Calendar No. 668

115TH CONGRESS *2d Session*	SENATE	REPORT 115–382

FEDERAL INFORMATION SYSTEMS SAFEGUARDS ACT OF 2018

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 3208

TO PROVIDE AGENCIES WITH DISCRETION IN SECURING INFORMATION TECHNOLOGY AND INFORMATION SYSTEMS

NOVEMBER 26, 2018.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE

89–010 WASHINGTON : 2018

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
JOHN HOEVEN, North Dakota
STEVE DAINES, Montana

CLAIRE MCCASKILL, Missouri
THOMAS R. CARPER, Delaware
HEIDI HEITKAMP, North Dakota
GARY C. PETERS, Michigan
MAGGIE HASSAN, New Hampshire
KAMALA D. HARRIS, California
DOUG JONES, Alabama

CHRISTOPHER R. HIXON, *Staff Director*
GABRIELLE D'ADAMO SINGER, *Chief Counsel*
ELLIOTT A. WALDEN, *Professional Staff Member*
MARGARET E. DAUM, *Minority Staff Director*
CHARLES A. MOSKOWITZ, *Minority Senior Legislative Counsel*
KATHERINE C. SYBENGA, *Minority Counsel*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 668

115th Congress
2d Session

SENATE

REPORT
115–382

FEDERAL INFORMATION SYSTEMS SAFEGUARDS ACT OF 2018

NOVEMBER 26, 2018.—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. 3208]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 3208) to provide agencies with discretion in securing information technology and information systems, having considered the same, reports favorably thereon with an amendment in the nature of a substitute and recommends that the bill, as amended, do pass.

CONTENTS

I. PURPOSE AND SUMMARY

S. 3208, the Federal Information Systems Safeguards Act of 2018, allows executive agencies to take action to protect their information technology (IT) systems, such as restricting access to

websites the agencies have deemed a security risk, without regard to Federal employee labor-management relationship requirements.[1]

II. BACKGROUND AND NEED FOR THE LEGISLATION

Information security is a significant and persistent challenge for the Federal Government. The Government Accountability Office (GAO) has repeatedly identified weaknesses in Federal agencies' information security programs and compliance with Federal information security policies and practices. In September 2015, GAO reported that information security remains a persistent weakness at twenty-four Federal agencies.[2] In February 2015, GAO reported that "federal cyber assets" have been identified as high-risk since 1997.[3] The current cybersecurity threat is increased due, in part, to the proliferation of increasingly sophisticated threat actors who have expertise and resources to defeat cyber defenses.[4] In 2016, the Office of Management and Budget alerted Congress that Federal agencies reported more than 77,000 security incidents during fiscal year (FY) 2015, an increase of ten percent over the prior year.[5]

Federal agencies identify nation-state actors as the most serious cybersecurity threat they face. In May 2016, GAO reported that 18 agencies with high impact systems—those where the loss of information can have severe impact on the nation or affected individuals—identified foreign nations as the most serious and frequently occurring threat.[6]

In 2015, the nation learned that a sophisticated threat actor had penetrated the information systems of the Office of Personnel Management (OPM), exfiltrating data that included 22.1 million records about Federal employees, including employee personnel and background investigation files.[7] An additional 5.6 million individuals had their fingerprint data stolen.[8] In the aftermath of the breach, OPM instituted a new policy to prohibit its employees from accessing certain websites, including Gmail and Facebook, from their work computers.[9] An OPM spokesperson described the change as a response to the breach and cybersecurity threats:

> As is the case throughout the Federal government, agencies monitor the use of official computers and other devices. In addition, at OPM, we provide guidance on the use

---

[1] On May 25, 2016, the Committee approved S. 2975, the Federal Information Systems Safeguards Act of 2016. That bill is substantially similar to S. 3208, which has been modified only slightly. Accordingly, this committee report is in large part a reproduction of Chairman Johnson's committee report for S. 2975, S. Rep. No. 114–361 (2016).

[2] Gov't Accountability Office, GAO–15–714, Federal Information Security: Agencies Need to Correct Weaknesses and Fully Implement Security Programs (Sept. 2015), http://www.gao.gov/assets/680/672801.pdf.

[3] *Id.*

[4] *Id.*

[5] Office of Management and Budget, Annual Report to Congress: Federal Information Security Modernization Act (Mar. 18, 2016).

[6] Gov't Accountability Office, GAO–16–501, Information Security: Agencies Need to Improve Controls Over Selected High-Impact Systems (May 2016), http://www.gao.gov/products/GAO-16-501.

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

[8] *See* Majority staff report, Cmte. on Oversight and Gov't. Reform, U.S. House of Reps., *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation,* Sept. 7, 2016, https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf.

[9] Statement of Samuel Schumach, Press Secretary, Office of Personnel Management, July 2, 2015.

> of computers and conduct yearly training. Out of caution, and in light of the recent breaches, OPM has recently tightened restrictions on internet access using web security technology. As we move forward with security measures which will ensure both agency and individual security, OPM will continue to monitor and make adjustments to our web security policies.[10]

Seven months later during her February 2016 confirmation hearing, OPM Acting Director Beth Cobert explained the reasoning behind OPM's decision to limit employees' access to certain websites:

> As the world of cybersecurity is changing, as we recognize the nature of these threats, we all need to change the way we interact, the way we use systems at work and at home. What we have done at OPM, and I think what is important for every agency to do, is to recognize what needs to change in the way they operate, what needs to change in the way their employees operate to make sure systems are secure. At OPM, for example, I cannot access my personal Gmail account from my OPM computer. That is the way a lot of threats come in.[11]

However, Federal employee labor unions have raised concerns that such measures could have an adverse impact on Federal employees. In 2011, U.S. Immigration and Customs Enforcement (ICE) imposed a similar policy to limit employees' access to personal email from their workstations to improve cybersecurity. The American Federation of Government Employees (AFGE) filed a grievance against ICE with the Federal Labor Relations Authority (FLRA).[12] The AFGE's grievance alleged that the agency's decision to block access to certain websites on employees' computers unlawfully bypassed the collective bargaining process.[13]

On July 8, 2014, the FLRA ruled that the agency was required to bargain with the union before changing the cybersecurity policy in this case.[14] The FLRA held that Federal employees' legal requirement to protect Federal information under the Federal Information Security Management Act (FISMA) did not provide the agency with sole and exclusive discretion to implement network-access policies affecting employees without first satisfying its bargaining obligations with the union.[15]

Although the remedy provided by the arbitrator and affirmed by the FLRA in this case directed bargaining over only the "impact and implementation" of the agency's decision to block webmail access, concerns have been raised by this decision that the remedy in a future case could include the requirement that an agency restore access and engage in pre-implementation bargaining.[16] Agency heads and their chief information officers must have the ability

---

[10] *Id.*

[11] *Nomination of the Honorable Beth F. Cobert to be Director, Office of Personnel Management: Hearing Before S. Comm. on Homeland Sec; & Governmental Affairs,* 114th Cong. (2016).

[12] *U.S. Department of Homeland Security, Immigration and Customs Enforcement (Agency) and American Federation of Government Employees, National Immigration and Customs Enforcement Council (Union),* 67 F.L.R.A. 126 (July 8, 2014), *available at* https://www.flra.gov/decisions/v67/67-126.html.

[13] *Id.*

[14] *Id.*

[15] *Id.*

[16] *Id.* (dissent by Member Pizzella).

to act quickly to respond to threats and address perceived weaknesses and vulnerabilities in their information systems. Failure to successfully defend against cyberattacks can have significant consequences for the nation and, in cases such as the OPM breach, millions of Federal employees.

The Federal Information Systems Safeguards Act of 2018 clarifies that an agency head may limit, restrict, or prohibit access to a website if the agency head determines such action is necessary to carry out his or her responsibilities as head of the agency. Although such a decision by the agency head is not subject to collective bargaining, after an agency head takes such an action, the bill as amended requires the agency head to seek guidance and take into consideration the personal communication needs of agency employees, upon the employees' request. However, the bill further clarifies that this requirement does not establish a right to collective bargaining.

This bill accurately captures the congressional intent of FISMA to permit agencies authority over securing their networks. Giving agency heads the authority to act swiftly to protect Federal information systems will improve Federal cybersecurity and, thus, national security.

III. LEGISLATIVE HISTORY

Chairman Ron Johnson (R–WI) introduced S. 3208, the Federal Information Systems Safeguards Act of 2018, on July 12, 2018. The bill was referred to the Committee on Homeland Security and Governmental Affairs. Senator Joni Ernst (R–IA) joined as a cosponsor on August 15, 2018.

The Committee considered S. 3208 at a business meeting on September 26, 2018. During the meeting, Chairman Johnson offered an amendment in the nature of a substitute to include language allowing for consideration of employee communication needs. The bill, as amended by the Johnson Substitute Amendment, was ordered reported favorably by voice vote. Senators present were Johnson, Portman, Lankford, Enzi, Hoeven, Daines, McCaskill, Carper, Heitkamp, Peters, Hassan, Harris, and Jones. Senators Peters, Hassan, and Harris were recorded as voting "no" for the record.

IV. SECTION-BY-SECTION ANALYSIS OF THE BILL, AS REPORTED

Section 1. Short title

This section provides that the bill may be referred to as the "Federal Information Systems Safeguards Act of 2018."

Sec. 2. Agency discretion to secure information technology and information systems

Section 2 establishes that agencies have discretion in securing their IT and information systems.

New subsection (a) states that the authority described in new subsection (b) may not be limited by a collective bargaining agreement, memorandum of agreement, any other agreement, or negotiated under section 7106(b) or any other section of chapter 71.

New subsection (b) gives the head of an agency the authority to take any action to limit, restrict, or prohibit access to a website or

to test, deploy, or update a cybersecurity measure if the agency head determines it necessary.

New subsection (c) states that, after having taken an action under this section and upon the request of employees of the agency, the agency head will take into consideration and seek guidance on the personal communication needs of the agency's employees. This does not establish a right to collective bargaining.

New subsection (d) states that the term "agency" has the same meaning as in section 3502 of title 44, United States Code.

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 bill and determined that the bill will have no regulatory impact within the meaning of the rules. The Committee agrees with the Congressional Budget Office's statement that the bill 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.

VI. CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, October 3, 2018.

Hon. RON JOHNSON,
Chairman, 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. 3208, the Federal Information Systems Safeguards Act of 2018.

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

Sincerely,

KEITH HALL.

Enclosure.

S. 3208—Federal Information Systems Safeguards Act of 2018

The Federal Information Security Management Act (FISMA) provides a framework to protect government information operations against security threats. S. 3208 would clarify that, under FISMA, federal agencies have the sole and exclusive authority to take appropriate and timely actions to secure their information technology and information systems. CBO estimates that implementing S. 3208 would clarify Congressional intent, but it would have no significant effect on the federal budget because it would not expand the duties of executive agencies.

Enacting the bill could affect direct spending by agencies not funded through annual appropriations; therefore, pay-as-you-go procedures apply. CBO estimates, however, that any net change in spending by those agencies would be negligible. S. 3208 would not affect revenues.

CBO estimates that enacting S. 3208 would not significantly increase net direct spending or on-budget deficits in any of the four consecutive 10-year periods beginning in 2029.

S. 3208 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act.

On August 10, 2018, CBO transmitted a cost estimate for H.R. 5300, the Federal Information Safeguards Act of 2018, as ordered reported by the House Committee on Oversight and Government Reform on July 17, 2018. The two pieces of legislation are similar and the estimated budgetary effects are the same.

The CBO staff contact for this estimate is Matthew Pickford. The estimate was reviewed by H. Samuel Papenfuss, Deputy Assistant Director for Budget Analysis.

VII. CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

Because S. 3208 would not repeal or amend any provision of current law, it would make no changes in existing law within the meaning of clauses (a) and (b) of paragraph 12 of rule XXVI of the Standing Rules of the Senate.

○