114TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPORT
114–599

FEDERAL INFORMATION SYSTEMS SAFEGUARDS ACT OF 2016

MAY 31, 2016.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. CHAFFETZ, from the Committee on Oversight and Government Reform, submitted the following

R E P O R T

together with

MINORITY VIEWS

[To accompany H.R. 4361]

[Including cost estimate of the Congressional Budget Office]

The Committee on Oversight and Government Reform, to whom was referred the bill (H.R. 4361) to amend section 3554 of title 44, United States Code, to provide for enhanced security of Federal information systems, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

	Page
Committee Statement and Views	2
Section-by-Section	5
Explanation of Amendments	5
Committee Consideration	5
Roll Call Votes	5
Application of Law to the Legislative Branch	7
Statement of Oversight Findings and Recommendations of the Committee	7
Statement of General Performance Goals and Objectives	7
Duplication of Federal Programs	7
Disclosure of Directed Rule Makings	7
Federal Advisory Committee Act	7
Unfunded Mandate Statement	7
Earmark Identification	8
Committee Estimate	8
Budget Authority and Congressional Budget Office Cost Estimate	8
Changes in Existing Law Made by the Bill, as Reported	9
Minority Views	15

59–006

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Federal Information Systems Safeguards Act of 2016".

SEC. 2. AGENCY DISCRETION TO SECURE INFORMATION TECHNOLOGY AND INFORMATION SYSTEMS.

Section 3554 of title 44, United States Code, is amended by adding at the end the following new subsection:

"(f) AGENCY DISCRETION.—The head of each agency has the sole and exclusive authority, with respect to any information technology or information system under the control of such agency—

"(1) to take any action the agency determines to be necessary to reduce or eliminate security weakness and risk, including to protect the information contained in the information technology or information system; and

"(2) to take any action the agency determines to be necessary to reduce or eliminate future security weakness and risk, including to protect the information contained in the information technology or information system.".

SEC. 3 RULE OF CONSTRUCTION.

Section 2 of this Act, which clarifies agency discretion with respect to any information technology or information system under control of such agency, does not modify existing law as enacted in the Consolidated Appropriations Act of Fiscal Year 2016, Division N – Cybersecurity Act of 2015, Public Law 114–113.

COMMITTEE STATEMENT AND VIEWS

PURPOSE AND SUMMARY

The Federal Information Systems Safeguards Act of 2016 was introduced to ensure federal agencies may take appropriate and timely action as permitted by law to secure their information technology (IT) systems without first providing an opportunity for collective bargaining on such actions.

BACKGROUND AND NEED FOR LEGISLATION

The federal government's most important responsibility is to protect the United States and its people. This responsibility includes ensuring the federal government protects the personally identifiable information (PII) of current and former federal employees as well as other information, including sensitive and classified information. H.R. 4361 is designed to help support that responsibility and clarifies federal agencies' existing authority under the Federal Information Security Management Act (FISMA) to secure their IT systems by clarifying that agencies' IT security functions are not subject to collective bargaining with federal employees.

In a July 8, 2014 decision, the Federal Labor Relations Authority (FLRA) held that agencies' ability to take action to fulfill their responsibilities under the FISMA could be subject to collective bargaining rules.[1]

In the case, the U.S. Department of Homeland Security's (DHS) Immigration and Customs Enforcement (ICE) subcomponent identified a significant increase in network infections and privacy compromises that were related to employees accessing their personnel email from work computers (webmail). In response, the agency notified the union and terminated employees' webmail access. The

[1] *U.S. Department of Homeland Security Immigration and Customs Enforcement and American Federation of Government Employees National Immigration and Customs Enforcement Council 118,* 67 FLRA No. 126 (July 8, 2014).

union objected, arguing that such action was subject to collective bargaining. In its decision, the FLRA held that the agency could not block webmail access through the agency's network without first providing the union an opportunity to bargain.

The FLRA majority's analysis stated that under federal labor law, matters concerning conditions of employment over which an agency has discretion are negotiable if the agency's discretion is not sole and exclusive . . ." Ultimately, the FLRA majority found that imprecise wording in FISMA on agencies' IT security responsibility failed to "demonstrate[] congressional intent to vest the Agency with sole and exclusive discretion over information security matters."

The FLRA's dissenting member disagreed stating that the majority's decision effectively undermined agencies' ability to fulfill their responsibilities under FISMA. He wrote: "it is obvious to me (after having served for seven and half years as the CIO at the U.S. Department of Labor) that neither the [FLRA] nor the Arbitrator possesses the specialized knowledge or expertise that would permit us to decide when a federal agency ought to address specific security risks or permit us to second guess how that agency should exercise those responsibilities." He further added, "I cannot conclude that Congress intended for our Statute to be read so expansively as to impose additional—in this case bargaining—requirements on federal agencies *before* they can act to secure the integrity of their federal IT systems, the breach of which, could directly impact our nation's security and economic prosperity."

H.R. 4361 will settle the unfortunate ambiguity identified by the majority in the 2014 FLRA case and make clear congressional intent with respect to agencies' sole and exclusive authority to take appropriate and timely action as permitted by law to secure their IT systems, pursuant to the provisions of FISMA.

Notably, the need for this bill was highlighted in June and July of 2015, when news of the largest government data breach to date became public, clearly illustrating the need for agencies to be able to take swift action in response to IT threats. In this case, in June and July 2015, the Office of Personnel Management announced that the personally-identifiable information (PII) of over 22 million individuals—current and former federal employees, contractors, and other related individuals—had been compromised as a result of a cyber attack. The data compromised included sensitive data collected for purposes of background investigations, including 5.6 million fingerprints. The national security impact of this breach will resonate for decades to come. In June 2015, government unions representing the federal workers and retirees who were impacted by the OPM data breach sued OPM for failing to protect their data.[2]

Moreover, in July 2015 the specific issue raised by the FLRA in 2014 was raised again as OPM sought to mitigate the security vulnerabilities as they continued investigation of the data breach incident. At that time, OPM took action to restrict employees' ac-

[2] AFGE Files Class Action Lawsuit against OPM Officials over Data Breach, *AFGE Press Release,* June 29, 2015, available at: *https://www.afge.org/?PressReleaseID=1771.*

cess to Facebook, Gmail and other sites in the interest of security.[3] In response, the American Federation of Government Employees (AFGE) Local 32 President complained that employees were shut out and OPM did not provide an opportunity for collective bargaining before taking this action. Although the union did not formally challenge the action, the 2014 FLRA case was cited as support for the demand to collectively bargain.

In response to this situation, both the sponsor of the legislation, Congressman Gary Palmer (R–AL), and Chairman Jason Chaffetz (R–UT) have stated that in light of the OPM data breach and the ambiguity of the FISMA language pointed out in the 2014 FLRA case, the need for legislation was apparent.[4] Thus, H.R. 4361 was written to provide clarity on agencies' FISMA responsibilities that should empower agencies to take appropriate and timely action as permitted by law to secure IT systems in response to threats the agency identifies and in accordance with policy direction from the Office of Management and Budget (OMB) and operational directives from DHS.

Importantly, H.R. 4361 does not exempt agencies from any other statute; it simply allows agencies the discretion to not bargain with its employees in order to take appropriate and timely action as permitted by law to secure IT networks. In particular, H.R. 4361 does not modify existing authority and responsibilities of the Director of the OMB and the Secretary of Homeland Security under title 44 section 3553 of the U.S. Code. In fact, by clarifying the law and ensuring that actions taken to secure agency IT systems are lawful when agencies do not provide an opportunity to bargain, H.R. 4361 will empower agencies to quickly respond to OMB and DHS direction and guidance. H.R. 4361 also does not modify requirements of the Privacy Act (5 U.S.C. § 552a), federal procurement law under Title 41 of the U.S. Code, and the Cybersecurity Act of 2015.[5]

LEGISLATIVE HISTORY

On June 16, 2015, the Committee held a hearing on OPM and the 2015 reported data breach. During this hearing, Congressman Gary Palmer (R–AL) discussed with the Director of OPM the risks related to federal employees accessing personnel e-mail accounts and the requirement to provide unions with the opportunity to bargain before restricting this access.

On January 11, 2016, Congressman Palmer introduced H.R. 4361, the Federal Information Systems Safeguards Act. The bill was referred to the Committee on Oversight and Government Reform. On March 1, 2016, the Committee on Oversight and Government Reform ordered the legislation favorably reported by a record vote of 21 to 16.

---

[3] OPM's Shift in Security Posture Raises Labor Law Questions, *Federal Computer Week,* July 15, 2015, available at: *https://fcw.com/articles/2015/07/15/opm-labor-law.aspx.*

[4] How Collective Bargaining Undermines Cybersecurity by Gary Palmer and Jason Chaffetz, *Washington Times,* February 24, 2016.

[5] *OPM Data Breach Part I: Hearing Before the H. Comm. On Oversight and Gov't Reform,* 114th Cong. (June 16, 2015).

SECTION-BY-SECTION

Section 1. Short title

Designates 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

Amends the Federal Information Security Management Act (44 U.S.C. § 3554) to clarify that the head of each agency has sole and exclusive authority to reduce or eliminate current or future security weaknesses and risks associated with its information technology or information systems in a timely manner.

Section 3. Rule of construction

Provides that Section 2 may not be construed to modify any provision or amendment of the Cybersecurity Act of 2015 (Public Law 114–113).

EXPLANATION OF AMENDMENTS

During Full Committee consideration of the bill, Congressman Palmer offered an amendment in the nature of a substitute to the bill, which included a provision to make clear that H.R. 4361 does not modify the Cybersecurity Act of 2015 (Public Law 114–113). The amendment in the nature of a substitute was agreed to by voice vote.

COMMITTEE CONSIDERATION

On March 1, 2016, the Committee met in open session and ordered reported favorably the bill, H.R. 4361, by a roll call vote, a quorum being present.

ROLL CALL VOTES

There was one recorded vote during consideration of H.R. 4361:

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

114TH CONGRESS

ROLL CALL

Vote #: 3

Vote on: H.R. 4361 – Report to House Favorably **Date: 3-1-16**

Republicans	Aye	No	Present	Democrats	Aye	No	Present
MR. CHAFFETZ (UT) *(Chairman)*	X			MR. CUMMINGS (MD) *(Ranking)*		X	
MR. MICA (FL)	X			MRS. MALONEY (NY)		X	
MR. TURNER (OH)				MS. NORTON (DC)		X	
MR. DUNCAN (TN)				MR. CLAY (MO)		X	
MR. JORDAN (OH)	X			MR. LYNCH (MA)		X	
MR. WALBERG (MI)	X			MR. COOPER (TN)		X	
MR. AMASH (MI)	X			MR. CONNOLLY (VA)			
MR. GOSAR (AZ)	X			MR. CARTWRIGHT (PA)		X	
MR. DesJARLAIS (TN)	x			MS. DUCKWORTH (IL)		X	
MR. GOWDY (SC)				MS. KELLY (IL)		X	
MR. FARENTHOLD (TX)				MS. LAWRENCE (MI)		X	
MRS. LUMMIS (WY)	X			MR. LIEU (CA)	X		
MR. MASSIE (KY)	X			MRS. WATSON COLEMAN (NJ)		X	
MR. MEADOWS (NC)	X			MS. PLASKETT (VI)		X	
MR. DeSANTIS (FL)	X			MR. DeSAULNIER (CA)		X	
MR. MULVANEY (SC)				MR. BOYLE (PA)		X	
MR. BUCK (CO)	X			MR. WELCH (VT)		X	
MR. WALKER (NC)	X			MS. LUJAN GRISHAM (NM)		X	
MR. BLUM (IA)	X						
MR. HICE (GA)	X						
MR. RUSSELL (OK)	X						
MR. CARTER (GA)	X						
MR. GROTHMAN (WI)	X						
MR. HURD (TX)	X						
MR. PALMER (AL)	X						

Roll Call Totals: Ayes: 21 Nays: 16 Present:

Passed: X Failed: _____

APPLICATION OF LAW TO THE LEGISLATIVE BRANCH

Section 102(b)(3) of Public Law 104–1 requires a description of the application of this bill to the legislative branch where the bill relates to the terms and conditions of employment or access to public services and accommodations. This bill amends section 3554 of title 44, United States Code, to provide for enhanced security of Federal information systems. As such this bill does not relate to employment or access to public services and accommodations.

STATEMENT OF OVERSIGHT FINDINGS AND RECOMMENDATIONS OF THE COMMITTEE

In compliance with clause 3(c)(1) of rule XIII and clause (2)(b)(1) of rule X of the Rules of the House of Representatives, the Committee's oversight findings and recommendations are reflected in the descriptive portions of this report.

STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

In accordance with clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, the Committee's performance goal and objective of the bill is to amend section 3554 of title 44, United States Code, to provide for enhanced security of Federal information systems.

DUPLICATION OF FEDERAL PROGRAMS

No provision of this bill establishes or reauthorizes a program of the Federal Government known to be duplicative of another Federal program, a program that was included in any report from the Government Accountability Office to Congress pursuant to section 21 of Public Law 111–139, or a program related to a program identified in the most recent Catalog of Federal Domestic Assistance.

DISCLOSURE OF DIRECTED RULE MAKINGS

The Committee estimates that enacting this bill does not direct the completion of any specific rule makings within the meaning of 5 U.S.C. 551.

FEDERAL ADVISORY COMMITTEE ACT

The Committee finds that the legislation does not establish or authorize the establishment of an advisory committee within the definition of 5 U.S.C. App., Section 5(b).

UNFUNDED MANDATE STATEMENT

Section 423 of the Congressional Budget and Impoundment Control Act (as amended by Section 101(a)(2) of the Unfunded Mandate Reform Act, P.L. 104–4) requires a statement as to whether the provisions of the reported include unfunded mandates. In compliance with this requirement the Committee has received a letter from the Congressional Budget Office included herein.

EARMARK IDENTIFICATION

This bill does not include any congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9 of rule XXI.

COMMITTEE ESTIMATE

Clause 3(d)(1) of rule XIII of the Rules of the House of Representatives requires an estimate and a comparison by the Committee of the costs that would be incurred in carrying out this bill. However, clause 3(d)(2)(B) of that rule provides that this requirement does not apply when the Committee has included in its report a timely submitted cost estimate of the bill prepared by the Director of the Congressional Budget Office under section 402 of the Congressional Budget Act of 1974.

BUDGET AUTHORITY AND CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

With respect to the requirements of clause 3(c)(2) of rule XIII of the Rules of the House of Representatives and section 308(a) of the Congressional Budget Act of 1974 and with respect to requirements of clause (3)(c)(3) of rule XIII of the Rules of the House of Representatives and section 402 of the Congressional Budget Act of 1974, the Committee has received the following cost estimate for this bill from the Director of Congressional Budget Office:

MARCH 24, 2016.

Hon. JASON CHAFFETZ,
Chairman, Committee on Oversight and Government Reform,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 4361, 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.

H.R. 4361—Federal Information Systems Safeguards Act of 2016

The Federal Information Security Management Act (FISMA) provides a comprehensive framework to protect government information operations against threats. H.R. 4361 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 H.R. 4361 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 H.R. 4361 would not affect revenues.

CBO estimates that enacting H.R. 4361 would not increase direct spending or on-budget deficits in any of the four consecutive 10-year periods beginning in 2027.

H.R. 4361 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.

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

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (new matter is printed in italic and existing law in which no change is proposed is shown in roman):

TITLE 44, UNITED STATES CODE

* * * * * * *

CHAPTER 35—COORDINATION OF FEDERAL INFORMATION POLICY

* * * * * * *

SUBCHAPTER II—INFORMATION SECURITY

* * * * * * *

§ 3554. Federal agency responsibilities

(a) IN GENERAL.—The head of each agency shall—

(1) be responsible for—

(A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—

(i) information collected or maintained by or on behalf of the agency; and

(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

(B) complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines, including—

(i) information security standards promulgated under section 11331 of title 40;

(ii) operational directives developed by the Secretary under section 3553(b);

(iii) policies and procedures issued by the Director;

(iv) information security standards and guidelines for national security systems issued in accordance with law and as directed by the President; and

(v) emergency directives issued by the Secretary under section 3553(h); and

(C) ensuring that information security management processes are integrated with agency strategic, operational, and budgetary planning processes;

(2) ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including through—

(A) assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;

(B) determining the levels of information security appropriate to protect such information and information systems in accordance with standards promulgated under section 11331 of title 40, for information security classifications and related requirements;

(C) implementing policies and procedures to cost-effectively reduce risks to an acceptable level; and

(D) periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented;

(3) delegate to the agency Chief Information Officer established under section 3506 (or comparable official in an agency not covered by such section) the authority to ensure compliance with the requirements imposed on the agency under this subchapter, including—

(A) designating a senior agency information security officer who shall—

(i) carry out the Chief Information Officer's responsibilities under this section;

(ii) possess professional qualifications, including training and experience, required to administer the functions described under this section;

(iii) have information security duties as that official's primary duty; and

(iv) head an office with the mission and resources to assist in ensuring agency compliance with this section;

(B) developing and maintaining an agencywide information security program as required by subsection (b);

(C) developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements, including those issued under section 3553 of this title and section 11331 of title 40;

(D) training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities; and

(E) assisting senior agency officials concerning their responsibilities under paragraph (2);

(4) ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines;

(5) ensure that the agency Chief Information Officer, in coordination with other senior agency officials, reports annually

to the agency head on the effectiveness of the agency information security program, including progress of remedial actions;

(6) ensure that senior agency officials, including chief information officers of component agencies or equivalent officials, carry out responsibilities under this subchapter as directed by the official delegated authority under paragraph (3); and

(7) ensure that all personnel are held accountable for complying with the agency-wide information security program implemented under subsection (b).

(b) AGENCY PROGRAM.—Each agency shall develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes—

(1) periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency, which may include using automated tools consistent with standards and guidelines promulgated under section 11331 of title 40;

(2) policies and procedures that—

(A) are based on the risk assessments required by paragraph (1);

(B) cost-effectively reduce information security risks to an acceptable level;

(C) ensure that information security is addressed throughout the life cycle of each agency information system; and

(D) ensure compliance with—

(i) the requirements of this subchapter;

(ii) policies and procedures as may be prescribed by the Director, and information security standards promulgated under section 11331 of title 40;

(iii) minimally acceptable system configuration requirements, as determined by the agency; and

(iv) any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President;

(3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate;

(4) security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of—

(A) information security risks associated with their activities; and

(B) their responsibilities in complying with agency policies and procedures designed to reduce these risks;

(5) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, of which such testing—

(A) shall include testing of management, operational, and technical controls of every information system identified in the inventory required under section 3505(c);

(B) may include testing relied on in an evaluation under section 3555; and

(C) shall include using automated tools, consistent with standards and guidelines promulgated under section 11331 of title 40;

(6) a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;

(7) procedures for detecting, reporting, and responding to security incidents, which—

(A) shall be consistent with the standards and guidelines described in section 3556(b);

(B) may include using automated tools; and

(C) shall include—

(i) mitigating risks associated with such incidents before substantial damage is done;

(ii) notifying and consulting with the Federal information security incident center established in section 3556; and

(iii) notifying and consulting with, as appropriate—

(I) law enforcement agencies and relevant Offices of Inspector General and Offices of General Counsel;

(II) an office designated by the President for any incident involving a national security system;

(III) for a major incident, the committees of Congress described in subsection (c)(1)—

(aa) not later than 7 days after the date on which there is a reasonable basis to conclude that the major incident has occurred; and

(bb) after the initial notification under item (aa), within a reasonable period of time after additional information relating to the incident is discovered, including the summary required under subsection (c)(1)(A)(i); and

(IV) any other agency or office, in accordance with law or as directed by the President; and

(8) plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

(c) AGENCY REPORTING.—

(1) ANNUAL REPORT.—

(A) IN GENERAL.—Each agency shall submit to the Director, the Secretary, the Committee on Government Reform, the Committee on Homeland Security, and the Committee on Science of the House of Representatives, the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate, the appropriate authorization and appropriations committees of Congress, and the Comptroller General

a report on the adequacy and effectiveness of information security policies, procedures, and practices, including—

(i) a description of each major information security incident or related sets of incidents, including summaries of—

(I) the threats and threat actors, vulnerabilities, and impacts relating to the incident;

(II) the risk assessments conducted under section 3554(a)(2)(A) of the affected information systems before the date on which the incident occurred;

(III) the status of compliance of the affected information systems with applicable security requirements at the time of the incident; and

(IV) the detection, response, and remediation actions;

(ii) the total number of information security incidents, including a description of incidents resulting in significant compromise of information security, system impact levels, types of incident, and locations of affected systems;

(iii) a description of each major information security incident that involved a breach of personally identifiable information, as defined by the Director, including—

(I) the number of individuals whose information was affected by the major information security incident; and

(II) a description of the information that was breached or exposed; and

(iv) any other information as the Director or the Secretary, in consultation with the Director, may require.

(B) UNCLASSIFIED REPORT.—

(i) IN GENERAL.—Each report submitted under subparagraph (A) shall be in unclassified form, but may include a classified annex.

(ii) ACCESS TO INFORMATION.—The head of an agency shall ensure that, to the greatest extent practicable, information is included in the unclassified version of the reports submitted by the agency under subparagraph (A).

(2) OTHER PLANS AND REPORTS.—Each agency shall address the adequacy and effectiveness of information security policies, procedures, and practices in management plans and reports.

(d) PERFORMANCE PLAN.—(1) In addition to the requirements of subsection (c), each agency, in consultation with the Director, shall include as part of the performance plan required under section 1115 of title 31 a description of—

(A) the time periods; and

(B) the resources, including budget, staffing, and training,

that are necessary to implement the program required under subsection (b).

(2) The description under paragraph (1) shall be based on the risk assessments required under subsection (b)(1).

(e) PUBLIC NOTICE AND COMMENT.—Each agency shall provide the public with timely notice and opportunities for comment on proposed information security policies and procedures to the extent that such policies and procedures affect communication with the public.

(f) AGENCY DISCRETION.—The head of each agency has the sole and exclusive authority, with respect to any information technology or information system under the control of such agency—

(1) to take any action the agency determines to be necessary to reduce or eliminate security weakness and risk, including to protect the information contained in the information technology or information system; and

(2) to take any action the agency determines to be necessary to reduce or eliminate future security weakness and risk, including to protect the information contained in the information technology or information system.

* * * * * * *

MINORITY VIEWS

Democratic Members of the Committee strongly oppose H.R. 4361. This bill would modify the Federal Information Management Security Act (FISMA) to give each agency head exclusive authority to take any action deemed necessary to reduce or eliminate security weakness and risk with respect to the agency's information technology (IT) systems.

This bill is unnecessary, and the language of the bill is dangerously overbroad and subject to abuse. The Committee has not held a single hearing on this bill to explore the potential impact it might have on security, human rights, privacy, contracting, or transparency protections. The Committee should investigate the impact of this bill before rushing to enact it.

The Majority asserts that this legislation "clarifies federal agencies' existing authority under [FISMA] to secure their IT systems by clarifying that agencies' IT security functions are not subject to collective bargaining with federal employees." [1]

FISMA requires agency heads to provide "information security protections commensurate with the risk and magnitude of the harm" posed to agency information.[2] The Majority has not demonstrated any gaps in this authority that would prevent an agency head from taking an action such as regulating employee use of personal email on work devices.

It is also not clear that blocking personal email is necessary. The House Committee on Science, Space, and Technology held a subcommittee hearing entitled, "Cybersecurity: What the Federal Government Can Learn from the Private Sector." [3] During that hearing, the bill's sponsor, Rep. Gary Palmer, asked a panel of private sector cybersecurity experts whether it makes sense to prevent employees from using company or government IT systems to access personal websites and emails.

In response, one expert stated, "I think it's unrealistic, from a day-to-day perspective, from an innovation perspective, to assume people at work aren't accessing outside information." This expert continued: "I just think if you want to be competitive, from a business perspective, against other companies you have to assume that your employees are going to be fully connected at all times." [4]

This testimony illustrates why the Committee needs to investigate the impact of this bill before rushing to enact it.

If the Majority wants to move forward with legislation to block access by agency employees to personal email, the Majority should

---

[1] House Committee on Oversight and Government Reform, *Federal Information Systems Safeguard Act of 2016,* 114th Cong. (2016).

[2] Pub.L. No. 113–283 (2014).

[3] House Committee on Science, Space and Technology, Subcommittee on Oversight and Subcommittee on Research and Technology, *Hearing on Cybersecurity: What the Federal Government Can Learn from the Private Sector* (Jan. 8, 2016).

[4] *Id.*

draft a bill that simply does that. Instead, the Majority drafted a bill that gives agency heads extraordinary authority that is open to abuse.

Democratic Members are concerned that under this bill an agency head could, in the name of security, take actions that conflict with transparency laws, the Privacy Act, fair contracting laws, or employment protections. We are also concerned that the bill would allow an agency head to bypass directives from the Department of Homeland Security (DHS) on cyber security. DHS has raised concerns that the bill could conflict with authorities over cybersecurity given to the Department and the Office of Management and Budget.

We can protect federal computer systems without the unnecessarily broad language included in this bill. Committee Democrats are willing to work together towards developing language that is carefully crafted towards fulfilling that goal. This dangerously overbroad bill is not the answer.

ELIJAH E. CUMMINGS,
Ranking Member.

○