

FEDERAL AGENCY DATA PROTECTION ACT

MAY 21, 2008.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. WAXMAN, from the Committee on Oversight and Government Reform, submitted the following

R E P O R T

together with

ADDITIONAL VIEWS

[To accompany H.R. 4791]

[Including cost estimate of the Congressional Budget Office]

The Committee on Oversight and Government Reform, to whom was referred the bill (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, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

	Page
Purpose and Summary	6
Background and Need for Legislation	6
Legislative History	8
Section-by-Section	8
Explanation of Amendments	11
Committee Consideration	11
Rollcall Votes	11
Application of Law to the Legislative Branch	11
Statement of Oversight Findings and Recommendations of the Committee	11
Statement of General Performance Goals and Objectives	11
Constitutional Authority Statement	12
Federal Advisory Committee Act	12
Unfunded Mandate Statement	12
Earmark Identification	12
Committee Estimate	12
Budget Authority and Congressional Budget Office Cost Estimate	12

Changes in Existing Law Made by the Bill as Reported	14
Additional Views	22

The amendment is as follows:

Strike all after the enacting clause and insert the following:

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. 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 information 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.

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 systems 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);”;

(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 government 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.

PURPOSE AND SUMMARY

H.R. 4791, the “Federal Agency Data Protection Act,” was introduced December 18, 2007, by Reps. Wm. Lacy Clay, Edolphus Towns, and Henry A. Waxman. The legislation strengthens protections of personally identifiable information of individuals that is maintained in or transmitted by federal agency information systems.

BACKGROUND AND NEED FOR LEGISLATION

Weaknesses in federal information security threaten both the operability of federal programs and the privacy of citizens whose personal information is maintained in government computer systems. To minimize vulnerabilities in federal information systems, the Federal Information Security Management Act (FISMA) was enacted in December 2002 as part of the Electronic Government Act of 2002.¹ FISMA reauthorized and strengthened provisions in the Government Information Security Reform Act (GISRA) that require federal agencies to identify and minimize potential risks to the security of their information and information systems.

FISMA requires that federal agencies assess the state of their information security management and submit these findings to the Office of Management and Budget (OMB) in September of each year. It also charges each federal agency’s Chief Information Officer (CIO) with evaluating the state of his or her agency’s information security management through a questionnaire developed by OMB. The results of each evaluation must be independently reviewed by the agency’s Inspector General (IG) (or another independent evaluator on behalf of the IG) and then submitted to OMB. OMB must summarize these findings and submit its analysis in an annual report to Congress.

FISMA requires agencies, as part of their information security stewardship responsibilities, to:

- conduct periodic risk assessments that evaluate likely threats against their information and systems;
- categorize the appropriate levels of risk among different information systems and to develop plans to minimize the risk posed by various threats;
- provide employees with security awareness training;
- maintain a detailed inventory of all information systems, both in-house and those operated by outside contractors; and
- develop a contingency plan for the continuation of operations in the event that systems are compromised.

In July 2005, GAO reported that weaknesses in federal information security persist despite FISMA.² According to GAO:

Pervasive weaknesses * * * threaten the integrity, confidentiality, and availability of federal information and in-

¹P.L. 107-347.

²Government Accountability Office, Information Security: Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements, (Jul. 2005) (GAO-05-552).

formation systems. * * * These weaknesses exist primarily because agencies have not yet fully implemented strong information security management programs. These weaknesses put federal operations and assets at risk of fraud, misuse, and destruction. In addition, they place financial data at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption.

These concerns were echoed during a number of significant data breaches at government agencies during 2006. According to the Congressional Research Service, agencies reporting incidents of potentially compromised data during FY 2006 included the Department of Veterans Affairs, Transportation, and Energy, and the Internal Revenue Service.³ In addition, the Department of State also suffered a series of hacking attacks.

In February 2008 testimony before the Subcommittee on Information Policy, Census, and the National Archives and the Subcommittee on Government Management, Organization, and Procurement, GAO reiterated that federal agencies “continue to confront longstanding information security control deficiencies” and that there are “opportunities for federal agencies to bolster information security.”⁴

Reps. Clay, Towns, and Waxman introduced H.R. 4791, the Federal Agency Data Protection Act in order to strengthen current requirements for protecting data that is stored or transmitted by federal agency systems. The bill would amend FISMA by adding several new information security policies and procedures. The following key provisions are contained in the legislation:

- a comprehensive definition of “personally identifiable information” that would encompass a broader category of information about an individual and provide greater clarity for agencies to determine what types of information need protection;
- requirements for OMB to review agency plans and schedules for conducting tests and evaluations, develop policies and procedures in order to secure personally identifiable information that is stored on mobile digital devices, and develop effective system configuration requirements for agency systems;
- requirements for agency compliance with OMB established policies and procedures regarding minimally acceptable system configuration requirements and testing and evaluation requirements;
- data breach notification to Director, federal information security incident center, and to individuals whose personally identifiable information could be compromised as a result of such breach;
- requirements for the development of agency plans to reduce the risks posed by peer-to-peer file sharing programs;
- requirements for an annual independent audit of agency information security programs in conformance with generally acceptable government auditing standards; and

³Library of Congress, Congressional Research Service, Data Security Breaches: Context and Incident Summaries (May 2007) (RL33199).

⁴Government Accountability Office, Information Security: Although Progress Reported, Agencies Need to Resolve Significant Deficiencies (Feb. 2008) (GAO-08-496T).

- a requirement for OMB to develop best practices for agencies conducting privacy impact assessments.

LEGISLATIVE HISTORY

H.R. 4791, legislation to strengthen current requirements for protecting personally identifiable information that is stored or transmitted by federal agency systems, was introduced on December 18, 2007, by Reps. Wm. Lacy Clay, Edolphus Towns, and Henry A. Waxman. H.R. 4791 was referred to the Committee on Oversight and Government Reform.

The Subcommittee on Information Policy, Census, and the National Archives and the Subcommittee on Government Management, Organization, and Procurement held a joint oversight hearing on June 4, 2007, to review the future of FISMA. The witnesses were Karen S. Evans, Administrator, Office of E-Government and Information Technology, Office of Management and Budget; Gregory C. Wilshusen, Director, Information Security Issues, Government Accountability Office; Vance Hitch, Chief Information Officer, U.S. Department of Justice; Phil Bond, President and CEO, Information Technology Association of America; Paul Kurtz, Partner & Chief Operating Officer, Good Harbor Consulting, LLC; John W. Carlson, Executive Director, Financial Services Roundtable/BITS; and James Andrew Lewis, Director and Senior Fellow, Technology and Public Policy Program, Center for Strategic and International Studies.

The Subcommittee on Information Policy, Census, and National Archives and the Subcommittee on Government Management, Organization, and Procurement held a joint legislative hearing on February 14, 2008, to review H.R. 4791. The witnesses were Karen S. Evans, Administrator, Office of Management and Budget; Gregory C. Wilshusen, Director, Government Accountability Office; Alan Paller, Director, SANS Institute (Research); Bruce McConnell, President, McConnell International, LLC; and Tim Bennett, President, Cyber Security Industry Alliance.

The full Committee held a business meeting on April 16, 2008, and approved H.R. 4791, as amended, by voice vote.

SECTION-BY-SECTION

Section 1: Short title and table of contents

This section states that the Act may be cited as the “Federal Data Protection Act” and provides a table of contents.

Section 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.

Section 3: Definitions

This Section establishes a comprehensive definition of “personally identifiable information” to clearly cover all information about an individual, including personal information about subjects such as one’s financial transactions or medical history, identifying information that can be used to locate or trace a person, and any other information associated with the individual. This definition will en-

sure that agencies develop controls to secure all personally identifiable information.

This section also defines “mobile digital device” to include any device that can store or process information electronically and is designed to be used in a manner not limited to a fixed location.

Section 4: Authority of Director of Office of Management and Budget to establish information security policies and procedures

This section requires OMB, when approving or disapproving agency information security programs, to ensure that such programs include testing, evaluation, and remediation according to risk.

In addition, this section requires OMB to establish 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.

This section also requires OMB to ensure agency compliance with minimally acceptable system configuration requirements consistent with best practices, including those developed by NIST. While FISMA required agencies to ensure compliance with agency-selected configuration requirements, it did not require that such requirements meet any standards. Moreover, this section has provisions that ensure that agency contracts for (or involving or including) the provision of information technology products or services include requirements for contractors meet minimally acceptable configuration requirements. Finally, this section directs OMB to ensure that information systems operated by contractors on behalf of a federal agency comply with the information security requirements of FISMA.

Section 5: Responsibilities of Federal agencies for information security

This section would require agencies to meet minimally acceptable system configuration requirements as OMB directs pursuant to Section 4 of this Act.

This section also requires agencies to include testing and evaluation of system configuration requirements as OMB directs pursuant to Section 4 of the Act. Moreover, this section clarifies that this includes 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.

Finally, this section requires agencies to have plans and procedures for ensuring the adequacy of information security protections for systems maintaining or transmitting personally identifiable information, including requirements for maintaining a current inventory of such systems; implementing requirements for mobile digital devices, and developing, implementing, and overseeing remediation plans to address vulnerabilities in information security protections for such information.

Section 6: Federal agency data breach notification requirements

This section requires OMB to keep a summary of information breaches reported to the Director and the federal information secu-

rity incident center. It also requires OMB to establish policies, procedures, and standards for agencies to follow in the event of a data breach involving disclosure of personally identifiable information, including a timely notice to those whose information could be compromised as a result of said breach. OMB would be required to give guidance on whether additional actions are necessary, such as a data breach analysis, fraud resolution services, identity theft insurance or credit protection services.

This section also requires agency CIOs to develop and maintain inventories of all personal computers, laptops, or any other hardware containing personally identifiable information.

In addition, this section requires agencies to establish procedures for notifying individuals whose personally identifiable information may have been compromised and procedures for timely reporting of information security breaches involving personally identifiable information to the Director and the federal information security incident center.

Finally, this section gives authority to agency Chief Human Capital Officers to prescribe 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.

Section 7: Protection of Government computers from risks of peer-to-peer file sharing

The growth in the use of peer-to-peer file sharing programs has soared and this growth poses a risk to the security of federal systems and networks. When federal employees install software to activate file sharing, they can provide an easy path for intruders to gain access to and compromise information on an agency's computer systems and networks. While the risk of unauthorized peer-to-peer file sharing is well-known, federal agencies have been slow to develop concerted plans for dealing with the threat.

This section requires the head of each agency to develop and implement a plan to ensure the security and privacy of information collected or maintained by or on behalf of the agency with respect to the risks posed by certain peer-to-peer file sharing programs. Further, to ensure that agencies develop viable plans, the legislation calls on GAO to review agency plans within 18 months of enactment.

Section 8: Annual independent audit

A fundamental element of the information security reforms of FISMA is the requirement for an annual independent evaluation of each agency's information security program. After about five years of experience with the implementation of the Act, it is clear that one weakness is the inconsistency of these annual evaluations.

This section would strengthen the annual evaluation process by requiring that such evaluations be audits, not merely evaluations, and that such audits conform to generally accepted government auditing standards. It further requires such audits to reach a conclusion as to whether the agency's information security controls are effective, including an identification of any significant deficiencies in such controls.

Section 9: Best practices for privacy impact assessments

This section requires the Director of the OMB to develop best practices for agencies to follow in conducting privacy impact assessments.

Section 10: Implementation

Section 10 requires that 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.

EXPLANATION OF AMENDMENTS

Subcommittee Chairman Wm. Lacy Clay offered an amendment in the nature of a substitute, which was accepted by voice vote. The Clay amendment creates a discrete data breach notification section, requires agency CIOs to maintain inventories of all hardware containing personally identifiable information, and clarifies CIOs' authority to enforce data breach policies. In addition, the amendment clarifies the definition of peer-to-peer file sharing programs and deletes two sections of the introduced bill regarding privacy impact assessments.

COMMITTEE CONSIDERATION

On Wednesday, April 16, 2008, the Committee ordered H.R. 4791 favorably reported to the House by a voice vote.

ROLLCALL VOTES

No rollcall votes were taken on this legislation.

APPLICATION OF LAW TO THE LEGISLATIVE BRANCH

Section 102(b)(3) of Public Law 104-1 requires a description of the application of this bill to the legislative branch where the bill relates to the terms and conditions of employment or access to public services and accommodations. This bill provides and strengthens requirements for ensuring the effectiveness of information security controls over information resources. As such this bill does not relate to employment or access to public services and accommodations.

STATEMENT OF OVERSIGHT FINDINGS AND RECOMMENDATIONS OF THE COMMITTEE

In compliance with clause 3(c)(1) of rule XIII and clause (2)(b)(1) of rule X of the Rules of the House of Representatives, the Committee's oversight findings and recommendations are reflected in the descriptive portions of this report, including the need to strengthen protections of personally identifiable information stored on federal information systems.

STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

In accordance with clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, the Committee's performance goals and objectives are reflected in the descriptive portions of this report, in-

cluding strengthening information security controls in the federal government.

CONSTITUTIONAL AUTHORITY STATEMENT

Under clause 3(d)(1) of rule XIII of the Rules of the House of Representatives, the Committee must include a statement citing the specific powers granted to Congress to enact the law proposed by H.R. 4791. Article I, Section 8, Clause 18 of the Constitution of the United States grants the Congress the power to enact this law.

FEDERAL ADVISORY COMMITTEE ACT

The Committee finds that the legislation does not establish or authorize the establishment of an advisory committee within the definition of 5 U.S.C. App., Section 5(b).

UNFUNDED MANDATE STATEMENT

Section 423 of the Congressional Budget and Impoundment Control Act (as amended by Section 101(a)(2) of the Unfunded Mandate Reform Act, P.L. 104-4) requires a statement whether the provisions of the reported include unfunded mandates. In compliance with this requirement the Committee has received a letter from the Congressional Budget Office that is included herein.

EARMARK IDENTIFICATION

H.R. 4791 does not contain any congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(d), 9(e), or 9(f) of rule XXI.

COMMITTEE ESTIMATE

Clause 3(d)(2) of rule XIII of the Rules of the House of Representatives requires an estimate and a comparison by the Committee of the costs that would be incurred in carrying out H.R. 4791. However, clause 3(d)(3)(B) of that rule provides that this requirement does not apply when the Committee has included in its report a timely submitted cost estimate of the bill prepared by the Director of the Congressional Budget Office under section 402 of the Congressional Budget Act.

BUDGET AUTHORITY AND CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

With respect to the requirements of clause 3(c)(2) of rule XIII of the Rules of the House of Representatives and section 308(a) of the Congressional Budget Act of 1974 and with respect to requirements of clause (3)(c)(3) of rule XIII of the Rules of the House of Representatives and section 402 of the Congressional Budget Act of 1974, the Committee has received the following cost estimate for H.R. 4791 from the Director of Congressional Budget Office:

MAY 14, 2008

Hon. HENRY A. WAXMAN,
*Chairman, Committee on Oversight and Government Reform, House
of Representatives, Washington, DC.*

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 4791, the Federal Agency Data Protection Act.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Matthew Pickford.

Sincerely,

PETER R. ORSZAG.

Enclosure.

H.R. 4791—Federal Agency Data Protection Act

Summary: H.R. 4791 would amend current law to enhance the protection of certain information collected by the federal government. CBO estimates that implementing the bill would cost about \$106 million over the 2009–2013 period, assuming appropriation of the necessary amounts. The bill could also affect direct spending by agencies not funded through annual appropriations (such as the Tennessee Valley Authority) or by agencies whose activities are considered off-budget (such as the U.S. Postal Service). CBO estimates, however, that any increase in spending by those agencies would not be significant or would be offset by corresponding increases in rates charged by those entities.

The bill contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would not affect the budgets of state, local, or tribal governments.

Estimated Cost to the Federal Government: The estimated budgetary impact of H.R. 4791 is shown in the following table. The cost of this legislation falls primarily within budget function 800 (general government) but also would affect budget functions that contain spending for inspectors general.

	By fiscal year in millions of dollars—				
	2009	2010	2011	2012	2013
CHANGES IN SPENDING SUBJECT TO APPROPRIATION					
Estimated Authorization Level	25	20	21	21	22
Estimated Outlays	23	20	20	21	22

Basis of estimate: For this estimate, CBO assumes that the bill will be enacted near the start of fiscal year 2009, that the necessary funds will be provided for each year, and that spending will follow historical patterns for similar activities.

H.R. 4791 would require the Office of Management and Budget (OMB) to establish additional security policies and procedures for federal agencies that collect and maintain personal information for employees or other individuals. The bill also would require agencies to establish security standards and notification procedures to be followed when personal information has been unlawfully accessed. Finally, the bill would require federal agencies to audit their information programs and practices.

Most of the provisions of the bill would codify and expand current practices of the federal government. Under the provisions of the Federal Information Security Management Act (FISMA), the Privacy Act, and OMB memoranda, federal agencies are already required to protect information about individuals, maintain standards for notifications of security breaches, and perform annual reviews to evaluate the security of their information systems. Agencies spent nearly \$6 billion on such activities in fiscal year 2007, including about \$20 million to perform security evaluations under FISMA.

CBO expects that implementing the legislation would require agencies to perform formal audits on information security systems rather than the evaluations they perform under existing law. Based on information from OMB and other agencies, CBO estimates that implementing those audit requirements would increase costs by \$23 million in 2009 to cover additional personnel and administrative costs in the affected agencies. We estimate that such costs would fall to about \$20 million a year after 2009, once audit standards and procedures have been developed.

Intergovernmental and private-sector impact: The bill contains no intergovernmental or private-sector mandates as defined in UMRA and would not affect the budgets of state, local, or tribal governments.

Estimate prepared by: Federal Costs: Matthew Pickford; Impact on State, Local, and Tribal Governments: Elizabeth Cove; Impact on the Private Sector: Paige Piper/Bach.

Estimate approved by: Theresa Gullo, Deputy Assistant Director for Budget Analysis.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, existing law in which no change is proposed is shown in roman):

TITLE 44, UNITED STATES CODE

* * * * *

CHAPTER 35—COORDINATION OF FEDERAL INFORMATION POLICY

* * * * *

SUBCHAPTER III—INFORMATION SECURITY

* * * * *

§ 3542. Definitions

(a) * * *

(b) ADDITIONAL DEFINITIONS.—As used in this subchapter:

(1) * * *

* * * * *

(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.

§ 3543. Authority and functions of the Director

(a) **IN GENERAL.**—The Director shall oversee agency information security policies and practices, including—

(1) * * *

* * * * *

(5) reviewing at least annually, and approving or disapproving, agency information security programs required under section 3544(b), *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;

* * * * *

(7) overseeing the operation of the Federal information security incident center required under section 3546; **[and]**

(8) reporting to Congress no later than March 1 of each year on agency compliance with the requirements of this subchapter, including—

*(A) a summary of the findings of **[evaluations]** audits required by section 3545;*

* * * * *

*(D) planned remedial action to address such deficiencies; **[and]***

*(E) a summary of, and the views of the Director on, the report prepared by the National Institute of Standards and Technology under section 20(d)(10) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3**[.]**); and*

- (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);
- (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
- (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.

* * * * *

§ 3544. Federal agency responsibilities

- (a) IN GENERAL.—The head of each agency shall—

(1) * * *

* * * * *

(3) delegate to the agency Chief Information Officer established under section 3506 (or comparable official in an agency not covered by such section) the authority to ensure compliance with *and, to the extent determined necessary and explicitly authorized by the head of the agency, to enforce* the requirements imposed on the agency under this subchapter, including—

(A) * * *

* * * * *

(D) training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities; **[and]**

(E) assisting senior agency officials concerning their responsibilities under paragraph (2); *and*

(F) *developing and maintaining an inventory of all personal computers, laptops, or any other hardware containing personally identifiable information;*

* * * * *

(b) AGENCY PROGRAM.—Each agency shall develop, document, and implement an agencywide information security program, approved by the Director under section 3543(a)(5), to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes—

(1) * * *

(2) policies and procedures that—

(A) * * *

* * * * *

(D) ensure compliance with—

(i) * * *

* * * * *

(iii) minimally acceptable system configuration requirements, **[as determined by the agency]** *as required by the Director under section 3543(a)(10); and*

* * * * *

(5) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually *and as approved by the Director*, of which such testing—

(A) shall include testing of management, operational, and technical controls of every information system identified in the inventory required under section 3505(c); **[and]**

(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*

[(B)] (D) may include testing relied on in [a evaluation] an audit under section 3545;

* * * * *

(7) procedures for detecting, reporting, and responding to security incidents, consistent with standards and guidelines issued pursuant to section 3546(b), including—

(A) * * *

* * * * *

(C) notifying and consulting with, as appropriate—

(i) * * *

* * * * *

(iii) any other agency or office, in accordance with law or as directed by the President; [and]

(8) plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency[.];

(9) plans and procedures for ensuring the adequacy of information security protections for systems 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;

(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.

* * * * *

§ 3545. Annual independent [evaluation] audit

(a) IN GENERAL.—(1) Each year each agency shall have performed an independent [evaluation] audit of the information security program and practices of that agency to determine the effectiveness of such program and practices.

(2) Each [evaluation] audit under this section shall include—

(A) testing of the effectiveness of information security policies, procedures, and practices of a representative [subset of the agency’s information systems;] 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) an assessment (made on the basis of the results of the testing) of compliance with—

(i) * * *

* * * * *

(ii) related information security policies, procedures, standards, and guidelines; **[and]**

(C) separate presentations, as appropriate, regarding information security relating to national security systems**[.]; and**

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

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

(b) INDEPENDENT AUDITOR.—Subject to subsection (c)—

(1) for each agency with an Inspector General appointed under the Inspector General Act of 1978 or any other law, the annual **[evaluation]** *audit* required by this section shall be performed by the Inspector General or by an independent external auditor, as determined by the Inspector General of the agency; and

(2) for each agency to which paragraph (1) does not apply, the head of the agency shall engage an independent external auditor to perform the **[evaluation]** *audit*.

(c) NATIONAL SECURITY SYSTEMS.—For each agency operating or exercising control of a national security system, that portion of the **[evaluation]** *audit* required by this section directly relating to a national security system shall be performed—

(1) * * *

* * * * *

[(d) EXISTING EVALUATIONS.—The evaluation required by this section may be based in whole or in part on an audit, evaluation, or report relating to programs or practices of the applicable agency.]

(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.

(e) AGENCY REPORTING.—(1) Each year, not later than such date established by the Director, the head of each agency shall submit to the Director the results of the **[evaluation]** *audit* required under this section.

(2) To the extent an **[evaluation]** *audit* required under this section directly relates to a national security system, the **[evaluation]** *audit* results submitted to the Director shall contain only a summary and assessment of that portion of the **[evaluation]** *audit* directly relating to a national security system.

(f) PROTECTION OF INFORMATION.—Agencies and **[evaluators]** *auditors* shall take appropriate steps to ensure the protection of information which, if disclosed, may adversely affect information security. Such protections shall be commensurate with the risk and comply with all applicable laws and regulations.

(g) OMB REPORTS TO CONGRESS.—(1) The Director shall summarize the results of the [evaluations] audits conducted under this section in the report to Congress required under section 3543(a)(8).

* * * * *

(3) [Evaluations] Audits and any other descriptions of information systems under the authority and control of the Director of Central Intelligence or of National Foreign Intelligence Programs systems under the authority and control of the Secretary of Defense shall be made available to Congress only through the appropriate oversight committees of Congress, in accordance with applicable laws.

* * * * *

SECTION 208 OF THE E-GOVERNMENT ACT OF 2002

SEC. 208. PRIVACY PROVISIONS.

(a) * * *

(b) PRIVACY IMPACT ASSESSMENTS.—

(1) RESPONSIBILITIES OF AGENCIES.—

(A) IN GENERAL.—An agency shall take actions described under subparagraph (B) before—

(i) developing or procuring information technology that collects, maintains, or disseminates [information that is in an identifiable form] personally identifiable information; or

(ii) initiating a new collection of information that—

(I) * * *

(II) includes any [information in an identifiable form permitting the physical or online contacting of a specific individual] personally identifiable information, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government.

* * * * *

(2) CONTENTS OF A PRIVACY IMPACT ASSESSMENT.—

(A) * * *

(B) GUIDANCE.—The guidance shall—

(i) ensure that a privacy impact assessment is commensurate with the size of the information system being assessed, the sensitivity of [information that is in an identifiable form] personally identifiable information in that system, and the risk of harm from unauthorized release of that information; and

* * * * *

(3) RESPONSIBILITIES OF THE DIRECTOR.—The Director shall—

(A) * * *

(B) oversee the implementation of the privacy impact assessment process throughout the Government; [and]

(C) require agencies to conduct privacy impact assessments of existing information systems or ongoing collections of [information that is in an identifiable form] personally identifiable information as the Director determines appropriate[.]; and

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

* * * * *

(d) DEFINITION.—[In this section, the term “identifiable form” means any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.] 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.

* * * * *

SECTION 1402 OF TITLE 5, UNITED STATES CODE

§ 1402. Authority and functions of agency Chief Human Capital Officers

(a) The functions of each Chief Human Capital Officer shall include—

(1) * * *

* * * * *

(5) identifying best practices and benchmarking studies[, and];

(6) applying methods for measuring intellectual capital and identifying links of that capital to organizational performance and growth[.]; and

(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.

* * * * *

ADDITIONAL VIEWS OF RANKING MEMBER TOM DAVIS

Secure information is the lifeblood of effective government. But we've seen a wide range of incidents involving data loss or theft, privacy breaches, and security incidents at federal agencies.

In almost all of these cases, Congress and the public would not have learned of these events had we not requested the information. After all, despite the volume of sensitive information held by agencies—tax returns, military records, health records, to name a few—there currently is no requirement agencies notify citizens whose personal information may have been compromised. We need to ensure the public knows when its sensitive personal information has been lost or compromised.

Therefore I am pleased we incorporated my legislation, H.R. 2124, which requires timely notice be provided to individuals whose sensitive personal information could be compromised by a breach of data security at a Federal agency.

In addition to focusing on ensuring adequate protection of individuals' personal information held by the federal government, I have also spent years focusing on general, government-wide information management and security policy.

For example, the Privacy Act and the E-Government Act of 2002 outline the parameters for the protection of personal information. The Federal Information Security Management Act (FISMA), which I authored, requires each agency to create a comprehensive risk-based approach to agency-wide information security management, through preparedness, evaluation, and reporting requirements.

These laws created a solid foundation for federal information security, making security management an integral part of an agency's operations and ensuring agencies are actively using best practices to secure the federal government's systems.

But it is now incumbent upon us to take federal information security to the next level—to find new and innovative ways to secure government information.

Unfortunately, I do not believe H.R. 4791 does enough. Most of the provisions contained in this bill are a grab bag of vague requirements, additional mandates, and misplaced priorities. It casts dynamic concepts in stone. And it gives agency personnel more boxes to check.

I have long called for a bill with teeth—and an opportunity to discuss and debate the overall issues associated with improving federal information security. I think we have missed some key opportunities in that regard.

For example:

(1) We haven't seriously considered, to my knowledge, the need to pursue providing incentives for agency success—such as financial incentives for agencies which excel.

(2) We haven't given enough consideration, to my knowledge, to the need to pursue funding penalties and personnel reforms which provide real motivation for an agency to improve its information security.

(3) Although I've pushed the scorecards for many years, we need increased Congressional oversight of agency information security practices.

(4) Have we done enough to bring greater consistency across the IG community regarding standards and review regarding improved information security?

(5) And in our recent review of this issue, I do not believe we have considered, nor do we address, what I believe is one of the most important and complex problems associated with these issues: the difficulties faced by agency Chief Information Officers in their attempts to be successful and effective—both in terms of their status within their agencies and their underlying statutory authority.

(6) Also, have we taken a serious look at whether the creation of a federal CIO or an Information Czar at OMB would improve the federal government's ability to handle and process information? I do not believe so.

Public confidence in government is essential. In the end, the public demands effective government. And effective government depends on secure information. I remain concerned that this legislation falls short in a number of these important areas.

TOM DAVIS.

