

110TH CONGRESS
1ST SESSION

H. R. 4791

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

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,*

3 **SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

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

6 (b) TABLE OF CONTENTS.—The table of contents of
7 this Act is as follows:

- Sec. 1. Short title; table of contents.
 Sec. 2. Purpose.
 Sec. 3. Definition of personally identifiable information.
 Sec. 4. Authority of Director of Office of Management and Budget to establish information security policies and procedures.
 Sec. 5. Responsibilities of Federal agencies for information security.
 Sec. 6. Protection of government computers from risks of peer-to-peer file sharing.
 Sec. 7. Annual independent audit.
 Sec. 8. Privacy impact assessment of Federal agency use of commercial information services containing personal information.
 Sec. 9. Prohibition on certain contracts with data brokers.
 Sec. 10. Authorization of appropriations.
 Sec. 11. Implementation.

1 **SEC. 2. PURPOSE.**

2 The purpose of this Act is to protect personally iden-
 3 tifiable information of individuals that is maintained in or
 4 transmitted by Federal agency information systems.

5 **SEC. 3. DEFINITION OF PERSONALLY IDENTIFIABLE INFOR-**
 6 **MATION.**

7 Section 3542(b) of title 44, United States Code, is
 8 amended by adding at the end the following new para-
 9 graph:

10 “(4) The term ‘personally identifiable informa-
 11 tion’, with respect to an individual, means any infor-
 12 mation about the individual maintained by an agen-
 13 cy, including information—

14 “(A) about the individual’s education, fi-
 15 nances, or medical, criminal, or employment
 16 history;

17 “(B) that can be used to distinguish or
 18 trace the individual’s identity, including name,

1 social security number, date and place of birth,
2 mother's maiden name, or biometric records; or
3 "(C) that is linked or linkable to the indi-
4 vidual."

5 **SEC. 4. AUTHORITY OF DIRECTOR OF OFFICE OF MANAGE-**
6 **MENT AND BUDGET TO ESTABLISH INFORMA-**
7 **TION SECURITY POLICIES AND PROCEDURES.**

8 Section 3543(a) of title 44, United States Code, is
9 amended—

10 (1) by striking "and" at the end of paragraph
11 (7);

12 (2) in paragraph (8)—

13 (A) by striking "and" at the end of sub-
14 paragraph (D);

15 (B) by striking the period and inserting ";
16 and" at the end of subparagraph (E); and

17 (C) by adding at the end the following new
18 subparagraph:

19 "(F) a summary of the breaches of infor-
20 mation security reported by agencies to the Di-
21 rector and the Federal information security in-
22 cident center pursuant to paragraph (10);"; and
23 (3) by adding at the end the following:

1 “(9) establishing minimum requirements re-
2 garding the protection of information maintained in
3 or transmitted by mobile digital devices, including—

4 “(A) requirements for the protection of
5 personally identifiable information; and

6 “(B) requirements for—

7 “(i) the encryption of such informa-
8 tion consistent with standards promulgated
9 under section 11331 of title 40; or

10 “(ii) the use of other commercially
11 available technologies that efficiently and
12 effectively render information unusable by
13 unauthorized persons;

14 “(10) establishing minimum requirements re-
15 garding agency action following a breach of informa-
16 tion security resulting in the disclosure of personally
17 identifiable information, including requirements
18 for—

19 “(A) timely agency reporting of such
20 breach to the Director and the Federal informa-
21 tion security incident center required under sec-
22 tion 3546; and

23 “(B) timely agency notification to individ-
24 uals whose personally identifiable information
25 may have been compromised or accessed during

1 such breach, based on government-wide risk
2 categories established by the Director after con-
3 sultation with agencies and the public that in-
4 clude exemptions from notification requirements
5 where such information can be reasonably de-
6 termined to be unusable by unauthorized per-
7 sons; and

8 “(11) requiring agencies to comply with mini-
9 mally acceptable system configuration requirements
10 consistent with best practices, including checklists
11 developed under section 8(e) of the Cyber Security
12 Research and Development Act (Public Law 107–
13 305; 116 Stat. 2378) by the Director of the Na-
14 tional Institute of Standards and Technology.”.

15 **SEC. 5. RESPONSIBILITIES OF FEDERAL AGENCIES FOR IN-**
16 **FORMATION SECURITY.**

17 Section 3544(b) of title 44, United States Code, is
18 amended—

19 (1) in paragraph (2)(D)(iii), by striking “as de-
20 termined by the agency” and inserting “as required
21 by the Director under section 3543(a)(11)”;

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

24 (3) by striking the period at the end of para-
25 graph (8) and inserting “; and”; and

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

2 “(9) plans and procedures for ensuring the ade-
3 quacy of information security protections for sys-
4 tems maintaining or transmitting personally identifi-
5 able information, including requirements for—

6 “(A) maintaining a current inventory of
7 systems maintaining or transmitting such infor-
8 mation;

9 “(B) implementing information security re-
10 quirements for mobile digital devices maintain-
11 ing or transmitting such information, as re-
12 quired by the Director (including encryption or
13 the use of other commercially available tech-
14 nologies rendering data unusable by unauthor-
15 ized persons);

16 “(C) timely reporting of information secu-
17 rity breaches involving such information to the
18 Director and the Federal information security
19 incident center required under section 3546;

20 “(D) timely notification to individuals
21 whose personally identifiable information may
22 have been compromised or accessed during an
23 information security breach, consistent with
24 policies and procedures issued by the Director;
25 and

1 “(E) developing, implementing, and over-
2 seeing remediation plans to address
3 vulnerabilities in information security protec-
4 tions for such information.”.

5 **SEC. 6. PROTECTION OF GOVERNMENT COMPUTERS FROM**
6 **RISKS OF PEER-TO-PEER FILE SHARING.**

7 (a) **PLANS REQUIRED.**—As part of the Federal agen-
8 cy responsibilities set forth in sections 3544 and 3545 of
9 title 44, United States Code, the head of each agency shall
10 develop and implement a plan to protect the security and
11 privacy of computers and networks of the Federal Govern-
12 ment from the risks posed by peer-to-peer file sharing.

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

20 (c) **IMPLEMENTATION OF PLANS.**—The head of each
21 agency shall—

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

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

3 (d) REVIEW OF PLANS.—Not later than 18 months
4 after the date of the enactment of this Act, the Comp-
5 troller General shall—

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

8 (2) submit to the Committee on Government
9 Reform of the House of Representatives and the
10 Committee on Governmental Affairs of the Senate a
11 report on the results of the review, together with any
12 recommendations the Comptroller General considers
13 appropriate.

14 (e) DEFINITIONS.—In this section:

15 (1) PEER-TO-PEER FILE SHARING.—The term
16 “peer-to-peer file sharing” means the use of com-
17 puter software, other than computer and network
18 operating systems, that has as its primary function
19 the capability to allow the computer on which such
20 software is used to designate files available for
21 transmission to another computer using such soft-
22 ware, to transmit files directly to another such com-
23 puter, and to request the transmission of files from
24 another such computer. The term does not include
25 the use of such software for file sharing between,

1 among, or within Federal, State, or local government
2 agencies.

3 (2) AGENCY.—The term “agency” has the
4 meaning provided by section 3502 of title 44, United
5 States Code.

6 **SEC. 7. ANNUAL INDEPENDENT AUDIT.**

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

10 (1) in the section heading, by striking “**eval-**
11 **uation**” and inserting “**audit**” ; and

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

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

17 (1) in paragraph (2)(A), by striking “subset of
18 the agency’s information systems;” and inserting the
19 following: “subset of—

20 “(i) the information systems used or
21 operated by the agency; and

22 “(ii) the information systems used,
23 operated, or supported on behalf of the
24 agency by a contractor of the agency, any

1 subcontractor (at any tier) of such a con-
2 tractor, or any other entity;” and

3 (2) by adding at the end the following new
4 paragraph:

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

7 (c) CONFORMING AMENDMENTS.—

8 (1) Each of the following provisions of section
9 3545 of title 44, United States Code, is amended by
10 striking “evaluation” and inserting “audit” each
11 place it appears:

12 (A) Subsection (b)(1).

13 (B) Subsection (b)(2).

14 (C) Subsection (c).

15 (D) Subsection (e)(1).

16 (E) Subsection (e)(2).

17 (2) Section 3545(d) of such title is amended by
18 striking “the evaluation required by this section”
19 and inserting “the audit required by this section”.

20 (3) Section 3545(f) of such title is amended by
21 striking “evaluators” and inserting “auditors”.

22 (4) Section 3545(g)(1) of such title is amended
23 by striking “evaluations” and inserting “audits”.

24 (5) Section 3545(g)(3) of such title is amended
25 by striking “Evaluations” and inserting “Audits”.

1 (6) Section 3543(a)(8)(A) of such title is
2 amended by striking “evaluations” and inserting
3 “audits”.

4 (7) Section 3544(b)(5)(B) of such title is
5 amended by striking “evaluation” and inserting
6 “audit”.

7 **SEC. 8. PRIVACY IMPACT ASSESSMENT OF FEDERAL AGEN-**
8 **CY USE OF COMMERCIAL INFORMATION**
9 **SERVICES CONTAINING PERSONAL INFORMA-**
10 **TION.**

11 (a) IN GENERAL.—Section 208(b)(1)(A) of the E-
12 Government Act of 2002 (44 U.S.C. 3501 note) is amend-
13 ed—

14 (1) by striking “or” at the end of clause (i);
15 and

16 (2) in clause (ii), by striking the period at the
17 end of subclause (II) and inserting “; or”; and

18 (3) by inserting after clause (ii) the following:

19 “(iii) purchasing or subscribing for a
20 fee to information in identifiable form from
21 a data broker.”.

22 (b) DEFINITIONS.—Section 208(d) of such Act (44
23 U.S.C. 3501 note) is amended to read as follows:

24 “(d) DEFINITIONS.—In this section:

1 (1) by redesignating subsection (d) as sub-
2 section (e); and

3 (2) by inserting after subsection (c) the fol-
4 lowing:

5 “(d) PROHIBITION ON CERTAIN CONTRACTS WITH
6 DATA BROKERS.—

7 “(1) PROHIBITION.—Notwithstanding any other
8 provision of law, beginning 1 year after the date of
9 the enactment of this subsection, no Federal agency
10 may enter into a contract with a data broker, or
11 issue a task or delivery order under a contract with
12 a data broker, to access for a fee any database con-
13 sisting primarily of information in identifiable form
14 concerning United States persons (other than a
15 database consisting of news reporting or telephone
16 directories) unless the head of such agency imple-
17 ments the requirements specified in paragraph (2).

18 “(2) REQUIREMENTS.—For purposes of para-
19 graph (1), the requirements specified in this para-
20 graph are the following:

21 “(A) COMPLETION OF PRIVACY IMPACT AS-
22 SESSMENT.—With respect to any database pro-
23 posed to be accessed, the head of the agency
24 shall complete a privacy impact assessment
25 under this section. The assessment shall, sub-

1 ject to the provisions in this section pertaining
2 to sensitive information, include a description
3 of—

4 “(i) such database;

5 “(ii) the name of the data broker
6 from which it is proposed to be obtained;
7 and

8 “(iii) the amount of the contract or
9 task or delivery order proposed to be en-
10 tered into or issued.

11 “(B) PROMULGATION OF REGULATIONS.—

12 The head of the agency shall promulgate regu-
13 lations that specify—

14 “(i) the personnel permitted to access,
15 analyze, or otherwise use databases of the
16 type described in paragraph (1);

17 “(ii) standards governing the access,
18 analysis, or use of such databases;

19 “(iii) any standards used to ensure
20 that the information in identifiable form
21 accessed, analyzed, or used is the minimum
22 necessary to accomplish the intended legiti-
23 mate purpose of the Federal agency;

1 “(iv) standards limiting the retention
2 and redisclosure of information in identifi-
3 able form obtained from such databases;

4 “(v) procedures ensuring that such
5 data meet standards of accuracy, rel-
6 evance, completeness, and timeliness;

7 “(vi) the auditing and security meas-
8 ures to protect against unauthorized ac-
9 cess, analysis, use, or modification of data
10 in such databases;

11 “(vii) applicable mechanisms by which
12 individuals may secure timely redress for
13 any adverse consequences wrongly incurred
14 due to the access, analysis, or use of such
15 databases;

16 “(viii) mechanisms, if any, for the en-
17 forcement and independent oversight of ex-
18 isting or planned procedures, policies, or
19 guidelines; and

20 “(ix) an outline of enforcement mech-
21 anisms for accountability to protect indi-
22 viduals and the public against unlawful or
23 illegitimate access or use of databases.

24 “(C) INCLUSION OF PENALTIES AND
25 OTHER REQUIREMENTS IN LARGER CON-

1 TRACTS.—With respect to any contract or task
2 or delivery order proposed to be entered into or
3 issued in an amount greater than \$500,000, the
4 head of the agency shall include in the contract
5 or order the following provisions:

6 “(i) Provisions providing for pen-
7 alties—

8 “(I) for failure to implement a
9 comprehensive personal data privacy
10 and security program that includes
11 administrative, technical, and physical
12 safeguards appropriate to the size and
13 complexity of the business entity and
14 the nature and scope of its activities;
15 or

16 “(II) for the provision to the
17 Federal agency of inaccurate informa-
18 tion in identifiable form, if the entity
19 knows or has reason to know that the
20 information being provided is inac-
21 curate.

22 “(ii) Provisions requiring a data
23 broker that retains service providers for re-
24 sponsibilities related to information in
25 identifiable form to—

1 “(I) exercise appropriate due dili-
2 gence in selecting those service pro-
3 viders for responsibilities related to
4 such information;

5 “(II) take reasonable steps to se-
6 lect and retain service providers that
7 are capable of maintaining appro-
8 priate safeguards for the security, pri-
9 vacy, and integrity of such informa-
10 tion; and

11 “(III) require such service pro-
12 viders, by contract, to implement a
13 comprehensive personal data privacy
14 and security program that includes
15 administrative, technical, and physical
16 safeguards appropriate to the size and
17 complexity of the business entity and
18 the nature and scope of its activities.

19 “(3) LIMITATION ON PENALTIES.—The pen-
20 alties under paragraph (2)(C)(i) shall not apply to
21 a data broker providing information in identifiable
22 form that is accurately and completely recorded
23 from a public record source.”.

1 **SEC. 10. AUTHORIZATION OF APPROPRIATIONS.**

2 Section 3548 of title 44, United States Code, is
3 amended by striking “2007” and inserting “2012”.

4 **SEC. 11. 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.

○