113TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPORT
113–562

SAFE AND SECURE FEDERAL WEBSITES ACT OF 2014

JULY 28, 2014.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

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

R E P O R T

[To accompany H.R. 3635]

[Including cost estimate of the Congressional Budget Office]

The Committee on Oversight and Government Reform, to whom was referred the bill (H.R. 3635) to ensure the functionality and security of new Federal websites that collect personally identifiable information, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

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 "Safe and Secure Federal Websites Act of 2014".

SEC. 2. ENSURING FUNCTIONALITY AND SECURITY OF NEW FEDERAL WEBSITES THAT COLLECT PERSONALLY IDENTIFIABLE INFORMATION.

(a) CERTIFICATION REQUIREMENT.—

(1) IN GENERAL.—Except as otherwise provided under this subsection, an agency may not deploy or make available to the public a new Federal PII website until the date on which the chief information officer of the agency submits a certification to Congress that the website is fully functional and secure.

(2) TRANSITION.—In the case of a new Federal PII website that is operational on the date of the enactment of this Act, paragraph (1) shall not apply until the end of the 90-day period beginning on such date of enactment. If the certification required under paragraph (1) for such website has not been submitted to Congress before the end of such period, the head of the responsible agency shall render the website inaccessible to the public until such certification is submitted to Congress.

(3) EXCEPTION FOR BETA WEBSITE WITH EXPLICIT PERMISSION.—Paragraph (1) shall not apply to a website (or portion thereof) that is in a development or testing phase, if the following conditions are met:

(A) A member of the public may access PII-related portions of the website only after executing an agreement that acknowledges the risks involved.

(B) No agency compelled, enjoined, or otherwise provided incentives for such a member to access the website for such purposes.

(4) CONSTRUCTION.—Nothing in this section shall be construed as applying to a website that is operated entirely by an entity (such as a State or locality) that is independent of the Federal Government, regardless of the receipt of funding in support of such website from the Federal Government.

(b) DEFINITIONS.—In this section:

(1) AGENCY.—The term "agency" has the meaning given that term under section 551 of title 5, United States Code.

(2) FULLY FUNCTIONAL.—The term "fully functional" means, with respect to a new Federal PII website, that the website can fully support the activities for which it is designed or intended with regard to the eliciting, collection, storage, or maintenance of personally identifiable information, including handling a volume of queries relating to such information commensurate with the purpose for which the website is designed.

(3) NEW FEDERAL PERSONALLY IDENTIFIABLE INFORMATION WEBSITE (NEW FEDERAL PII WEBSITE).—The terms "new Federal personally identifiable information website" and "new Federal PII website" mean a website that—

(A) is operated by (or under a contract with) an agency;

(B) elicits, collects, stores, or maintains personally identifiable information of individuals and is accessible to the public; and

(C) is first made accessible to the public and collects or stores personally identifiable information of individuals, on or after October 1, 2012.

(4) OPERATIONAL.—The term "operational" means, with respect to a website, that such website elicits, collects, stores, or maintains personally identifiable information of members of the public and is accessible to the public.

(5) PERSONALLY IDENTIFIABLE INFORMATION (PII).—The terms "personally identifiable information" and "PII" mean any information about an individual elicited, collected, stored, or maintained by an agency, including—

(A) any information that can be used to distinguish or trace the identity of an individual, such as a name, a social security number, a date and place of birth, a mother's maiden name, or biometric records; and

(B) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

(6) RESPONSIBLE AGENCY.—The term "responsible agency" means, with respect to a new Federal PII website, the agency that is responsible for the operation (whether directly or through contracts with other entities) of the website.

(7) SECURE.—The term "secure" means, with respect to a new Federal PII website, that the following requirements are met:

(A) The website is in compliance with subchapter III of chapter 35 of title 44, United States Code.

(B) The website ensures that personally identifiable information elicited, collected, stored, or maintained in connection with the website is captured at the latest possible step in a user input sequence.

(C) The responsible agency for the website has taken reasonable efforts to minimize domain name confusion, including through additional domain registrations.

(D) The responsible agency requires all personnel who have access to personally identifiable information in connection with the website to have completed a Standard Form 85P and signed a non-disclosure agreement with

respect to personally identifiable information, and the agency takes proper precautions to ensure only trustworthy persons may access such information.

(E) The responsible agency maintains (either directly or through contract) sufficient personnel to respond in a timely manner to issues relating to the proper functioning and security of the website, and to monitor on an ongoing basis existing and emerging security threats to the website.

(8) STATE.—The term "State" means each State of the United States, the District of Columbia, each territory or possession of the United States, and each federally recognized Indian tribe.

SEC. 3. PRIVACY BREACH REQUIREMENTS.

(a) INFORMATION SECURITY AMENDMENT.—Subchapter III of chapter 35 of title 44, United States Code, is amended by adding at the end the following:

"§ 3550. Privacy breach requirements

"(a) POLICIES AND PROCEDURES.—The Director of the Office of Management and Budget shall establish and oversee policies and procedures for agencies to follow in the event of a breach of information security involving the disclosure of personally identifiable information, including requirements for—

"(1) not later than 72 hours after the agency discovers such a breach, or discovers evidence that reasonably indicates such a breach has occurred, notice to the individuals whose personally identifiable information could be compromised as a result of such breach;

"(2) timely reporting to a Federal cybersecurity center, as designated by the Director of the Office of Management and Budget; and

"(3) any additional actions that the Director finds necessary and appropriate, including data breach analysis, fraud resolution services, identity theft insurance, and credit protection or monitoring services.

"(b) REQUIRED AGENCY ACTION.—The head of each agency shall ensure that actions taken in response to a breach of information security involving the disclosure of personally identifiable information under the authority or control of the agency comply with policies and procedures established by the Director of the Office of Management and Budget under subsection (a).

"(c) REPORT.—Not later than March 1 of each year, the Director of the Office of Management and Budget shall report to Congress on agency compliance with the policies and procedures established under subsection (a).

"(d) FEDERAL CYBERSECURITY CENTER DEFINED.—The term 'Federal cybersecurity center' means any of the following:

"(1) The Department of Defense Cyber Crime Center.

"(2) The Intelligence Community Incident Response Center.

"(3) The United States Cyber Command Joint Operations Center.

"(4) The National Cyber Investigative Joint Task Force.

"(5) Central Security Service Threat Operations Center of the National Security Agency.

"(6) The United States Computer Emergency Readiness Team.

"(7) Any successor to a center, team, or task force described in paragraphs (1) through (6).

"(8) Any center that the Director of the Office of Management and Budget determines is appropriate to carry out the requirements of this section.".

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of sections for subchapter III of chapter 35 of title 44, United States Code, is amended by adding at the end the following:

"3550. Privacy breach requirements.".

COMMITTEE STATEMENT AND VIEWS

PURPOSE AND SUMMARY

H.R. 3635, the Safe and Secure Federal Websites Act of 2014, will help ensure the functionality and security of federal websites, giving individuals confidence that their privacy and personal information is secure. The bill guards against the loss of the public's trust by requiring agency chief information officers to certify that federal websites collecting personally identifiable information are fully functional and secure. In addition, the bill requires agencies to notify affected individuals that their personally identifiable in-

formation may have been compromised within 72 hours of a known or suspected data breach.

BACKGROUND AND NEED FOR LEGISLATION

2013 marked a year of high-profile data breaches. From data breaches at Target, one of the nation's largest retail chains, to Neiman Marcus, a high-end department store chain, the public is now more aware than ever of the potential severity and consequences of such occurrences.[1] Other widely publicized data breaches at federal agencies in recent years include the Federal Retirement Thrift Investment Board (2012), the Federal Aviation Administration (2009), and the Department of Veterans Affairs (2006).[2] The loss of public trust resulting from large scale data breaches is damaging to the economy and the overall fabric and spirit of our country. The public should feel confident and secure in knowing that their personal information is protected by businesses and especially by the government who serves them.

Ensuring website security is especially important in an era where the federal government increasingly relies on technology to conduct its work more efficiently. Balancing the desire to strive for technological advancements with the need to constantly monitor and neutralize cyber threats and vulnerabilities is vital. The federal government should be ever vigilant in working to regain and maintain the public's trust. The "Safe and Secure Federal Websites Act of 2014" is a major step in reestablishing that trust.

This act requires, among other things, the Director of the Office of Management and Budget (OMB) to establish and oversee policies and procedures for agencies to follow in the event of a breach of information security involving the disclosure of personally identifiable information. This includes establishing requirements for the timely notification of individuals affected; timely reporting of the compromise to a federal cyber security center; and any additional actions the Director deems necessary and appropriate. These actions can include data breach analysis, fraud resolution services, identity theft insurance, and credit protection or monitoring services. Further, OMB is required to report to Congress on its oversight of agencies implementation of its policies. In a December 2013 report, GAO found that agency responses to breaches of personally identifiable information were inconsistent and recommended that OMB update its guidance on federal agencies' response to data breach.[3] Though OMB previously issued five memoranda to advise agencies on proper protocols, GAO found the guid-

[1] Senate Judiciary Committee hearing: *Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime.* February 4, 2014. http://www.judiciary.senate.gov/meetings/privacy-in-the-digital-age-preventing-data-breaches-and-combating-cybercrime.

[2] The Federal Retirement Thrift Investment Board data breach was the subject of a Senate Committee on Homeland Security & Governmental Affairs (Subcommittee on Oversight of Government Management, the Federal Workforce and the District of Columbia) hearing: *State of Federal Privacy and Data Security Law: Lagging Behind the Times?* July 31, 2012. http://www.hsgac.senate.gov/subcommittees/oversight-of-government-management/hearings/state-of-federal-privacy-and-data-security-law-lagging-behind-the-times.

The Federal Aviation Administration issued a press release on February 9, 2009 about its data breach: *Press Release—FAA Notifies Employees of Personal Identity Breach.* http://www.faa.gov/news/press_releases/news_story.cfm?newsId=10394.

Department of Veterans Affairs Office of Inspector General, *Review of Issues Related to the Loss of VA Information Involving the Identity of Millions of Veterans,* Report No. 06–02238–163 (Washington, D.C.: July 11, 2006).

[3] GAO, *Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent,* GAO–14–34 (Washington, D.C.: Dec. 9, 2013).

ance to be incomplete thus contributing to agencies' inconsistent implementation.[4] Adopting the "Safe and Secure Federal Websites Act of 2014" will help remedy the problem of data breach.

SECTION-BY-SECTION

Section 1. Short title

The short title of the bill is the "Safe and Secure Federal Websites Act of 2014."

Section 2. Ensuring functionality and security of new federal websites that collect personally identifiable information

Federal agency chief information officers must certify to Congress the functionality and security of new (or substantially modified) agency websites that collect personally identifiable information. The bill applies to websites created (or substantially modified) on or after October 1, 2012, and requires agency chief information officers to submit certifications within 90 days for websites operational on the date of enactment. Agency heads must render inaccessible each website that is not certified before the end of the certification period established in the bill. An exception is made for beta websites.

Under the bill, certification as a "fully functional" website means the website can fully support the activities for which it is designed, including the collection, storage, and maintenance of personally identifiable information.

Under the bill, certification as a "secure" website means the website complies with the Federal Information Security Management Act (FISMA); the host agency has taken steps to minimize domain name confusion; personally identifiable information is captured at the latest possible step in the data collection sequence; individuals who have access to personally identifiable information have completed public trust questionnaire and signed a non-disclosure agreement; and the agency maintains sufficient personnel to respond in a timely manner to issues related to proper functioning and security of the website, including emerging security threats.

The bill uses a definition developed by the National Institute of Standards and Technology (Special Publication 800–122) to describe personally identifiable information.

Section 3. Privacy breach requirements

The Director of the Office of Management and Budget shall establish and oversee policies and procedures for agencies to follow in the event of a breach of information security involving the disclosure of personally identifiable information. Notice must be given to individuals whose personally identifiable information could be compromised within 72 hours of the agency discovering a breach or discovering evidence that reasonably indicates occurrence of a breach.

---

[4] OMB, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information,* M–07–16 (May 22, 2007); OMB, *Use of Commercial Credit Monitoring Services Blanket Purchase Agreements,* M–07–04 (Washington, D.C.: Dec. 22, 2006); OMB, *Recommendations for Identity Theft Related Data Breach Notification* (Washington, D.C.: Sept. 20, 2006); OMB, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments,* M–06–19 (July 12, 2006); and OMB, *Safeguarding Personally Identifiable Information,* M–06–15 (Washington, D.C.: May 22, 2006.

The Director of the Office of Management and Budget must annually report to Congress by March 1 of each year on agency compliance with the breach notification procedures.

EXPLANATION OF AMENDMENTS

The provisions of the adopted amendments are explained in this report.

COMMITTEE CONSIDERATION

On March 12, 2014, the Committee met in open session and ordered reported favorably the bill, H.R. 3635, as amended, by voice vote, a quorum being present.

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 requires agencies to notify affected individuals that their personally identifiable information may have been compromised within 72 hours of a known or suspected data breach. 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 goals and objectives are reflected in the descriptive portions of this report.

DUPLICATION OF FEDERAL PROGRAMS

No provision of H.R. 3635 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

H.R. 3635 requires the Director of the Office of Management and Budget to establish policies and procedures for agencies to follow in the event of a breach of information security involving the disclosure of personally identifiable information.

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 Mandates 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

H.R. 3635 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)(2) 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 H.R. 3635. However, clause 3(d)(3)(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.

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 H.R. 3635 from the Director of Congressional Budget Office:

APRIL 22, 2014.

Hon. DARRELL ISSA,
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. 3635, the Safe and Secure Federal Websites Act of 2014.

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

Sincerely,

DOUGLAS W. ELMENDORF.

Enclosure.

H.R. 3635—Safe and Secure Federal Websites Act of 2014

CBO estimates that enacting H.R. 3635 would have no significant effect on the federal budget. The legislation would amend federal laws that protect the privacy of personally identifiable information collected by the government. Personally identifiable information includes any information that identifies an individual such as name, Social Security number, and medical or financial records. The legislation would prohibit an agency from deploying a new website until the agency's Chief Information Officer certifies that all such information is safe and secure. Existing federal websites would have 90 days following enactment of H.R. 3635 to comply with this requirement. The legislation also would require the Office of Management and Budget (OMB) to issue policies and procedures for agencies to follow in the event of a security breach of a federal data system that contains personally identifiable information.

No single federal law or regulation governs the security of all types of sensitive personal information collected by federal agencies. The Federal Information Security Management Act requires each federal agency to develop, document, and implement an agencywide security program for sensitive information. The Privacy Act of 1974 governs the collection, use, and dissemination by federal agencies of personal records. OMB's "Breach Notification Policy" requires all agencies to implement a policy to safeguard personally identifiable information and to provide notification of a security breach.

Because those laws and policies regarding the security of personally identifiable information are already in place, CBO estimates that the cost of certifying the safety of information collected by federal websites would be less than $500,000 over the next five years. 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. Enacting the bill would not affect revenues.

H.R. 3635 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act and would impose no costs on state, local, or tribal governments.

The CBO staff contact for this estimate is Matthew Pickford. The estimate was approved by Theresa Gullo, 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 I—FEDERAL INFORMATION POLICY

SUBCHAPTER III—INFORMATION SECURITY

* * * * * * *

§ 3550. Privacy breach requirements

(a) POLICIES AND PROCEDURES.—The Director of the Office of Management and Budget shall establish and oversee policies and procedures for agencies to follow in the event of a breach of information security involving the disclosure of personally identifiable information, including requirements for—

(1) not later than 72 hours after the agency discovers such a breach, or discovers evidence that reasonably indicates such a breach has occurred, notice to the individuals whose personally identifiable information could be compromised as a result of such breach;

(2) timely reporting to a Federal cybersecurity center, as designated by the Director of the Office of Management and Budget; and

(3) any additional actions that the Director finds necessary and appropriate, including data breach analysis, fraud resolution services, identity theft insurance, and credit protection or monitoring services.

(b) REQUIRED AGENCY ACTION.—The head of each agency shall ensure that actions taken in response to a breach of information security involving the disclosure of personally identifiable information under the authority or control of the agency comply with policies and procedures established by the Director of the Office of Management and Budget under subsection (a).

(c) REPORT.—Not later than March 1 of each year, the Director of the Office of Management and Budget shall report to Congress on agency compliance with the policies and procedures established under subsection (a).

(d) FEDERAL CYBERSECURITY CENTER DEFINED.—The term "Federal cybersecurity center" means any of the following:

(1) The Department of Defense Cyber Crime Center.

(2) The Intelligence Community Incident Response Center.

(3) The United States Cyber Command Joint Operations Center.

(4) The National Cyber Investigative Joint Task Force.

(5) Central Security Service Threat Operations Center of the National Security Agency.

(6) The United States Computer Emergency Readiness Team.

(7) Any successor to a center, team, or task force described in paragraphs (1) through (6).

(8) Any center that the Director of the Office of Management and Budget determines is appropriate to carry out the requirements of this section.

* * * * * * *

○