Calendar No. 647

114TH CONGRESS *2d Session*	SENATE	REPORT 114–361

FEDERAL INFORMATION SYSTEMS SAFEGUARDS ACT OF 2016

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 2975

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

SEPTEMBER 27, 2016.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE
59–010 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*
DANIEL P. LIPS, *Policy Director*
GABRIELLE A. BATKIN, *Minority Staff Director*
JOHN P. KILVINGTON, *Minority Deputy Staff Director*
MARY BETH SCHULTZ, *Minority Chief Counsel*
JOHN A. KANE, *Minority Senior Governmental Affairs Advisor*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 647

114TH CONGRESS *2d Session* | SENATE | REPORT 114–361

FEDERAL INFORMATION SYSTEMS SAFEGUARDS ACT OF 2016

SEPTEMBER 27, 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. 2975]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 2975) to provide agencies with discretion in securing information technology and information systems, 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. 2975, the Federal Information Systems Safeguards Act of 2016, is to strengthen Federal cybersecurity by providing agencies greater discretion to secure their information technology and information systems. The legislation clarifies agency heads' authority to limit, restrict, or prohibit access to websites that may present current or future security weakness or risk to the agency's information system.

II. BACKGROUND AND THE NEED FOR 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.[1] In February 2015, GAO reported that "federal cyber assets" have been identified as high-risk since 1997.[2] 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.[3] 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.[4]

Federal agencies identify nation-state actors as the most serious cybersecurity threat they face. In May 2016, GAO reported that 18 agencies that have 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.[5]

In 2015, the nation learned that a sophisticated threat actor had penetrated the information system of the Office of Personnel Management (OPM), exfiltrating data that included millions of sensitive records about Federal employees, including employee background investigations.[6] In the aftermath of the OPM breach, OPM instituted a new policy to prohibit its employees from accessing certain websites, including Gmail and Facebook, from their work computers.[7] 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 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.[8]

---

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

[2] *Id.*

[3] *Id.*

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

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

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

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

[8] *Id.*

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.[9]

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.[10] The American Federation of Government Employees (AFGE) filed a grievance against ICE with the Federal Labor Relations Authority (FLRA).[11] 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.[12]

On July 8, 2014, the FLRA issued a decision ruling that the agency was required to bargain with the union before changing the cybersecurity policy in this case.[13] 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.[14]

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. Agency heads and their chief information officers must have the ability 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 2016 will clarify that an agency head may limit, restrict, or prohibit access to certain websites that are determined to present a current or future security risk. Although such a decision by the agency head is

---

[9] *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).

[10] U.S. *Department of Homeland Security Immigration and Customs Enforcement and American Federation of Government Employees National Immigration and Customs Enforcement Council 118*, 67 F.L.R.A. 126 (July 8, 2014).

[11] *Id.*

[12] *Id.*

[13] *Id.*

[14] *Id.*

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 and work-related communication and access needs of agency employees, upon the employees' request. However, the bill further clarifies that this requirement does not establish a right to collective bargaining.

The legislation will clarify Federal agency heads' cyber security authorities and discretion to act quickly to protect Federal information systems and, therefore, improve Federal cybersecurity.

III. LEGISLATIVE HISTORY

Senator Joni Ernst introduced the Federal Information Systems Safeguard Act of 2016, S. 2975, on May 23, 2016. The bill was referred to the Senate Homeland Security and Governmental Affairs Committee. The Committee considered S. 2975 at a business meeting on May 25, 2016.

During the business meeting, Senator Ernst offered an amendment which was modified by a second degree amendment co-sponsored by Senator Ernst and Senator Carper. The second degree amendment struck language expressing a sense of the Senate and inserted language to clarify that agency heads shall consider employees' communications needs, upon the request of the employees, after taking an action described in the legislation. The Ernst-Carper second degree amendment further clarified that nothing in this subsection shall be construed to establish a right to collective bargaining. The Ernst amendment, as amended by the Ernst-Carper second degree amendment, was adopted by voice vote with Senators Johnson, Portman, Paul, Lankford, Ayotte, Ernst, Sasse, Carper, McCaskill, Tester, Baldwin, Heitkamp, Booker, and Peters present.

S. 2975, as amended, was reported favorably by voice vote with Senators Johnson, Portman, Paul, Lankford, Ayotte, Ernst, Sasse, Carper, McCaskill, Tester, Baldwin, Heitkamp, Booker, and Peters present.

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

Section 1. Short title

This section establishes the short title of the bill as the "Federal Information Systems Safeguards Act of 2016."

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

This section enhances Federal information security by clarifying that any action taken by the head of an agency that is necessary to limit, restrict, or prohibit access to any website the head of the agency determines to present a current or future security weakness or risk to the information technology or information system under the control of the agency, shall not be subject to chapter 71 of title 5, United States Code, regarding labor-management relations.

The section requires that agency heads shall, upon the request of employees of the agency, take into consideration and seek guidance on the personal communication needs of the employees of the agency. The section includes a rule of construction that nothing in

this subsection shall be construed to establish a right to collective bargaining.

The section also defines the terms "agency," "information systems," and "information technology."

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, June 28, 2016.

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. 2975, the Federal Information Systems Safeguards Act of 2016.

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. 2975—Federal Information Systems Safeguards Act of 2016

The Federal Information Security Management Act (FISMA) provides a comprehensive framework to protect the security of federal information systems. S. 2975 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 while implementing S. 2975 would clarify Congressional intent, it would have no significant effect on the federal budget because it would not expand the duties of executive agencies. Because enacting the bill could affect direct spending by agencies not funded through annual appropriations, pay-as-you-go procedures apply. CBO estimates, however, that any net change in spending by those agencies would be negligible. Enacting S. 2975 would not affect revenues.

CBO estimates that enacting S. 2975 would not increase direct spending or on-budget deficits in any of the four consecutive 10-year periods beginning in 2027.

S. 2975 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act and would not affect the budgets of state, local, or tribal governments.

On March 24, 2016, CBO transmitted a cost estimate for H.R. 4361, the Federal Information Systems Safeguards Act of 2016, as

ordered reported by the House Committee on Oversight and Government Reform on March 1, 2016. The two bills are similar and CBO's estimate of their budgetary effects are the same.

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

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

Because S. 2975 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.

○