

113TH CONGRESS
2^D SESSION

H. R. 3635

IN THE SENATE OF THE UNITED STATES

JULY 29, 2014

Received; read twice and referred to the Committee on Homeland Security and
Governmental Affairs

AN ACT

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,*

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “Safe and Secure Fed-
3 eral Websites Act of 2014”.

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

7 (a) **CERTIFICATION REQUIREMENT.—**

8 (1) **IN GENERAL.—**Except as otherwise pro-
9 vided under this subsection, an agency may not de-
10 ploy or make available to the public a new Federal
11 PII website until the date on which the chief infor-
12 mation officer of the agency submits a certification
13 to Congress that the website is fully functional and
14 secure.

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

25 (3) **EXCEPTION FOR BETA WEBSITE WITH EX-**
26 **PLICIT PERMISSION.—**Paragraph (1) shall not apply

1 to a website (or portion thereof) that is in a develop-
2 ment or testing phase, if the following conditions are
3 met:

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

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

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

17 (b) DEFINITIONS.—In this section:

18 (1) AGENCY.—The term “agency” has the
19 meaning given that term under section 551 of title
20 5, United States Code.

21 (2) FULLY FUNCTIONAL.—The term “fully
22 functional” means, with respect to a new Federal
23 PII website, that the website can fully support the
24 activities for which it is designed or intended with
25 regard to the eliciting, collection, storage, or mainte-

1 nance of personally identifiable information, includ-
2 ing handling a volume of queries relating to such in-
3 formation commensurate with the purpose for which
4 the website is designed.

5 (3) NEW FEDERAL PERSONALLY IDENTIFIABLE
6 INFORMATION WEBSITE (NEW FEDERAL PII
7 WEBSITE).—The terms “new Federal personally
8 identifiable information website” and “new Federal
9 PII website” mean a website that—

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

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

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

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

24 (5) PERSONALLY IDENTIFIABLE INFORMATION
25 (PII).—The terms “personally identifiable informa-

1 tion” and “PII” mean any information about an in-
2 dividual elicited, collected, stored, or maintained by
3 an agency, including—

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

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

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

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

21 (A) The website is in compliance with sub-
22 chapter III of chapter 35 of title 44, United
23 States Code.

24 (B) The website ensures that personally
25 identifiable information elicited, collected,

1 stored, or maintained in connection with the
2 website is captured at the latest possible step in
3 a user input sequence.

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

8 (D) The responsible agency requires all
9 personnel who have access to personally identi-
10 fiable information in connection with the
11 website to have completed a Standard Form
12 85P and signed a non-disclosure agreement
13 with respect to personally identifiable informa-
14 tion, and the agency takes proper precautions
15 to ensure only trustworthy persons may access
16 such information.

17 (E) The responsible agency maintains (ei-
18 ther directly or through contract) sufficient per-
19 sonnel to respond in a timely manner to issues
20 relating to the proper functioning and security
21 of the website, and to monitor on an ongoing
22 basis existing and emerging security threats to
23 the website.

24 (8) STATE.—The term “State” means each
25 State of the United States, the District of Columbia,

1 each territory or possession of the United States,
2 and each federally recognized Indian tribe.

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

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

7 **“§ 3550. Privacy breach requirements**

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

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

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

23 “(3) any additional actions that the Director
24 finds necessary and appropriate, including data
25 breach analysis, fraud resolution services, identity

1 theft insurance, and credit protection or monitoring
2 services.

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

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

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

17 “(1) The Department of Defense Cyber Crime
18 Center.

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

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

23 “(4) The National Cyber Investigative Joint
24 Task Force.

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

3 “(6) The United States Computer Emergency
4 Readiness Team.

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

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

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

“3550. Privacy breach requirements.”.

Passed the House of Representatives July 28, 2014.

Attest:

KAREN L. HAAS,

Clerk.