110TH CONGRESS
2D SESSION

H. R. 4791

IN THE SENATE OF THE UNITED STATES

JUNE 4, 2008

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

AN ACT

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.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Federal Agency Data Protection Act''.

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

SEC. 2. PURPOSE.

The purpose of this Act is to protect personally identifiable information of individuals that is maintained in or transmitted by Federal agency information systems.

SEC. 3. DEFINITIONS.

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

''(4) The term 'personally identifiable information', with respect to an individual, means any information about the individual maintained by an agency, including information—

''(A) about the individual's education, finances, or medical, criminal, or employment history;

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

''(C) that is otherwise linked or linkable to the individual.

''(5) The term 'mobile digital device' includes any device that can store or process information electronically and is designed to be used in a manner not limited to a fixed location, including—

''(A) processing devices such as laptop computers, communication devices, and other hand-held computing devices; and

''(B) storage devices such as portable hard drives, CD–ROMs, DVDs, and other portable electronic media.''.

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

(1) in subsection (b)(1)(A)—

(A) in clause (i), by striking ''information that is in an identifiable form'' and inserting ''personally identifiable information''; and

(B) in clause (ii)(II), by striking ''information in an identifiable form permitting the physical or online contacting of a specific individual'' and inserting ''personally identifiable information'';

(2) in subsection (b)(2)(B)(i), by striking ''information that is in an identifiable form'' and inserting ''personally identifiable information'';

(3) in subsection (b)(3)(C), by striking ''information that is in an identifiable form'' and inserting ''personally identifiable information''; and

(4) in subsection (d), by striking the text and inserting ''In this section, the term 'personally identifiable information' has the meaning given that term in section 3542(b)(4) of title 44, United States Code.''.

SEC. 4. AUTHORITY OF DIRECTOR OF OFFICE OF MANAGEMENT AND BUDGET TO ESTABLISH INFORMATION SECURITY POLICIES AND PROCEDURES.

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

(1) by inserting before the semicolon at the end of paragraph (5) the following: ‘‘, including plans and schedules, developed by the agency on the basis of priorities for addressing levels of identified risk, for conducting—

‘‘(A) testing and evaluation, as required under section 3544(b)(5); and

‘‘(B) remedial action, as required under section 3544(b)(6), to address deficiencies identified by such testing and evaluation’’; and

(2) by adding at the end the following:

‘‘(9) establishing minimum requirements regarding the protection of personally identifiable information maintained in or transmitted by mobile digital devices, including requirements for the use of technologies that efficiently and effectively render information unusable by unauthorized persons;

‘‘(10) requiring agencies to comply with—

‘‘(A) minimally acceptable system configuration requirements consistent with best practices, including checklists developed under section 8(c) of the Cyber Security Research and Development Act (Public Law 107–305; 116 Stat. 2378) by the Director of the National Institute of Standards and Technology; and

''(B) minimally acceptable requirements for periodic testing and evaluation of the implementation of such configuration requirements;

''(11) ensuring that agency contracts for (or involving or including) the provision of information technology products or services include requirements for contractors to meet minimally acceptable configuration requirements, as required under paragraph (10);

''(12) ensuring the establishment through regulation and guidance of contract requirements to ensure compliance with this subchapter with regard to providing information security for information and information systems used or operated by a contractor of an agency or other organization on behalf of the agency; and''.

SEC. 5. RESPONSIBILITIES OF FEDERAL AGENCIES FOR INFORMATION SECURITY.

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

(1) in paragraph (2)(D)(iii), by striking ''as determined by the agency'' and inserting ''as required by the Director under section 3543(a)(10)'';

(2) in paragraph (5)—

(A) by inserting after ''annually'' the following: ''and as approved by the Director'';

(B) by striking ''and'' at the end of subparagraph (A);

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

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

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

''(C) shall include testing of systems operated by a contractor of the agency or other organization on behalf of the agency, which testing requirement may be satisfied by independent testing, evaluation, or audit of such systems; and'';

(3) by striking ''and'' at the end of paragraph (7);

(4) by striking the period at the end of paragraph (8) and inserting a semicolon; and

(5) by adding at the end the following:

''(9) plans and procedures for ensuring the adequacy of information security protections for sys-

tems maintaining or transmitting personally identifiable information, including requirements for—

''(A) maintaining a current inventory of systems maintaining or transmitting such information;

''(B) implementing information security requirements for mobile digital devices maintaining or transmitting such information, as required by the Director (including the use of technologies rendering data unusable by unauthorized persons); and

''(C) developing, implementing, and overseeing remediation plans to address vulnerabilities in information security protections for such information;''.

SEC. 6. FEDERAL AGENCY DATA BREACH NOTIFICATION REQUIREMENTS.

(a) AUTHORITY OF DIRECTOR OF OFFICE OF MANAGEMENT AND BUDGET TO ESTABLISH DATA BREACH POLICIES.—Section 3543(a) of title 44, United States Code, as amended by section 4, is further amended—

(1) by striking ''and'' at the end of paragraph (7);

(2) in paragraph (8)—

(A) by striking ''and'' at the end of subparagraph (D);

(B) by striking the period and inserting ''; and'' at the end of subparagraph (E); and

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

''(F) a summary of the breaches of information security reported by agencies to the Director and the Federal information security incident center pursuant to paragraph (13);''; and

(3) by adding at the end the following:

''(13) establishing policies, procedures, and standards for agencies to follow in the event of a breach of data security involving the disclosure of personally identifiable information, specifically including—

''(A) a requirement for timely notice to be provided to those individuals whose personally identifiable information could be compromised as a result of such breach, except no notice shall be required if the breach does not create a reasonable risk—

''(i) of identity theft, fraud, or other unlawful conduct regarding such individual; or

''(ii) of other harm to the individual;

''(B) guidance on determining how timely notice is to be provided;

''(C) guidance regarding whether additional special actions are necessary and appropriate, including data breach analysis, fraud resolution services, identify theft insurance, and credit protection or monitoring services; and

''(D) a requirement for timely reporting by the agencies of such breaches to the Director and Federal information security center.''.

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

(1) by inserting after ''authority to ensure compliance with'' the following: ''and, to the extent determined necessary and explicitly authorized by the head of the agency, to enforce'';

(2) by striking ''and'' at the end of subparagraph (D);

(3) by inserting ''and'' at the end of subparagraph (E); and

(4) by adding at the end the following:

''(F) developing and maintaining an inventory of all personal computers, laptops, or any

other hardware containing personally identifiable information;''.

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

''(10) procedures for notifying individuals whose personally identifiable information may have been compromised or accessed following a breach of information security; and

''(11) procedures for timely reporting of information security breaches involving personally identifiable information to the Director and the Federal information security incident center.''.

(d) AUTHORITY OF AGENCY CHIEF HUMAN CAPITAL OFFICERS TO ASSESS FEDERAL PERSONAL PROPERTY.—Section 1402(a) of title 5, United States Code, is amended—

(1) by striking '', and'' at the end of paragraph (5) and inserting a semicolon;

(2) by striking the period and inserting ''; and'' at the end of paragraph (6); and

(3) by adding at the end the following:

''(7) prescribing policies and procedures for exit interviews of employees, including a full accounting

of all Federal personal property that was assigned to the employee during the course of employment.''.

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

(a) PLANS REQUIRED.—As part of the Federal agency responsibilities set forth in sections 3544 and 3545 of title 44, United States Code, the head of each agency shall develop and implement a plan to ensure the security and privacy of information collected or maintained by or on behalf of the agency from the risks posed by certain peer-to-peer file sharing programs.

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

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

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

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

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

(1) review the adequacy of the agency plans required by this section; and

(2) submit to the Committee on Oversight and Government Reform of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the results of the review, together with any recommendations the Comptroller General considers appropriate.

(e) DEFINITIONS.—In this section:

(1) PEER-TO-PEER FILE SHARING PROGRAM.—The term ''peer-to-peer file sharing program'' means computer software that allows the computer on which such software is installed (A) to designate files available for transmission to another such computer, (B) to transmit files directly to another such computer, and (C) to request the transmission of files from another such computer. The term does not include the use of such software for file sharing between, among, or within Federal, State, or local gov-

ernment agencies in order to perform official agency business.

(2) AGENCY.—The term ''agency'' has the meaning provided by section 3502 of title 44, United States Code.

SEC. 8. ANNUAL INDEPENDENT AUDIT.

(a) REQUIREMENT FOR AUDIT INSTEAD OF EVALUATION.—Section 3545 of title 44, United States Code, is amended—

(1) in the section heading, by striking ''**evaluation**'' and inserting ''**audit**'' ; and

(2) in paragraphs (1) and (2) of subsection (a), by striking ''evaluation'' and inserting ''audit'' both places it appears.

(b) ADDITIONAL SPECIFIC REQUIREMENTS FOR AUDITS.—Section 3545(a) of such title is amended—

(1) in paragraph (2)—

(A) in subparagraph (A), by striking ''subset of the agency's information systems;'' and inserting the following: ''subset of—

''(i) the information systems used or operated by the agency; and

''(ii) the information systems used, operated, or supported on behalf of the agency by a contractor of the agency, any subcontractor

(at any tier) of such a contractor, or any other entity;'';

(B) in subparagraph (B), by striking ''and'' at the end;

(C) in subparagraph (C), by striking the period and inserting ''; and''; and

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

''(D) a conclusion whether the agency's information security controls are effective, including an identification of any significant deficiencies in such controls.''; and

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

''(3) Each audit under this section shall conform to generally accepted government auditing standards.''.

(c) CONFORMING AMENDMENTS.—

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

(A) Subsection (b)(1).

(B) Subsection (b)(2).

(C) Subsection (c).

(D) Subsection (e)(1).

(E) Subsection (e)(2).

(2) Section 3545(d) of such title is amended to read as follows:

''(d) EXISTING AUDITS.—The audit required by this section may be based in whole or in part on an audit relating to programs or practices of the applicable agency.''.

(3) Section 3545(f) of such title is amended by striking ''evaluators'' and inserting ''auditors''.

(4) Section 3545(g)(1) of such title is amended by striking ''evaluations'' and inserting ''audits''.

(5) Section 3545(g)(3) of such title is amended by striking ''Evaluations'' and inserting ''Audits''.

(6) Section 3543(a)(8)(A) of such title is amended by striking ''evaluations'' and inserting ''audits''.

(7) Section 3544(b)(5)(D) of such title (as redesignated by section 5(2)(C)) is amended by striking ''a evaluation'' and inserting ''an audit''.

SEC. 9. BEST PRACTICES FOR PRIVACY IMPACT ASSESSMENTS.

Section 208(b)(3) of the E-Government Act of 2002 (Public Law 107–347; 44 U.S.C. 3501 note) is amended—

(1) in subparagraph (B), by striking ''and'' at the end;

(2) in subparagraph (C), by striking the period and inserting ''; and'', and

(3) by adding at the end the following:

''(D) develop best practices for agencies to follow in conducting privacy impact assessments.''.

SEC. 10. IMPLEMENTATION.

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

Passed the House of Representatives June 3, 2008.

Attest: LORRAINE C. MILLER,

Clerk.