

Union Calendar No.

114TH CONGRESS
1ST SESSION

H. R. 451

[Report No. 114-]

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 21, 2015

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

JUNE --, 2015

Reported with an amendment, committed to the Committee of the Whole House on the State of the Union, and ordered to be printed

[Strike out all after the enacting clause and insert the part printed in italic]

[For text of introduced bill, see copy of bill as introduced on January 21, 2015]

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 Federal*
5 *Websites Act of 2015”.*

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

9 *(a) CERTIFICATION REQUIREMENT.—*

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

16 *(2) TRANSITION.—In the case of a new Federal*
17 *PII website that is operational on the date of the en-*
18 *actment of this Act, paragraph (1) shall not apply*
19 *until the end of the 90-day period beginning on such*
20 *date of enactment. If the certification required under*
21 *paragraph (1) for such website has not been submitted*
22 *to Congress before the end of such period, the head of*
23 *the responsible agency shall render the website inac-*
24 *cessible to the public until such certification is sub-*
25 *mitted to Congress.*

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

6 (A) *A member of the public may access PII-*
7 *related portions of the website only after exe-*
8 *cuting an agreement that acknowledges the risks*
9 *involved.*

10 (B) *No agency compelled, enjoined, or other-*
11 *wise provided incentives for such a member to*
12 *access the website for such purposes.*

13 (4) *CONSTRUCTION.*—Nothing in this section
14 shall be construed as applying to a website that is op-
15 erated entirely by an entity (such as a State or local-
16 ity) that is independent of the Federal Government,
17 regardless of the receipt of funding in support of such
18 website from the Federal Government.

19 (b) *DEFINITIONS.*—In this section:

20 (1) *AGENCY.*—The term “agency” has the mean-
21 ing given that term under section 551 of title 5,
22 United States Code.

23 (2) *FULLY FUNCTIONAL.*—The term “fully func-
24 tional” means, with respect to a new Federal PII
25 website, that the website can fully support the activi-

1 *ties for which it is designed or intended with regard*
2 *to the eliciting, collection, storage, or maintenance of*
3 *personally identifiable information, including han-*
4 *dling a volume of queries relating to such information*
5 *commensurate with the purpose for which the website*
6 *is designed.*

7 (3) *NEW FEDERAL PERSONALLY IDENTIFIABLE*
8 *INFORMATION WEBSITE (NEW FEDERAL PII*
9 *WEBSITE).—The terms “new Federal personally iden-*
10 *tifiable information website” and “new Federal PII*
11 *website” mean a website that—*

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

14 (B) *elicits, collects, stores, or maintains per-*
15 *sonally identifiable information of individuals*
16 *and is accessible to the public; and*

17 (C) *is first made accessible to the public*
18 *and collects or stores personally identifiable in-*
19 *formation of individuals, on or after October 1,*
20 *2012.*

21 (4) *OPERATIONAL.—The term “operational”*
22 *means, with respect to a website, that such website*
23 *elicits, collects, stores, or maintains personally identi-*
24 *fiable information of members of the public and is ac-*
25 *cessible to the public.*

1 (5) *PERSONALLY IDENTIFIABLE INFORMATION*
2 (PII).—*The terms “personally identifiable informa-*
3 *tion” and “PII” mean any information about an in-*
4 *dividual elicited, collected, stored, or maintained by*
5 *an agency, including—*

6 (A) *any information that can be used to*
7 *distinguish or trace the identity of an indi-*
8 *vidual, such as a name, a social security num-*
9 *ber, a date and place of birth, a mother’s maiden*
10 *name, or biometric records; and*

11 (B) *any other information that is linked or*
12 *linkable to an individual, such as medical, edu-*
13 *cational, financial, and employment informa-*
14 *tion.*

15 (6) *RESPONSIBLE AGENCY.*—*The term “respon-*
16 *sible agency” means, with respect to a new Federal*
17 *PII website, the agency that is responsible for the op-*
18 *eration (whether directly or through contracts with*
19 *other entities) of the website.*

20 (7) *SECURE.*—*The term “secure” means, with re-*
21 *spect to a new Federal PII website, that the following*
22 *requirements are met:*

23 (A) *The website is in compliance with sub-*
24 *chapter II of chapter 35 of title 44, United*
25 *States Code.*

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

6 (C) The responsible agency for the website
7 has encrypted, masked, or taken other similar
8 actions to protect personally identifiable infor-
9 mation elicited, collected, stored, or maintained
10 in connection with the website.

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

15 (E) The responsible agency requires all per-
16 sonnel who have access to personally identifiable
17 information in connection with the website to
18 have completed a Standard Form 85P and
19 signed a non-disclosure agreement with respect to
20 personally identifiable information, and the
21 agency takes proper precautions to ensure that
22 only the fewest reasonable number of trustworthy
23 persons may access such information.

24 (F) The responsible agency maintains (ei-
25 ther directly or through contract) sufficient per-

1 sonnel to respond in a timely manner to issues
2 relating to the proper functioning and security
3 of the website, and to monitor on an ongoing
4 basis existing and emerging security threats to
5 the website.

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

10 **SEC. 3. PRIVACY BREACH REQUIREMENTS.**

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

14 **“§ 3559. Privacy breach requirements**

15 “(a) *POLICIES AND PROCEDURES*.—The Director of
16 the Office of Management and Budget shall establish and
17 oversee policies and procedures for agencies to follow in the
18 event of a breach of information security involving the dis-
19 closure of personally identifiable information, including re-
20 quirements for—

21 “(1) not later than 72 hours after the agency dis-
22 covers such a breach, or discovers evidence that rea-
23 sonably indicates such a breach has occurred, notice
24 to the individuals whose personally identifiable infor-

1 *mation could be compromised as a result of such*
2 *breach;*

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

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

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

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

22 *“(d) FEDERAL CYBERSECURITY CENTER DEFINED.—*
23 *The term ‘Federal cybersecurity center’ means any of the*
24 *following:*

1 “(1) *The Department of Defense Cyber Crime*
2 *Center.*

3 “(2) *The Intelligence Community Incident Re-*
4 *sponse Center.*

5 “(3) *The United States Cyber Command Joint*
6 *Operations Center.*

7 “(4) *The National Cyber Investigative Joint*
8 *Task Force.*

9 “(5) *Central Security Service Threat Operations*
10 *Center of the National Security Agency.*

11 “(6) *The United States Computer Emergency*
12 *Readiness Team.*

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

15 “(8) *Any center that the Director of the Office of*
16 *Management and Budget determines is appropriate to*
17 *carry out the requirements of this section.”.*

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

“3559. Privacy breach requirements.”.