

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.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Safe and Secure Fed-
5 eral Websites Act of 2017”.

6 **SEC. 2. ENSURING FUNCTIONALITY AND SECURITY OF NEW**
7 **FEDERAL WEBSITES THAT COLLECT PERSON-**
8 **ALLY IDENTIFIABLE INFORMATION.**

9 (a) CERTIFICATION REQUIREMENT.—

1 (1) IN GENERAL.—Except as otherwise pro-
2 vided under this subsection, an agency may not de-
3 ploy or make available to the public a new Federal
4 PII website until the date on which the chief infor-
5 mation officer of the agency submits a certification
6 to Congress that the website is fully functional and
7 secure.

8 (2) TRANSITION.—In the case of a new Federal
9 PII website that is operational on the date of the en-
10 actment of this Act, paragraph (1) shall not apply
11 until the end of the 90-day period beginning on such
12 date of enactment. If the certification required under
13 paragraph (1) for such website has not been sub-
14 mitted to Congress before the end of such period,
15 the head of the responsible agency shall render the
16 website inaccessible to the public until such certifi-
17 cation is submitted to Congress.

18 (3) EXCEPTION FOR BETA WEBSITE WITH EX-
19 PLICIT PERMISSION.—Paragraph (1) shall not apply
20 to a website (or portion thereof) that is in a develop-
21 ment or testing phase, if the following conditions are
22 met:

23 (A) A member of the public may access
24 PII-related portions of the website only after

1 executing an agreement that acknowledges the
2 risks involved.

3 (B) No agency compelled, enjoined, or oth-
4 erwise provided incentives for such a member to
5 access the website for such purposes.

6 (4) CONSTRUCTION.—Nothing in this section
7 shall be construed as applying to a website that is
8 operated entirely by an entity (such as a State or lo-
9 cality) that is independent of the Federal Govern-
10 ment, regardless of the receipt of funding in support
11 of such website from the Federal Government.

12 (b) DEFINITIONS.—In this section:

13 (1) AGENCY.—The term “agency” has the
14 meaning given that term under section 551 of title
15 5, United States Code.

16 (2) FULLY FUNCTIONAL.—The term “fully
17 functional” means, with respect to a new Federal
18 PII website, that the website can fully support the
19 activities for which it is designed or intended with
20 regard to the eliciting, collection, storage, or mainte-
21 nance of personally identifiable information, includ-
22 ing handling a volume of queries relating to such in-
23 formation commensurate with the purpose for which
24 the website is designed.

1 (3) NEW FEDERAL PERSONALLY IDENTIFIABLE
2 INFORMATION WEBSITE (NEW FEDERAL PII
3 WEBSITE).—The terms “new Federal personally
4 identifiable information website” and “new Federal
5 PII website” mean a website that—

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

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

11 (C) is first made accessible to the public
12 and collects or stores personally identifiable in-
13 formation of individuals, on or after October 1,
14 2012.

15 (4) OPERATIONAL.—The term “operational”
16 means, with respect to a website, that such website
17 elicits, collects, stores, or maintains personally iden-
18 tifiable information of members of the public and is
19 accessible to the public.

20 (5) PERSONALLY IDENTIFIABLE INFORMATION
21 (PII).—The terms “personally identifiable informa-
22 tion” and “PII” mean any information about an in-
23 dividual elicited, collected, stored, or maintained by
24 an agency, including—

1 (A) any information that can be used to
2 distinguish or trace the identity of an indi-
3 vidual, such as a name, a social security num-
4 ber, a date and place of birth, a mother's maid-
5 en name, or biometric records; and

6 (B) any other information that is linked or
7 linkable to an individual, such as medical, edu-
8 cational, financial, and employment informa-
9 tion.

10 (6) RESPONSIBLE AGENCY.—The term “respon-
11 sible agency” means, with respect to a new Federal
12 PII website, the agency that is responsible for the
13 operation (whether directly or through contracts
14 with other entities) of the website.

15 (7) SECURE.—The term “secure” means, with
16 respect to a new Federal PII website, that the fol-
17 lowing requirements are met:

18 (A) The website is in compliance with sub-
19 chapter II of chapter 35 of title 44, United
20 States Code.

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

1 (C) The responsible agency for the website
2 has encrypted, masked, or taken other similar
3 actions to protect personally identifiable infor-
4 mation elicited, collected, stored, or maintained
5 in connection with the website.

6 (D) The responsible agency for the website
7 has taken reasonable efforts to minimize do-
8 main name confusion, including through addi-
9 tional domain registrations.

10 (E) The responsible agency requires all
11 personnel who have access to personally identi-
12 fiable information in connection with the
13 website to have completed a Standard Form
14 85P and signed a nondisclosure agreement with
15 respect to personally identifiable information,
16 and the agency takes proper precautions to en-
17 sure that only the fewest reasonable number of
18 trustworthy persons may access such informa-
19 tion.

20 (F) The responsible agency maintains (ei-
21 ther directly or through contract) sufficient per-
22 sonnel to respond in a timely manner to issues
23 relating to the proper functioning and security
24 of the website, and to monitor on an ongoing

1 basis existing and emerging security threats to
2 the website.

3 (8) STATE.—The term “State” means each
4 State of the United States, the District of Columbia,
5 each territory or possession of the United States,
6 and each federally recognized Indian tribe.

7 **SEC. 3. PRIVACY BREACH REQUIREMENTS.**

8 (a) INFORMATION SECURITY AMENDMENT.—Sub-
9 chapter II of chapter 35 of title 44, United States Code,
10 is amended by adding at the end the following:

11 **“§ 3559. Privacy breach requirements**

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

18 “(1) not later than 72 hours after the agency
19 discovers such a breach, or discovers evidence that
20 reasonably indicates such a breach has occurred, no-
21 tice to the individuals whose personally identifiable
22 information could be compromised as a result of
23 such breach;

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

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

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

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

20 “(d) FEDERAL CYBERSECURITY CENTER DE-
21 FINED.—The term ‘Federal cybersecurity center’ means
22 any of the following:

23 “(1) The Department of Defense Cyber Crime
24 Center.

1 “(2) The Intelligence Community Incident Re-
2 sponse Center.

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

5 “(4) The National Cyber Investigative Joint
6 Task Force.

7 “(5) Central Security Service Threat Oper-
8 ations Center of the National Security Agency.

9 “(6) The United States Computer Emergency
10 Readiness Team.

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

13 “(8) Any center that the Director of the Office
14 of Management and Budget determines is appro-
15 priate to carry out the requirements of this sec-
16 tion.”.

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

“3559. Privacy breach requirements.”.

○