

Union Calendar No. 417

110TH CONGRESS
2^D SESSION

H. R. 4791

[Report No. 110-664]

To amend title 44, United States Code, to strengthen requirements for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

DECEMBER 18, 2007

Mr. CLAY (for himself, Mr. TOWNS, and Mr. WAXMAN) introduced the following bill; which was referred to the Committee on Oversight and Government Reform

MAY 21, 2008

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 *italie*]

[For text of introduced bill, see copy of bill as introduced on December 18, 2007]

A BILL

To amend title 44, United States Code, to strengthen requirements for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets, 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; TABLE OF CONTENTS.**

2 (a) *SHORT TITLE.*—*This Act may be cited as the*
 3 *“Federal Agency Data Protection Act”.*

4 (b) *TABLE OF CONTENTS.*—*The table of contents of this*
 5 *Act is as follows:*

Sec. 1. Short title; table of contents.

Sec. 2. Purpose.

Sec. 3. Definitions.

Sec. 4. Authority of Director of Office of Management and Budget to establish in-
formation security policies and procedures.

Sec. 5. Responsibilities of Federal agencies for information security.

Sec. 6. Federal agency data breach notification requirements.

Sec. 7. Protection of government computers from risks of peer-to-peer file sharing.

Sec. 8. Annual independent audit.

Sec. 9. Best practices for privacy impact assessments.

Sec. 10. Implementation.

6 **SEC. 2. PURPOSE.**

7 *The purpose of this Act is to protect personally identi-*
 8 *fiable information of individuals that is maintained in or*
 9 *transmitted by Federal agency information systems.*

10 **SEC. 3. DEFINITIONS.**

11 (a) *PERSONALLY IDENTIFIABLE INFORMATION AND*
 12 *MOBILE DIGITAL DEVICE DEFINITIONS.*—*Section 3542(b)*
 13 *of title 44, United States Code, is amended by adding at*
 14 *the end the following new paragraphs:*

15 “(4) *The term ‘personally identifiable informa-*
 16 *tion’, with respect to an individual, means any infor-*
 17 *mation about the individual maintained by an agen-*
 18 *cy, including information—*

1 “(A) about the individual’s education, fi-
2 nances, or medical, criminal, or employment his-
3 tory;

4 “(B) that can be used to distinguish or
5 trace the individual’s identity, including name,
6 social security number, date and place of birth,
7 mother’s maiden name, or biometric records; or

8 “(C) that is otherwise linked or linkable to
9 the individual.

10 “(5) The term ‘mobile digital device’ includes
11 any device that can store or process information elec-
12 tronically and is designed to be used in a manner not
13 limited to a fixed location, including—

14 “(A) processing devices such as laptop com-
15 puters, communication devices, and other hand-
16 held computing devices; and

17 “(B) storage devices such as portable hard
18 drives, CD-ROMs, DVDs, and other portable
19 electronic media.”.

20 (b) CONFORMING AMENDMENTS.—Section 208 of the
21 E-Government Act of 2002 (Public Law 107–347; 44 U.S.C.
22 3501 note) is amended—

23 (1) in subsection (b)(1)(A)—

1 (A) in clause (i), by striking “information
2 that is in an identifiable form” and inserting
3 “personally identifiable information”; and

4 (B) in clause (ii)(II), by striking “informa-
5 tion in an identifiable form permitting the phys-
6 ical or online contacting of a specific indi-
7 vidual” and inserting “personally identifiable
8 information”;

9 (2) in subsection (b)(2)(B)(i), by striking “infor-
10 mation that is in an identifiable form” and inserting
11 “personally identifiable information”;

12 (3) in subsection (b)(3)(C), by striking “informa-
13 tion that is in an identifiable form” and inserting
14 “personally identifiable information”; and

15 (4) in subsection (d), by striking the text and in-
16 serting “In this section, the term ‘personally identifi-
17 able information’ has the meaning given that term in
18 section 3542(b)(4) of title 44, United States Code.”.

19 **SEC. 4. AUTHORITY OF DIRECTOR OF OFFICE OF MANAGE-**
20 **MENT AND BUDGET TO ESTABLISH INFORMA-**
21 **TION SECURITY POLICIES AND PROCEDURES.**

22 Section 3543(a) of title 44, United States Code, is
23 amended—

24 (1) by inserting before the semicolon at the end
25 of paragraph (5) the following: “, including plans

1 *and schedules, developed by the agency on the basis of*
2 *priorities for addressing levels of identified risk, for*
3 *conducting—*

4 *“(A) testing and evaluation, as required*
5 *under section 3544(b)(5); and*

6 *“(B) remedial action, as required under sec-*
7 *tion 3544(b)(6), to address deficiencies identified*
8 *by such testing and evaluation”;* and

9 *(2) by adding at the end the following:*

10 *“(9) establishing minimum requirements regard-*
11 *ing the protection of personally identifiable informa-*
12 *tion maintained in or transmitted by mobile digital*
13 *devices, including requirements for the use of tech-*
14 *nologies that efficiently and effectively render infor-*
15 *mation unusable by unauthorized persons;*

16 *“(10) requiring agencies to comply with—*

17 *“(A) minimally acceptable system configu-*
18 *ration requirements consistent with best prac-*
19 *tices, including checklists developed under section*
20 *8(c) of the Cyber Security Research and Develop-*
21 *ment Act (Public Law 107–305; 116 Stat. 2378)*
22 *by the Director of the National Institute of*
23 *Standards and Technology; and*

1 “(B) minimally acceptable requirements for
2 periodic testing and evaluation of the implemen-
3 tation of such configuration requirements;

4 “(11) ensuring that agency contracts for (or in-
5 volving or including) the provision of information
6 technology products or services include requirements
7 for contractors to meet minimally acceptable configu-
8 ration requirements, as required under paragraph
9 (10);

10 “(12) ensuring the establishment through regula-
11 tion and guidance of contract requirements to ensure
12 compliance with this subchapter with regard to pro-
13 viding information security for information and in-
14 formation systems used or operated by a contractor of
15 an agency or other organization on behalf of the agen-
16 cy; and”.

17 **SEC. 5. RESPONSIBILITIES OF FEDERAL AGENCIES FOR IN-**
18 **FORMATION SECURITY.**

19 Section 3544(b) of title 44, United States Code, is
20 amended—

21 (1) in paragraph (2)(D)(iii), by striking “as de-
22 termined by the agency” and inserting “as required
23 by the Director under section 3543(a)(10)”;

24 (2) in paragraph (5)—

1 (A) by inserting after “annually” the fol-
2 lowing: “and as approved by the Director”;

3 (B) by striking “and” at the end of sub-
4 paragraph (A);

5 (C) by redesignating subparagraph (B) as
6 subparagraph (D); and

7 (D) by inserting after subparagraph (A) the
8 following:

9 “(B) shall include testing and evaluation of
10 system configuration requirements as required
11 under section 3543(a)(10);

12 “(C) shall include testing of systems oper-
13 ated by a contractor of the agency or other orga-
14 nization on behalf of the agency, which testing
15 requirement may be satisfied by independent
16 testing, evaluation, or audit of such systems;
17 and”;

18 (3) by striking “and” at the end of paragraph
19 (7);

20 (4) by striking the period at the end of para-
21 graph (8) and inserting a semicolon; and

22 (5) by adding at the end the following:

23 “(9) plans and procedures for ensuring the ade-
24 quacy of information security protections for systems

1 *maintaining or transmitting personally identifiable*
2 *information, including requirements for—*

3 *“(A) maintaining a current inventory of*
4 *systems maintaining or transmitting such infor-*
5 *mation;*

6 *“(B) implementing information security re-*
7 *quirements for mobile digital devices maintain-*
8 *ing or transmitting such information, as re-*
9 *quired by the Director (including the use of tech-*
10 *nologies rendering data unusable by unauthor-*
11 *ized persons); and*

12 *“(C) developing, implementing, and over-*
13 *seeing remediation plans to address*
14 *vulnerabilities in information security protec-*
15 *tions for such information;”.*

16 **SEC. 6. FEDERAL AGENCY DATA BREACH NOTIFICATION RE-**
17 **QUIREMENTS.**

18 *(a) AUTHORITY OF DIRECTOR OF OFFICE OF MANAGE-*
19 *MENT AND BUDGET TO ESTABLISH DATA BREACH POLI-*
20 *CIES.—Section 3543(a) of title 44, United States Code, as*
21 *amended by section 4, is further amended—*

22 *(1) by striking “and” at the end of paragraph*
23 *(7);*

24 *(2) in paragraph (8)—*

1 (A) by striking “and” at the end of sub-
2 paragraph (D);

3 (B) by striking the period and inserting “;
4 and” at the end of subparagraph (E); and

5 (C) by adding at the end the following new
6 subparagraph:

7 “(F) a summary of the breaches of informa-
8 tion security reported by agencies to the Director
9 and the Federal information security incident
10 center pursuant to paragraph (13);”;

11 (3) by adding at the end the following:

12 “(13) establishing policies, procedures, and
13 standards for agencies to follow in the event of a
14 breach of data security involving the disclosure of per-
15 sonally identifiable information, specifically includ-
16 ing—

17 “(A) a requirement for timely notice to be
18 provided to those individuals whose personally
19 identifiable information could be compromised as
20 a result of such breach, except no notice shall be
21 required if the breach does not create a reason-
22 able risk—

23 “(i) of identity theft, fraud, or other
24 unlawful conduct regarding such indi-
25 vidual; or

1 “(i) of other harm to the individual;

2 “(B) guidance on determining how timely
3 notice is to be provided;

4 “(C) guidance regarding whether additional
5 special actions are necessary and appropriate,
6 including data breach analysis, fraud resolution
7 services, identify theft insurance, and credit pro-
8 tection or monitoring services; and

9 “(D) a requirement for timely reporting by
10 the agencies of such breaches to the Director and
11 Federal information security center.”.

12 (b) *AUTHORITY OF CHIEF INFORMATION OFFICER TO*
13 *DEVELOP AND MAINTAIN INVENTORIES.*—Section
14 3544(a)(3) of title 44, United States Code, is amended—

15 (1) by inserting after “authority to ensure com-
16 pliance with” the following: “and, to the extent deter-
17 mined necessary and explicitly authorized by the head
18 of the agency, to enforce”;

19 (2) by striking “and” at the end of subpara-
20 graph (D);

21 (3) by inserting “and” at the end of subpara-
22 graph (E); and

23 (4) by adding at the end the following:

24 “(F) developing and maintaining an inven-
25 tory of all personal computers, laptops, or any

1 *other hardware containing personally identifi-*
2 *able information;”.*

3 (c) *INCLUSION OF DATA BREACH NOTIFICATION.*—
4 *Section 3544(b) of title 44, United States Code, as amended*
5 *by section 5, is further amended by adding at the end the*
6 *following:*

7 “(10) *procedures for notifying individuals whose*
8 *personally identifiable information may have been*
9 *compromised or accessed following a breach of infor-*
10 *mation security; and*

11 “(11) *procedures for timely reporting of informa-*
12 *tion security breaches involving personally identifi-*
13 *able information to the Director and the Federal in-*
14 *formation security incident center.”.*

15 (d) *AUTHORITY OF AGENCY CHIEF HUMAN CAPITAL*
16 *OFFICERS TO ASSESS FEDERAL PERSONAL PROPERTY.*—
17 *Section 1402(a) of title 5, United States Code, is amend-*
18 *ed—*

19 (1) *by striking “, and” at the end of paragraph*
20 (5) *and inserting a semicolon;*

21 (2) *by striking the period and inserting “; and”*
22 *at the end of paragraph (6); and*

23 (3) *by adding at the end the following:*

24 “(7) *prescribing policies and procedures for exit*
25 *interviews of employees, including a full accounting*

1 of all Federal personal property that was assigned to
2 the employee during the course of employment.”.

3 **SEC. 7. PROTECTION OF GOVERNMENT COMPUTERS FROM**
4 **RISKS OF PEER-TO-PEER FILE SHARING.**

5 (a) *PLANS REQUIRED.*—As part of the Federal agency
6 responsibilities set forth in sections 3544 and 3545 of title
7 44, United States Code, the head of each agency shall de-
8 velop and implement a plan to ensure the security and pri-
9 vacy of information collected or maintained by or on behalf
10 of the agency from the risks posed by certain peer-to-peer
11 file sharing programs.

12 (b) *CONTENTS OF PLANS.*—Such plans shall set forth
13 appropriate methods, including both technological (such as
14 the use of software and hardware) and nontechnological
15 methods (such as employee policies and user training), to
16 achieve the goal of securing and protecting such information
17 from the risks posed by peer-to-peer file sharing programs.

18 (c) *IMPLEMENTATION OF PLANS.*—The head of each
19 agency shall—

20 (1) develop and implement the plan required
21 under this section as expeditiously as possible, but in
22 no event later than six months after the date of the
23 enactment of this Act; and

24 (2) review and revise the plan periodically as
25 necessary.

1 (d) *REVIEW OF PLANS.*—Not later than 18 months
2 after the date of the enactment of this Act, the Comptroller
3 General shall—

4 (1) review the adequacy of the agency plans re-
5 quired by this section; and

6 (2) submit to the Committee on Oversight and
7 Government Reform of the House of Representatives
8 and the Committee on Homeland Security and Gov-
9 ernmental Affairs of the Senate a report on the results
10 of the review, together with any recommendations the
11 Comptroller General considers appropriate.

12 (e) *DEFINITIONS.*—In this section:

13 (1) *PEER-TO-PEER FILE SHARING PROGRAM.*—
14 The term “peer-to-peer file sharing program” means
15 computer software that allows the computer on which
16 such software is installed (A) to designate files avail-
17 able for transmission to another such computer, (B)
18 to transmit files directly to another such computer,
19 and (C) to request the transmission of files from an-
20 other such computer. The term does not include the
21 use of such software for file sharing between, among,
22 or within Federal, State, or local government agencies
23 in order to perform official agency business.

1 (2) *AGENCY.*—*The term “agency” has the mean-*
2 *ing provided by section 3502 of title 44, United*
3 *States Code.*

4 **SEC. 8. ANNUAL INDEPENDENT AUDIT.**

5 (a) *REQUIREMENT FOR AUDIT INSTEAD OF EVALUA-*
6 *TION.*—*Section 3545 of title 44, United States Code, is*
7 *amended—*

8 (1) *in the section heading, by striking “evalua-*
9 *tion” and inserting “audit” ; and*

10 (2) *in paragraphs (1) and (2) of subsection (a),*
11 *by striking “evaluation” and inserting “audit” both*
12 *places it appears.*

13 (b) *ADDITIONAL SPECIFIC REQUIREMENTS FOR AU-*
14 *DITS.*—*Section 3545(a) of such title is amended—*

15 (1) *in paragraph (2)—*

16 (A) *in subparagraph (A), by striking “sub-*
17 *set of the agency’s information systems;” and in-*
18 *serting the following: “subset of—*

19 (i) *the information systems used or oper-*
20 *ated by the agency; and*

21 (ii) *the information systems used, oper-*
22 *ated, or supported on behalf of the agency by a*
23 *contractor of the agency, any subcontractor (at*
24 *any tier) of such a contractor, or any other enti-*
25 *ty;”;*

1 (B) in subparagraph (B), by striking “and”
2 at the end;

3 (C) in subparagraph (C), by striking the
4 period and inserting “; and”; and

5 (D) by adding at the end the following new
6 subparagraph:

7 “(D) a conclusion whether the agency’s informa-
8 tion security controls are effective, including an iden-
9 tification of any significant deficiencies in such con-
10 trols.”; and

11 (2) by adding at the end the following new para-
12 graph:

13 “(3) Each audit under this section shall conform to
14 generally accepted government auditing standards.”.

15 (c) CONFORMING AMENDMENTS.—

16 (1) Each of the following provisions of section
17 3545 of title 44, United States Code, is amended by
18 striking “evaluation” and inserting “audit” each
19 place it appears:

20 (A) Subsection (b)(1).

21 (B) Subsection (b)(2).

22 (C) Subsection (c).

23 (D) Subsection (e)(1).

24 (E) Subsection (e)(2).

1 “(D) develop best practices for agencies to
2 follow in conducting privacy impact assess-
3 ments.”.

4 **SEC. 10. IMPLEMENTATION.**

5 *Except as otherwise specifically provided in this Act,*
6 *implementation of this Act and the amendments made by*
7 *this Act shall begin not later than 90 days after the date*
8 *of the enactment of this Act.*

Union Calendar No. 417

110TH CONGRESS
2^D SESSION

H. R. 4791

[Report No. 110-664]

A BILL

To amend title 44, United States Code, to strengthen requirements for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets, and for other purposes.

MAY 21, 2008

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