I

115TH CONGRESS
1ST SESSION

H. R. 404

To ensure the functionality and security of new Federal websites that collect personally identifiable information, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JANUARY 10, 2017

Mr. FLEISCHMANN introduced the following bill; which was referred to the Committee on Oversight and Government Reform

---

A BILL

To ensure the functionality and security of new Federal websites that collect personally identifiable information, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Safe and Secure Federal Websites Act of 2017''.

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 nondisclosure 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.''.

○