114TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPORT
114–390

SAFE AND SECURE FEDERAL WEBSITES ACT OF 2015

JANUARY 6, 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

[To accompany H.R. 451]

[Including cost estimate of the Congressional Budget Office]

The Committee on Oversight and Government Reform, to whom was referred the bill (H.R. 451) to ensure the functionality and security of new Federal websites that collect personally identifiable information, and for other purposes, having considered the same, reports favorably thereon with an amendment and recommends 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 2015".

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 II 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 encrypted, masked, or taken other similar actions to protect personally identifiable information elicited, collected, stored, or maintained in connection with the website.

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

(E) 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 that only the fewest reasonable number of trustworthy persons may access such information.

(F) 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 II of chapter 35 of title 44, United States Code, is amended by adding at the end the following:

"§ 3559. 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 II of chapter 35 of title 44, United States Code, is amended by adding at the end the following:

"3559. Privacy breach requirements.".

COMMITTEE STATEMENT AND VIEWS

PURPOSE AND SUMMARY

H.R. 451, the Safe and Secure Federal Websites Act of 2015, would enhance security and functionality requirements for federal websites handling personally identifiable information (PII). The legislation would require certification that new federal websites meet certain standards for security and functionality before the website can be made accessible to the public and would prohibit federal websites made accessible after October 1, 2012, from being kept available to the public without this certification. The legislation would help increase public trust by heightening security standards for the protection of PII. The legislation would also increase the number of required actions for federal agencies in the event of a data breach involving PII, including a requirement to notify potential victims of the breach within 72 hours of the discovery that their information may have been compromised.

BACKGROUND AND NEED FOR LEGISLATION

Data breaches are becoming increasingly prevalent and damaging to the American public. At the same time, there is growing demand for access to web-based services both in the private and public sectors. Federal agencies are increasingly offering online service options for purposes of meeting these demands, providing further access, and increasing efficiency of services.[1] Federal agencies have a responsibility to the public trust, which includes taking all necessary measures to protect information that the American people have entrusted to their government.

Recent reports and incidents have indicated an inconsistent and insufficient approach to information security protocols across the federal government. Last year, reported incidents involving PII nearly tripled compared to the number reported only five years before—increasing from 10,481 in fiscal year 2009 to 27,624 in fiscal year 2014.[2]

Even a small selection of incidents from 2014 and 2015 show the widespread impact of data breaches. A September 2014 breach of the U.S. Postal Service resulted in unauthorized access to PII of an estimated 800,000 postal employees.[3] From February to May 2015, breaches of an Internal Revenue Service website led to the release of approximately 100,000 taxpayers' PII.[4] In June 2015, the Office of Personnel Management (OPM) reported a cyber-intrusion detected in April 2015. The intrusion into OPM computer systems re-

---

[1] Gov't Accountability Office, *Testimony before the Subc. on Cybersecurity, Infrastructure Protection, & Security Technologies, Comm. on Homeland Security, Cybersecurity: Recent Data Breaches Illustrate Need for Strong Controls across Federal Agencies* (June 24, 2015) (GAO–15–725T), *available at http://www.gao.gov/assets/680/670935.pdf* [hereinafter GAO June 2015]; *See* S. Comm. on Homeland Security & Gov't Affairs, *The IRS Data Breach: Steps to Protect Americans' Personal Information,* (June 2, 2015) (statement of John A. Koskinen, Commissioner, Internal Revenue Service), *available at http://www.hsgac.senate.gov/hearings/the-irs-data-breach-steps-to-protect-americans-personal-information.*

[2] GAO June 2015, *supra* note 1.

[3] GAO June 2015, *supra* note 1.

[4] S. Comm. on Finance, *Internal Revenue Service Data Theft Affecting Taxpayer Information,* 114th Cong. (June 2, 2015) (statement of John A. Koskinen, Commissioner, Internal Revenue Service), *available at http://www.finance.senate.gov/imo/media/doc/2015FINAL%20JAK%20testimony%20SFC%20060215%20on%20GT.pdf.*

sulted in the compromise of 4.2 million individuals' PII.[5] A separate breach of OPM's systems exposed background investigation data—including the highly sensitive information provided by federal employees and federal contractor through the SF–86.[6] According to current reports, the breach may have compromised the PII data of as many as 18 million individuals.[7] This most recent OPM data breach brings a renewed sense of urgency to information security, and it is more important than ever for agencies to take the necessary precautions to protect PII.

Federal websites are an important component of agency collection and storage of PII, as websites are the predominant means whereby individual supply PII to the federal government. Federal websites often store and transmit PII data for workability, allowing users to update and change their data as needed. Thus, information security controls of federal PII websites are critical to the website's integrity and the safe collection and storage of PII data. According to the Government Accountability Office (GAO), cyber threats and data breaches show that Federal agencies must implement stronger information security controls.[8] GAO has reported weaknesses in information security controls at in a number of federal agencies, including not ensuring that only authorized users can access an agency's system and not using encryption to protect sensitive data from being intercepted and compromised.[9] H.R. 451 addresses these weaknesses by requiring that an agency's Chief Information Officer (CIO) certify that the agency has limited the number of individuals with access to PII and that PII data collected and maintained by agencies is encrypted, masked, or similarly protected.

In addition to security, functionality is a vital component for federal PII websites. Users should be able to use the websites for their intended purposes. The federal government continues to struggle with achieving functionality of its websites. The October 2013 deployment of Healthcare.gov is just one example of a website launched with significant functional deficiencies. The Patient Protection and Affordable Care Act relies on health insurance exchanges to facilitate the purchase of health insurance plans by individuals and small businesses.[10] The Department of Health and

---

[5] S. Comm. on Homeland Security & Gov't Affairs, *Under Attack: Federal Cybersecurity & the OPM Data Breach,* 114th Cong. (June 25, 2015) (statement of Katherine Archuleta, Director, Office of Personnel Management), *available at http://www.hsgac.senate.gov/hearings/under-attack-federal-cybersecurity-and-the-opm-data-breach;* Pierre Thomas, Jack Date, Mike Levin and Jack Cloherty, *Cabinet Secretaries Potentially exposed in OPM Data Beach,* ABCNEWS (June 9, 2015), *available at http://abcnews.go.com/US/cabinet-secretaries-potentially-exposed-opm-data-breach/story?id=31626021.*

[6] Damian Paletta, *Hackers Likely Stole Security-Clearance Information During Breach of Government Agency,* WALL ST. J., (June 12, 2015), *available at http://www.wsj.com/articles/security-clearance-information-likely-stolen-during-breach-of-government-agency-1434143820.*

[7] GovExec Staff, *Size of the OPM Hack Quadruples to 18 Million,* Gov't Executive, (June 22, 2015), *available at http://www.govexec.com/pay-benefits/2015/06/size-opm-hack-quadruples-18-million/116011/.*

[8] Gov't Accountability Office, *Testimony Before the Subcommittees on Research and Technology and Oversight, Committee on Science, Space, and Technology, H. of Representatives, Information Security: Cyber Threats & Data Breaches Illustrate Need for Stronger Controls across Federal Agencies* (July 8, 2015) (GAO–15–758T), *available at http://www.gao.gov/assets/680/671253.pdf;* Gov't Accountability Office, *Testimony Before the Comm. on Oversight & Gov't Reform, H. of Representatives, Cybersecurity: Actions Needed to Address Challenges Facing Federal Systems* (Apr. 22, 2015) (GAO–15–573T), *available at http://www.gao.gov/assets/670/669810.pdf.*

[9] *Id.* at 11.

[10] Patient Protection and Affordable Care Act, P.L.111–148, 3201–02, 124 Stat. 119, 442, 454 (Mar. 23, 2010), as amended.

Human Services' (HHS) Centers for Medicare & Medicaid Services (CMS) is responsible for facilitating the federal health insurance exchange and for launching and operating HealthCare.gov, the federal exchange web portal.[11]

HealthCare.gov launched on October 1, 2013, with numerous problems. Many consumers were unable to create accounts or browse the various insurance plans. Those consumers who were successful often had incomplete and inaccurate enrollment information sent from the exchange to health insurers.[12] There were significant problems with the functionality of HealthCare.gov for months after launch.[13]

Embedded in the functionality issues were security concerns that could result from technological deficiencies. A September 2014 GAO report found that while CMS took steps to protect PII maintained by Healthcare.gov, considering the degree of the systems complexity, CMS did not take all reasonable steps to limit security and privacy risks.[14] Similarly, the Committee's investigation into the Healthcare.gov rollout found that several CMS and HHS officials with responsibility for ensuring website functionality expressed concerns about the website's readiness prior to the Healthcare.gov rollout.[15] Officials advised delaying or limiting the full launch, but the website was deployed despite these concerns. However, to date, there has been no successful malicious breach of Healthcare.gov. H.R. 451 would require agency CIOs to certify to Congress that a new federal PII website is secure and fully functional for its intended purposes prior to launching the website.

LEGISLATIVE HISTORY

H.R. 451, the Safe and Secure Federal Websites Act of 2015, was introduced on January 21, 2015 by Congressman Charles J. "Chuck" Fleischmann (R–TN) and referred to the Committee on Oversight and Government Reform. On May 19, 2015, the Committee on Oversight and Government Reform ordered H.R. 451 favorably reported, with an amendment.

Similar legislation passed the House by voice vote, as amended, under suspension on the rules on July 28, 2014 (H.R. 3635).

---

[11] Gov't Accountability Office, *Actions Needed to Address Weaknesses in Information Security & Privacy Controls* (Sept. 2014) (GAO–14–730), *available at http://www.gao.gov/assets/670/665840.pdf* [hereinafter GAO Sept. 2014].

[12] Christopher Weaver, Shira Ovide and Louise Radnofsky, *Software, Design Defects Cripple Health-Care Website,* WALL ST. J. (Oct. 6, 2013), *available at http://online.wsj.com/news/articles/SB10001424052702304441404579119740283413018;* Christopher Weaver and Louise Radnofsky, *Health Website Woes Widen as Insurers Get Wrong Data,* WALL ST. J. (Oct. 17, 2013), *available at http://online.wsj.com/news/articles/SB10001424052702304410204579142141827109638.*

[13] Ezra Klein, *Five Thoughts on the Obamacare Disaster,* The Washington Post, Oct. 14, 2013, *available at http://www.washingtonpost.com/blogs/wonkblog/wp/2013/10/14/five-thoughts-on-the-obamacare-disaster/.*

[14] GAO Sept. 2014, *supra* note 9.

[15] *See* H. Comm. on Oversight & Gov't Reform, *HHS' Own Security Concerns about Healthcare.gov,* 113th Cong. (Jan. 16, 2014), *available at https://oversight.house.gov/hearing/hhs-security-concerns-healthcare-gov/;* H. Comm. on Oversight & Gov't Reform, *Obamacare Implementation: The Rollout of Healthcare.gov,* 113th Cong., (Nov. 13, 2013), *available at https://oversight.house.gov/hearing/obamacare-implementation-rollout-healthcare-gov/.*

SECTION-BY-SECTION

Section 1. Short title

Designates the short title as the "Safe and Secure Federal Websites Act of 2015."

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

Explains the certification requirement for Federal websites that elicit, collect, store, or maintain personally identifiable information (PII) of individuals. Prohibits an agency (as defined by section 551 of title 5, United States Code) from making a new Federal PII website available to the public until the agency's Chief Information Officer (CIO) certifies to Congress that the website is fully functional and secure.

An agency's CIO must certify to Congress that an existing Federal PII website is fully functional and secure within 90 days of enactment of this law. After the 90-day period, any Federal PII website that has not been certified under these requirements must be rendered inaccessible to the public until certification is submitted.

Makes an exception to the certification requirement when the Federal PII website is in the development or testing phase. The exception only applies if the website meets two conditions: (1) a member of the public cannot access PII-related portions of the website without first acknowledging that he or she understands the risks; and (2) a member of the public is not receiving agency compelled, enjoined, or otherwise provided incentives for accessing PII-related portions of the website.

This section only applies to websites operated by the Federal Government. It does not apply to websites operated by entities independent of the Federal Government, such as a state or locality, even if the independent entity or the website operates on some form of Federal funding.

Defines "personally identifiable information" and "PII" as any information about an individual elicited, collected, stored, or maintained by an agency including the following: (1) 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 (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. Defines "responsible agency" as the agency that is responsible for the operation (whether directly or through contracts with other entities) of the website.

Defines "operational" as a website that elicits, collects, stores, or maintains PII of members of the public and is accessible to the public. Defines "new Federal personally identifiable information website" and "new Federal PII website" as a website that is (1) operated by (or under contract with) a Federal agency; (2) operational; and (3) operational on or after October 1, 2012. For a new Federal PII website to be considered "fully functional," the website must be able to fully support the activities for which it is designed or intended, specifically with regard to PII-related functions. To be considered "secure," the new Federal PII website must meet the

following requirements: (1) in compliance with information security provisions of U.S. Code, specifically Subchapter II of Chapter 35 of Title 44; (2) captures PII at the latest possible step in a user input sequence; (3) PII captured or stored through the website has been encrypted, masked, or similarly protected by the agency; (4) agency responsible for website development and operation has taken all reasonable steps to help prevent domain name confusion, including through additional domain registrations; (5) responsible agency takes proper precautions to ensure only trustworthy persons may access PII in connection with the website, number of persons with access to such information is limited to the fewest reasonable individuals, and all personnel who have access to PII in connection with the website have completed a Standard Form 85P and signed a non-disclosure agreement with respect to PII; and (6) responsible agency maintains sufficient personnel to respond in a timely manner to issues relating to the proper functioning and security of the website and sufficient personnel to monitor on an ongoing basis existing and emerging security threats to the website.

Section 3. Privacy breach requirements

Requires 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 PII. The OMB requirements must include, and agencies facing a privacy breach must comply with, the following: (1) agency must notify affected individuals no later than 72 hours after the agency discovers the breach or evidence reasonably indicating such a breach occurred; (2) agency must report the breach to a Federal cybersecurity center as defined by this section; and (3) any additional actions that the Director deems, including data breach analysis, fraud resolution services, identity theft insurance, and credit protection or monitoring services. Requires the Director of OMB to report to Congress annually on agency compliance with the aforementioned policies and procedures.

EXPLANATION OF AMENDMENTS

Congresswoman Robin Kelly (D–IL) offered an amendment that creates an additional requirement for a new federal website to be certified as "secure." This amendment would require the responsible agency to encrypt, mask, or take other actions to protect personally identifiable information related to a website, and limit to the fewest reasonable number the personnel with access to personally identifiable information. The website must meet both requirements before it can be certified as "secure." The Kelly amendment was adopted by voice vote.

COMMITTEE CONSIDERATION

On May 19, 2015, the Committee met in open session and ordered reported favorably the bill, H.R. 451, as amended, by voice vote, a quorum being present.

ROLL CALL VOTES

There were no recorded votes during Full Committee consideration of H.R. 451.

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 ensures the functionality and security of new Federal websites that collect personally identifiable information. 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 or objective of this bill is to ensure the functionality and security of new Federal websites that collect personally identifiable information.

DUPLICATION OF FEDERAL PROGRAMS

No provision of H.R. 451 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 direct the completion of a specific rule making within the meaning of 5 U.S.C. 551. H.R. 451 requires the Director of the Office of Management and Budget to develop policies and procedures for agencies when responding to an information security breach that involves 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

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:

H.R. 451—Safe and Secure Federal Websites Act of 2015

CBO estimates that enacting H.R. 451 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. 451 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 agencies to develop, document, and implement agencywide security programs for sensitive information. The Privacy Act of 1974 governs the collection, use, and dissemination by federal agencies of personal records. OMB's 2007 memorandum on safeguarding against and responding to the breach of personally identifiable information requires all agencies to implement a policy to safeguard such information and to notify affected individuals of a security breach.

Because those laws and policies regarding the security of personally identifiable information and already in place, CBO estimates that the cost of certifying the safety of information collected by fed-

eral websites would be less than $500,000 over the next five years. Enacting H.R. 451 could affect direct spending by some agencies (such as the Tennessee Valley Authority) because they are authorized to use receipts from the sale of goods, fees, and other collections to cover their operating costs. Therefore, pay-as-you-go procedures apply. Because most of those agencies can make adjustments to the amounts collected, CBO estimates that any net changes in direct spending by those agencies would not be significant. Enacting the bill would not affect revenues.

H.R. 451 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, 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 italics 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

Sec.
3501. Purposes.

* * * * * * *

SUBCHAPTER II—INFORMATION SECURITY

* * * * * * *

3559. Privacy breach requirements.

* * * * * * *

SUBCHAPTER II—INFORMATION SECURITY

* * * * * * *

§ 3559. 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.

* * * * * * *

○