. PETERS, Michigan

CHRISTOPHER R. HIXON, *Staff Director*
GABRIELLE D'ADAMO SINGER, *Chief Counsel*
BROOKE N. ERICSON, *Chief Counsel for Homeland Security*
GABRIELLE A. BATKIN, *Minority Staff Director*
JOHN P. KILVINGTON, *Minority Deputy Staff Director*
MARY BETH SCHULTZ, *Minority Chief Counsel*
STEPHEN R. VIÑA, *Minority Chief Counsel for Homeland Security*
LAURA W. KILBRIDE, *Chief Clerk*

**Calendar No. 673**

114TH CONGRESS *2d Session* | SENATE | REPORT 114–378

# FEDERAL CYBERSECURITY ENHANCEMENT ACT OF 2015

NOVEMBER 17, 2016.—Ordered to be printed

Mr. JOHNSON, from the Committee on Homeland Security and Governmental Affairs, submitted the following

# R E P O R T

[To accompany S. 1869]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 1869), to improve Federal network security and authorize and enhance an existing intrusion detection and prevention system for civilian Federal networks, having considered the same, reports favorably thereon with amendments and recommends that the bill, as amended, do pass.

CONTENTS



## I. PURPOSE AND SUMMARY

The purpose of S. 1869, the Federal Cybersecurity Enhancement Act of 2015, is to improve cybersecurity at Federal civilian agencies through improvements to network and computer security and implementation of best practices in information security across the Federal Government.

First, to improve perimeter security and detect and defend against cyberattacks, the bill would authorize a government-wide intrusion detection and prevention system, operated by the Department of Homeland Security (DHS or "the Department") and today operationally implemented under the "EINSTEIN" programs. The bill would require several significant enhancements to EINSTEIN

and enable and require agencies to apply the intrusion detection and prevention system to all information traveling to and from their information systems, clarifying that agencies may and shall deploy EINSTEIN notwithstanding any other law. Second, the bill would require that agencies implement important cybersecurity best practices, such as encryption of sensitive data and multi-factor authentication for high-risk users. Third, the bill would ensure agencies proactively seek out adversaries that may have already established a presence in their networks through a requirement that the Office of Management and Budget (OMB) and DHS create an intrusion assessment plan. Fourth, the bill would require the Director of OMB and the Secretary of Homeland Security (the Secretary) to prioritize advanced security tools for network monitoring, including within the Continuous Diagnostics and Mitigation (CDM) program.

Fifth, the bill would require the Director of National Intelligence (the DNI) to identify information systems, which although unclassified, could reveal classified information if compromised. Sixth, the bill requires an assessment of the impact of the 2015 data breach at the Office of Personnel Management (OPM). Seventh, the bill would authorize the Secretary, in response to substantial threats, to issue directives to the heads of other agencies to take lawful action to protect their information systems and take direct action in response to imminent threats. Finally, the bill includes reporting and oversight requirements to ensure effective implementation.

## II. Background and the Need for Legislation

Recent reports conservatively estimate that cybercrime and cyber espionage cost United States companies and citizens approximately $100 billion annually, resulting in the loss of as many as 508,000 jobs.[1] The DNI has recognized that cybersecurity remains a top national security priority as "Cyber threats to US national and economic security are increasing in frequency, scale, sophistication, and severity of impact."[2] The United States Government, private sector, and the American public face real-time threats from a variety of actors and capabilities. These include nation-states with highly sophisticated cyber programs, nations with less technical capabilities but a more disruptive intent, profit-motivated cybercriminals, and ideologically-motivated hackers and extremists.[3]

In recent years, foreign adversaries have stolen tens of millions of Americans' sensitive data as a result of data breaches at Federal agencies.[4] For example, OPM has identified five major breaches of their information technology (IT) systems from malicious hackers.[5]

---

[1] McAfee, The Econ. Impact of Cybercrime (July 2013), http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf.

[2] James R. Clapper, Off. of the Director of Nat'l Intelligence, Worldwide Threat Assessment of the US Intelligence Community 1 (2015), http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf.

[3] *Id.* at 2.

[4] *See e.g.,* Off. of Personnel Management, Cybersecurity Resource Center: Cybersecurity Incidents (2016), https://www.opm.gov/cybersecurity/cybersecurity-incidents/#WhatHappened. *See also* Press Release, IRS Statement on "Get Transcript," IRS (Feb. 26, 2016), https://www.irs.gov/uac/newsroom/irs-statement-on-get-transcript.

[5] Off. of Personnel Management, Final Audit Report: Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Serena Business Manager FY 2013 (2013), https://www.opm.gov/our-inspector-general/reports/2013/audit-of-the-information-technology-security-controls-of-the-us-office-of-personnel-managements-serena-business-man-

The most recent breach was in 2015, when OPM discovered two separate, yet related, breaches that impacted the data of Federal employees, contractors, and other individuals.[6] Earlier that year, it was discovered that 4.2 million current and former Federal employees' personal data had been stolen.[7] In June 2015, OPM also discovered that the sensitive information of 21.5 million individuals, collected in relation to background investigation records of current, former, and prospective Federal employees and contractors, had been breached.[8] Of this amount, 19.7 million individuals had applied for a background investigation, and 1.8 million were non-applicants (such as spouses or co-habitants). Approximately 5.6 million of the records contained individual fingerprints. Some records also contained findings from background investigation interviews.[9]

In 2015, the Internal Revenue Service (IRS) also suffered a breach involving the IRS Get Transcript application, which allows taxpayers to view and download their information, such as account transactions, line-by-line tax return information, and reported income via the IRS public website.[10] The IRS removed the application on May 21, 2015, after discovering that it was being used by unauthorized users to access taxpayer data.[11] An analysis by the Treasury Inspector General for Tax Administration (TIGTA) identified 620,931 taxpayer accounts implicated by potentially unauthorized access from January 1, 2014 through May 21, 2015.[12] Further analysis found that the unauthorized users were successful in accessing and obtaining transcripts for 355,262 taxpayers' accounts.[13] TIGTA also discovered that the IRS did not identify 2,470 additional taxpayers that were targeted through the Get Transcript application.[14]

As demonstrated through Committee oversight,[15] Federal agencies such as OPM and the IRS have not always used best practices to secure their networks, which have contributed to data thefts. On June 2, 2015, the Committee held a hearing on the IRS data breach, where it was revealed that the IRS's lack of multi-factor authentication led to a weakened cyber defense against bad actors.[16] Later that month, on June 25, 2015, the Committee examined the missteps leading up to the OPM data breach.[17]

S. 1869 seeks to reduce and mitigate future breaches at Federal agencies through its requirements for cybersecurity best practices

---

ager-fy-2013 4a-ci-00-13-023.pdf; *see also* Off. of Personnel Management, Cybersecurity Resource Center: Cybersecurity Incidents (2016), https://www.opm.gov/cybersecurity/cybersecurity-incidents/#WhatHappened.

[6] Off. of Personnel Management, Cybersecurity Resource Center: Cybersecurity Incidents (2016).

[7] *Id.*

[8] *Id.*

[9] *Id.*

[10] Treasury Inspector Gen. for Tax Admin., 2016–40–037, The Internal Revenue Serv. Did Not Identify and Assist All Individuals Potentially Affected by the Get Transcript Application Data Breach 1 (2016), https://www.treasury.gov/tigta/auditreports/2016reports/201640037fr.pdf.

[11] *Id.* at 2.

[12] *Id.* at 7.

[13] *Id.*

[14] *Id.* at 11.

[15] *The IRS Data Breach: Steps to Protect Americans' Personal Information: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs, 114th Cong. (2015); Under Attack: Federal Cybersecurity and the OPM Data Breach: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs,* 114th Cong. (2015).

[16] *The IRS Data Breach: Steps to Protect Americans' Personal Information: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs,* 114th Cong. (2015).

[17] *Under Attack: Federal Cybersecurity and the OPM Data Breach: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs,* 114th Cong. (2015).

and authorization and mandated application and acceleration of the EINSTEIN program. This bill addresses those agency failures by mandating cybersecurity best practices such as encryption, multi-factor authentication, and stronger access controls. Further, S. 1869 requires OMB and DHS to develop a government-wide intrusion assessment to root out and eliminate intruders already in government networks.

By authorizing the Department's intrusion detection and intrusion prevention system today operationally implemented under the EINSTEIN programs, S. 1869 will also further enable the Federal Government to detect and block malicious activity on agencies' networks. This bill for the first time would require the system to be available to all agencies. This bill would clear legal and other hurdles to deploying EINSTEIN and mandate that civilian agencies implement it within one year. Crucially, S. 1869 would also require that DHS make significant improvements to EINSTEIN to include, among other things, non-signature based detection technologies, like heuristic and behavior-based detection technologies. Current reliance on decades old signature-based detection technology limits the effectiveness of EINSTEIN against advanced persistent threats. The legislation would require DHS to regularly deploy new technologies and modify existing technologies for the system and to assess and use commercial and non-commercial technologies to improve detection and prevention capabilities. In furtherance of improving EINSTEIN, S. 1869 would authorize a pilot program so DHS can quickly deploy and test new or improved detection and prevention technologies, and mandates that agencies adopt improvements within six months after DHS makes them available.

While an intrusion detection and prevention system can provide much needed protections against cyber-attacks, it alone is insufficient to protect government data. As the cyber threat is constantly evolving, EINSTEIN must be complemented with current cybersecurity best practices. The bill would also give the Secretary of DHS the authority, in response to a known or reasonably suspected cyber threat, to issue an emergency directive to the head of another agency to take lawful action to protect their Federal information systems. The bill further would authorize the Secretary to use protective capabilities under the control of the Secretary to address an imminent threat against a civilian agency information system if an emergency directive action is not reasonably likely to result in a timely response to a cyber threat.

Finally, the bill would require substantial privacy protections, robust reporting requirements, and a sunset so Congress can ensure that the Federal Cybersecurity Enhancement Act works as intended and agencies carry out their responsibilities effectively.

## III. LEGISLATIVE HISTORY

On July 27, 2015, Ranking Member Tom Carper and Chairman Ron Johnson introduced S. 1869, the Federal Cybersecurity Enhancement Act of 2015, which was referred to the Committee on Homeland Security and Governmental Affairs.

The Committee considered S. 1869 at a business meeting on July 29, 2015. Senator Rand Paul offered an amendment to clarify that the liability protections afforded in the bill did not extend to a situ-

ation in which an Internet Service Provider breaks a user agreement with its customer.

An additional amendment offered by Senator Paul added data to a reporting requirement from the Secretary, namely the number of individuals whose information was not related to a cybersecurity risk but was nevertheless retained by EINSTEIN.

Senators Kelly Ayotte and Claire McCaskill offered a modified amendment to require the Secretary to ensure that EINSTEIN is necessary to protect information systems from cyber threats, that DHS will only keep information related to cyberattacks, and that users of the system are notified that EINSTEIN could be used. The amendment also required the Attorney General to review policies and procedures governing access to information under EINSTEIN within one year.

Senators Ayotte, McCaskill, Johnson, and Carper also offered a modified amendment to provide the Secretary with expanded authority to issue directives to agencies, in coordination with OMB, to mitigate substantial cybersecurity threats, implement those measures if the threat is imminent and the directive is not reasonably likely to result in a timely response, and require DHS to report to Congress annually regarding the Secretary's implementation of this amendment.

Senator Ben Sasse offered a modified amendment to require the DNI to submit a report to Congress identifying unclassified information systems that, when combined, could comprise classified information, and assessing the risk associated with potential breaches of such systems.

Senator Sasse also offered a modified amendment to require DHS to conduct a damage assessment on the OPM data breaches and report to Congress within 180 days. This includes an assessment of what data was compromised or changed, the impact on national security, and an analysis of whether any of the data stolen has been leaked.

The Committee adopted all six amendments by voice vote. Senators present for the voice vote on the amendments were: Johnson, Portman, Lankford, Ernst, Sasse, Carper, Baldwin, Heitkamp, and Peters. The Committee favorably reported the bill, as amended, on a roll call vote of nine yeas to zero nays. Senators present and voting in the affirmative were Johnson, Portman, Lankford, Ernst, Sasse, Carper, Baldwin, Heitkamp, and Peters. Senators voting in the affirmative by proxy and for the record only were McCain, Enzi, Ayotte, McCaskill, Tester, and Booker. No Senators voted in the negative.

S. 1869 was included in H.R. 2029, the Consolidated Appropriations Act of 2016, which was signed into law by President Obama on December 18, 2015, as Public Law Number 114–113.

## IV. Section-by-Section Analysis of the Bill, as Reported

*Section 1. Short title*

This section provides the bill's short title, the "Federal Cybersecurity Enhancement Act of 2015."

*Section 2. Definitions*

This section defines several terms, including "agency," "agency information system," "appropriate congressional committees," "cybersecurity risk," "information system," "Director," "intelligence community," and "Secretary."

*Section 3. Improved Federal network security*

Section 3(a) amends Title II of the Homeland Security Act of 2002 to add a new section (Sec. 228) on "Cybersecurity Plans."

Subsection (a) of the new section 228 of the Homeland Security Act of 2002, as redesignated, provides definitions for the following terms: "agency information system," "cybersecurity risk," "information sharing," and "intelligence community."

Subsection (b) of the new section requires the Secretary, in coordination with the Director of OMB, to develop and implement an intrusion assessment plan for all Federal agencies' information systems except that of the Department of Defense. The intrusion assessment plan should provide a continuous mechanism to detect, isolate, and eradicate current and past threats in Federal agencies' information systems and complements other security controls.

Section 3(a) further amends Title II of the Homeland Security Act of 2002 to add a new section 230 on "Federal Intrusion Detection and Prevention System," which authorizes the Department's existing signature-based network intrusion detection and prevention system, operationally known as EINSTEIN, with required improvements to the program's capabilities, cost-effectiveness, deployment schedule, and privacy protections.

Subsection (a) of the new section 230 provides definitions for the following terms: "agency," "agency information," "agency information system," "cybersecurity risk," and "information system."

Subsection (b) of the new section authorizes the Department's intrusion detection and prevention system, by requiring the Secretary to deploy, operate, and maintain an intrusion detection capability (operationally known as EINSTEIN 1 and 2) and an intrusion prevention capability (operationally known as EINSTEIN 3A). In addition, the subsection authorizes and requires expansion of the existing EINSTEIN capabilities through the addition of new technologies and modification of existing technologies to improve those capabilities. The capabilities authorized in subsection (b) apply to network traffic that is transiting within an agency information system, to network traffic that is traveling to an agency information system, and to traffic that is traveling from an agency information system.

Subsection (c)(1) of the new section provides an authorization for DHS to deploy EINSTEIN on agencies network traffic, and for other agencies to allow deployment of the system on their network traffic, notwithstanding any other statute. A key limitation in previous efforts to deploy the EINSTEIN program, for example, has been statutes that restrict or prevent disclosure of certain types of information such as, statistical, proprietary, tax, and health data. Subsection (c)(1) provides that for the purpose of deploying EINSTEIN in its various current and fu-

ture iterations, such laws do not apply. The Secretary and agencies with sensitive data are expected to confer regarding the sensitivity of, and statutory protections otherwise applicable to, information on agency information systems. The Secretary is expected to ensure that the policies and procedures developed under this section appropriately restrict and limit Department access, use, retention, and handling of such information to protect the privacy and confidentiality of such information, including ensuring that the Department protects such sensitive data from disclosure, and trains appropriate staff accordingly.

Subsection (c)(2)–(7) of the new section sets forth several authorities and requirements for the operation of the EINSTEIN intrusion detection and prevention system and other activities the Secretary may undertake to enhance federal agency cybersecurity. Specifically, the subsection authorizes the Secretary to contract with other entities in deploying, operating, and maintaining the intrusion detection capability. The Secretary is provided with authorities to improve EINSTEIN and is required to regularly assess and utilize advanced protective technologies in EINSTEIN and non-signature based detection such as heuristic and behavior-based detection technologies. A pilot program is created to enable fast acquisition, testing, and deployment of such advanced protective technologies. The Department of Defense's SHARKSEER program, for example, rapidly acquires and integrates advanced commercial cybersecurity technology for detecting intrusions and malware for which signatures are not already known and may possibly serve as a model for the DHS operated intrusion detection and prevention system. Finally, appropriate privacy protections for EINSTEIN are provided, including: authorization to use, retain and disclose data derived from the intrusion detection and prevention capability only for protection from cybersecurity risks; periodic updates to privacy impact assessments; notice to users of the potential access by EINSTEIN; and policies and procedures implementing these requirements.

Subsection (d) of the new section includes privacy protections related to contractors offering EINSTEIN services, such as internet service providers. Contractors are prohibited from inappropriately using or disclosing information received through EINSTEIN to entities other than DHS or the affected agency. Private entities are immune from liability for their assistance to the Secretary in deploying, operating, and maintaining EINSTEIN in accordance with the Act. However, paragraph (3) clarifies that this protection does not extend to internet service providers' violations of their terms of service with their customers.

Subsection (e) of the new section requires the Attorney General to review the policies and guidelines for EINSTEIN to ensure they are consistent with applicable laws.

Section 3(b) of the bill requires the Director of OMB and the Secretary to review and update government-wide policies and programs to ensure appropriate use of network security monitoring tools. This section also requires OMB and the Secretary to brief Congress on these efforts.

Section 3(c) requires that within one year agencies implement all EINSTEIN intrusion detection and intrusion prevention capabilities on all data traveling between an agency information system and any information system other than an agency information system, or two months after which it is made available, whichever is later. Similarly, this subsection requires agencies to deploy any improvements to EINSTEIN, such as new detection or prevention technologies, within six months after they are made available. This subsection does not apply to the Department of Defense or the intelligence community. Because this subsection relies on the definition of "agency information system" in Section 228 of the Homeland Security Act of 2002, as redesignated by this bill, it would not require deployment of EINSTEIN between two agency information systems, or an agency information system and an information system operated by a contractor to the agency. If the definition of "agency information system" was constrained to mean only information systems owned or operated by an agency, the EINSTEIN requirement would apply to network traffic between an agency owned information system and a contractor owned information system.

Section 3(d) updates the table of contents of the Homeland Security Act of 2002 to reflect changes made by this bill.

*Section 4. Advanced internal defenses*

This section refers to the Department's Continuous Diagnostics and Mitigation (CDM) program authorized under 44 U.S.C. 3553(b)(6)(B). It requires the Secretary to include in CDM advanced network security tools for improving continuous monitoring of agency networks. This includes using best practices to improve lateral security within agency networks such as the use of micro segmentation to mitigate cyber-attacks, as well as developing metrics to measure security effectiveness with regard to intrusion and incident detection and response times. To increase transparency and accountability, the Secretary is required to implement a plan and share the agencies' metrics for intrusion detection and response times with the public to the extent practicable.

*Section 5. Federal cybersecurity best practices*

This section requires the Secretary, in consultation with OMB, to regularly assess and implement best practices across all Federal agencies to continuously identify intrusions and prevent data exfiltration. In addition, it prescribes specific security requirements to be implemented within one year at all Federal agencies. These requirements are informed by recent data breaches at Federal agencies. Specifically, all Federal agencies must identify sensitive and mission-critical data, assess the access controls to the sensitive data including whether there is a need to store the data digitally at all or in a networked environment, and encrypt the data in order to protect it. This section also requires that agencies that allow users to logon to their websites utilize the General Services Administration's Connect.gov platform. This platform implements the National Strategy for Trusted Identities in Cyberspace by creating a single sign-on across Federal agency websites. Finally the section requires agencies to use multi-factor authentication for remote access to agency information and logons by privileged users. This sec-

tion does not apply to the Department of Defense or the intelligence community.

The Department should leverage the benefits of emerging cybersecurity technologies that shift from a perimeter protection paradigm to an automated policy-based approach where the protection can be implemented at a more granular level within the enterprise infrastructure. Such emerging technologies may include the use of multi-factor authentication, network segmentation, real-time monitoring, and proactive management of compliance using configuration management for software patching, event logging, and other advanced security measures to achieve trusted security in the infrastructure.

*Section 6. Assessments; reports*

This section requires the Government Accountability Office (GAO) to assess and report on the effectiveness of the EINSTEIN program within three years of enactment. In addition, the Secretary must report on the status of the development of intrusion detection and prevention capabilities within six months of enactment and annually thereafter. This section also requires two reports from OMB: a report that analyzes Federal agency application of intrusion detection and prevention capabilities (which shall be included in OMB's annual interagency report under the Federal Information Security Management Act, as amended), and an annual report on the update of the intrusion assessment plan and best practices. In addition, it requires OMB to submit the intrusion assessment plan to Congress within six months of enactment.

*Section 7. Termination*

This section sunsets section 230 of the Homeland Security Act of 2002, authorizing the EINSTEIN program, as well as all reporting requirements, seven years after enactment. However, the termination does not end the limitation on liability to private entities that assist with implementing this statute.

*Section 8. Identification of unclassified information systems*

This section requires the DNI to work with all agencies to identify and assess unclassified information systems that when added to other unclassified information could pose a risk to classified information. The DNI is also required to report the findings to Congress. This section does not apply to the Department of Defense or the intelligence community.

*Section 9. OPM data breach damage assessment*

This section requires the Secretary and the DNI to work together to assess the damage and risk related to the OPM data breach and provide an unclassified report to Congress within 180 days of enactment.

*Section 10. Direction to agencies*

This section allows the Secretary, after coordination with the OMB, and in response to a known or reasonably suspected information security threat, vulnerability or incident that represents a substantial threat to the information security of an agency, to issue a directive to an agency head to take specific action to protect an in-

formation system that the agency owns, operates, or benefits from to prevent or mitigate a security threat. DHS must submit a report each February 1 regarding the Secretary's implementation of this paragraph. In addition, if there is an imminent threat to agency information systems and an emergency directive is not reasonably likely to result in a timely response to the threat, the Secretary may use any controls available to combat the threat without prior consultation with the affected agency. The Secretary must immediately notify OMB and the appropriate congressional committees of any action taken under this section. The authorities under this section may not be delegated below an Under Secretary for DHS.

## V. Evaluation of Regulatory Impact

Pursuant to the requirements of paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee has considered the regulatory impact of this act and determined that the act will have no regulatory impact within the meaning of the rules. The Committee agrees with the Congressional Budget Office's statement that the act contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would impose no costs on state, local, or tribal governments because this bill.

## VI. Congressional Budget Office Cost Estimate

JANUARY 15, 2016.

Hon. RON JOHNSON,
*Committee on Homeland Security and Governmental Affairs,*
*U.S. Senate, Washington, DC.*

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for S. 1869, the Federal Cybersecurity Enhancement Act of 2015.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is William Ma.

Sincerely,

KEITH HALL.

Enclosure.

*S. 1869—Federal Cybersecurity Enhancement Act of 2015*

S. 1869 would require the Department of Homeland Security (DHS) to make available the tools and capabilities necessary to protect the federal government's digital infrastructure and information systems against cyber threats. The bill would further require all federal agencies (except the Department of Defense and elements of the intelligence community) to adopt those tools once available. With the recent enactment of the Consolidated Appropriations Act, 2016, DHS and all federal agencies are already required to perform the same activities as those required by S. 1869. One notable difference, though, is that the Consolidated Appropriations Act, 2016, authorized the Office of Management and Budget to waive the requirement that agencies implement certain cybersecurity measures if doing so would either be unnecessary to secure agency information systems or extremely burdensome. S. 1869 contains no such exception.

Although CBO does not have enough information to provide a precise estimate of the costs of implementing S. 1869, the costs of eliminating an agency's ability to obtain a waiver from some of the bill's requirements could be significant. The extent of those costs would depend not only on the number of agencies that will receive waivers under current law, but also the degree to which those agencies can implement the protections required by the bill. For example, one requirement in both S. 1869 and the Consolidated Appropriations Act, 2016, is to encrypt data stored on or moving through agency information systems.

Based on information from various agencies, CBO expects that data residing on some older or out-of-date information systems cannot be encrypted. Those systems would either have to be updated or replaced. Under current law, CBO expects that some agencies in that situation will receive a waiver allowing them time to develop plans to update or replace their current systems. Under S. 1869, those agencies would be required to implement all capabilities, including data encryption, on all information systems not later than one year after enactment. Having to accelerate those agencies' plans to update or replace those systems within one year could cost hundreds of millions of dollars over the 2016–2020 period, CBO estimates. Such spending would be subject to the availability of appropriated funds.

S. 1869 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act.

Enacting S. 1869 would not affect direct spending or revenues; therefore, pay-as-you-go procedures do not apply. CBO estimates that enacting S. 1869 would not increase net direct spending or on-budget deficits in any of the four consecutive 10-year periods beginning in 2026.

The CBO staff contact for this estimate is William Ma. The estimate was approved by H. Samuel Papenfuss, Deputy Assistant Director for Budget Analysis.

## VII. Changes in Existing Law Made By The Bill, as Reported

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, changes in existing law made by S. 1869 as reported, are shown as follows (existing law proposed to be omitted is enclosed in brackets, new matter is printed in italic, and existing law in which no change is proposed is shown in roman):

# UNITED STATES CODE

* * * * * * *

# TITLE 44—PUBLIC PRINTING AND DOCUMENTS

* * * * * * *

## CHAPTER 35—COORDINATION OF FEDERAL INFORMATION POLICY

* * * * * * *

**SEC. 3553. AUTHORITY AND FUNCTIONS OF THE DIRECTOR AND THE SECRETARY.**

(a) * * *

* * * * * * *

*(h) DIRECTION OF THE AGENCIES.—*

*(1) AUTHORITY.—*

*(A) IN GENERAL.—Not withstanding section 3554, and subject to subparagraph (B), in response to a known or reasonably suspected information security threat, vulnerability or incident that represents a substantial threat to the information security of an agency, the Secretary may issue a directive to the head of an agency to take any lawful action with respect to the operation of the information system, including such systems owned or operated by another entity on behalf of an agency, that collects, processes, stores, transmits, disseminates, or otherwise maintains agency information, for the purpose of protecting the information system from, or mitigating, an information security threat.*

*(B) EXCEPTION.—The authorities of the Secretary under this subsection shall not apply to a system described in paragraph (2) or (3) of subsection (e).*

*(2) PROCEDURES FOR USE OF AUTHORITY.—The Secretary shall—*

*(A) in coordination with the Director, establish procedures governing the circumstances under which a directive may be issued under this subsection, which shall include—*

*(i) thresholds and other criteria;*

*(ii) privacy and civil liberties protections; and*

*(iii) providing notice to potentially affected third parties;*

*(B) specify the reasons for the required action and the duration of the directive;*

*(C) minimize the impact of a directive under this subsection by—*

*(i) adopting the least intrusive means possible under the circumstances to secure the agency information systems; and*

*(ii) limiting directives to the shortest period practicable;*

*(D) notify the Director and the head of any affected agency immediately upon the issuance of a directive under this subsection; and*

*(E) not later than February 1 of each year, submit to the appropriate congressional committees a report regarding the specific actions the Secretary has taken pursuant to paragraph (1)(A).*

*(3) IMMINENT THREATS.—*

*(A) IN GENERAL.—If the Secretary determines that there is an imminent threat to agency information systems and a directive under this subsection is not reasonably likely to result in a timely response to the threat, the Secretary may authorize the use of protective capabilities under the control of the Secretary for communications or other system traffic transiting to or from or stored on an agency information system without prior consultation with the affected agency*

*for the purpose of ensuring the security of the information or information system or other agency information systems.*

*(B) NOTICE.—The Secretary shall immediately notify the Director, the head and chief information officer (or equivalent official) of each agency to which specific actions were taken pursuant to subparagraph (A), and the appropriate congressional committees and authorizing committees of each such agencies of—*

*(i) any action taken under subparagraph (A); and*

*(ii) the reasons for and duration and nature of the action.*

*(C) OTHER LAW.—Any action of the Secretary under this paragraph shall be consistent with applicable law.*

*(D) LIMITATION OF DELEGATION.—The authority under this paragraph may not be delegated to an official in a position lower than an Under Secretary of the Department of Homeland Security.*

*(4) LIMITATION.—The Secretary may direct or authorize lawful action or protective capability under this subsection only to—*

*(A) protect agency information from unauthorized access, use, disclosure, disruption, modification, or destruction; or*

*(B) require the remediation of or protect against identified information security risks with respect to—*

*(i) information collected or maintained by or on behalf of an agency; or*

*(ii) that portion of an information system used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.*

*(i) ANNUAL REPORT TO CONGRESS.—Not later than February 1 of each year, the Director shall submit to the appropriate congressional committees a report regarding the specific actions the Director has taken pursuant to subsection (a)(5), including any actions taken pursuant to section 11303(b)(5) of title 40.*

*(j) APPROPRIATE CONGRESSIONAL COMMITTEES.—In this section, the term 'appropriate congressional committees' means—*

*(1) the Committee on Appropriations and the Committee on Homeland Security and Governmental Affairs of the Senate; and*

*(2) the Committee on Appropriations and the Committee on Homeland Security of the House of Representatives.*

* * * * * * *

**HOMELAND SECURITY ACT OF 2002**

* * * * * * *

# TITLE II—INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION

* * * * * * *

## Subtitle C—Information Security

**[SEC. 227. CYBER INCIDENT RESPONSE PLAN.**

**[**The Under Secretary appointed under section 103(a)(1)(H) shall, in coordination with appropriate Federal departments and agencies, State and local governments, sector coordinating councils, information sharing and analysis organizations (as defined in section 212(5)), owners and operators of critical infrastructure, and other appropriate entities and individuals, develop, regularly update, maintain, and exercise adaptable cyber incident response plans to address cybersecurity risks (as defined in section 226) to critical infrastructure.**]**

* * * * * * *

**SEC. [228] *229.* CLEARANCES.**

* * * * * * *

***SEC. 228. CYBERSECURITY PLANS.***

*(a) DEFINITIONS.—In this section—*

*(1) the term "agency information system" means an information system used or operated by an agency, by a contractor of an agency, or by another entity on behalf of an agency;*

*(2) the terms "cybersecurity risk" and "information system" have the meanings given those terms in section 227; and*

*(3) the term "intelligence community" has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).*

*(b) INTRUSION ASSESSMENT PLAN.—*

*(1) REQUIREMENT.—The Secretary, in coordination with the Director of the Office of Management and Budget, shall develop and implement an intrusion assessment plan to identify and remove intruders in agency information systems on a routine basis.*

*(2) EXCEPTION.—The intrusion assessment plan required under paragraph (1) shall not apply to the Department of Defense or an element of the intelligence community.*

*(c) CYBER INCIDENT RESPONSE PLAN.—The Under Secretary appointed under section 103(a)(1)(H) shall, in coordination with appropriate Federal departments and agencies, State and local governments, sector coordinating councils, information sharing and analysis organizations (as defined in section 212(5)), owners and operators of critical infrastructure, and other appropriate entities and individuals, develop, regularly update, maintain, and exercise adaptable cyber incident response plans to address cybersecurity risks (as defined in section 227) to critical infrastructure.*

* * * * * * *

***SEC. 230. FEDERAL INTRUSION DETECTION AND PREVENTION SYSTEM.***

*(a) DEFINITIONS.—In this section—*

*(1) the term 'agency' has the meaning given that term in section 3502 of title 44, United States Code;*

*(2) the term 'agency information' means information collected or maintained by or on behalf of an agency;*

*(3) the term 'agency information system' has the meaning given the term in section 228; and*

*(4) the terms 'cybersecurity risk' and 'information system' have the meanings given those terms in section 227.*

*(b) REQUIREMENT.—*

*(1) IN GENERAL.—Not later than 1 year after the date of enactment of this section, the Secretary shall deploy, operate, and maintain, to make available for use by any agency, with or without reimbursement—*

*(A) a capability to detect cybersecurity risks in network traffic transiting or traveling to or from an agency information system; and*

*(B) a capability to prevent network traffic associated with such cybersecurity risks from transiting or traveling to or from an agency information system or modify such network traffic to remove the cybersecurity risk.*

*(2) REGULAR IMPROVEMENT.—The Secretary shall regularly deploy new technologies and modify existing technologies to the intrusion detection and prevention capabilities described in paragraph (1) as appropriate to improve the intrusion detection and prevention capabilities.*

*(c) ACTIVITIES.—In carrying out subsection (b), the Secretary—*

*(1) may access, and the head of an agency may disclose to the Secretary or a private entity providing assistance to the Secretary under paragraph (2), information transiting or traveling to or from an agency information system, regardless of the location from which the Secretary or a private entity providing assistance to the Secretary under paragraph (2) accesses such information, notwithstanding any other provision of law that would otherwise restrict or prevent the head of an agency from disclosing such information to the Secretary or a private entity providing assistance to the Secretary under paragraph (2);*

*(2) may enter into contracts or other agreements with, or otherwise request and obtain the assistance of, private entities to deploy and operate technologies in accordance with subsection (b);*

*(3) may retain, use, and disclose information obtained through the conduct of activities authorized under this section only to protect information and information systems from cybersecurity risks;*

*(4) shall regularly assess through operational test and evaluation in real world or simulated environments available advanced protective technologies to improve detection and prevention capabilities, including commercial and non-commercial technologies and detection technologies beyond signature-based detection, and utilize such technologies when appropriate;*

*(5) shall establish a pilot to acquire, test, and deploy, as rapidly as possible, technologies described in paragraph (4); and*

*(6) shall periodically update the privacy impact assessment required under section 208(b) of the E Government Act of 2002 (44 U.S.C. 3501 note); and*

*(7) shall ensure that—*

*(A) activities carried out under this section are reasonably necessary for the purpose of protecting agency informa-*

*tion and agency information systems from a cybersecurity risk;*

*(B) information accessed by the Secretary will be retained no longer than reasonably necessary for the purpose of protecting agency information and agency information systems from a cybersecurity risk;*

*(C) notice has been provided to users of an agency information system concerning access to communications of users of the agency information system for the purpose of protecting agency information and the agency information system; and*

*(D) the activities are implemented pursuant to policies and procedures governing the operation of the intrusion detection and prevention capabilities.*

*(d) PRIVATE ENTITIES.—*

*(1) CONDITIONS.—A private entity described in subsection (c)(2) may not—*

*(A) disclose any network traffic transiting or traveling to or from an agency information system to any entity other than the Department or the agency that disclosed the information under subsection (c)(1); or*

*(B) use any network traffic transiting or traveling to or from an agency information system to which the private entity gains access in accordance with this section for any purpose other than to protect agency information and agency information systems against cybersecurity risks or to administer a contract or other agreement entered into pursuant to subsection (c)(2) or as part of another contract with the Secretary.*

*(2) LIMITATION OF LIABILITY.—No cause of action shall lie in any court against a private entity for assistance provided to the Secretary in accordance with this section and any contract or agreement entered into pursuant to subsection (c)(2).*

*(3) RULE OF CONSTRUCTION.—Nothing in paragraph (2) shall be construed to authorize an Internet service provider to break a user agreement with a customer.*

*(e) ATTORNEY GENERAL REVIEW.—Not later than 1 year after the date of enactment of this section, the Attorney General shall review the policies and guidelines for the program carried out under this section to ensure that the policies and guidelines are consistent with applicable law governing the acquisition, interception, retention, use, and disclosure of communications.*

○