AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

109TH CONGRESS
2d Session

HOUSE OF REPRESENTATIVES

REPT. 109–651
Part 1

VETERANS IDENTITY AND CREDIT SECURITY ACT OF 2006

SEPTEMBER 13, 2006.—Ordered to be printed

Mr. BUYER, from the Committee on Veterans' Affairs, submitted the following

R E P O R T

[To accompany H.R. 5835]

[Including cost estimate of the Congressional Budget Office]

The Committee on Veterans' Affairs, to whom was referred the bill (H.R. 5835) to amend title 38, United States Code, to improve information management within the Department of Veterans Affairs, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Veterans Identity and Credit Security Act of 2006".

SEC. 2. 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, is amended—

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

(2) by striking the period and inserting "; and" at the end of paragraph (8); and

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

"(9) establishing policies, procedures, and standards for agencies to follow in the event of a breach of data security involving the disclosure of sensitive personal information in violation of section 552a of title 5, including a requirement for timely notice to be given to those individuals whose sensitive personal 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 of identity theft, fraud, or other unlawful conduct regarding such individual.".

(b) AUTHORITY OF CHIEF INFORMATION OFFICER TO ENFORCE DATA BREACH POLICIES.—Section 3544(a)(3) of title 44, United States Code, is amended 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".

(c) INCLUSION OF DATA BREACH NOTIFICATION IN AGENCY INFORMATION SECURITY PROGRAMS.—Section 3544(b) of title 44, United States Code, is amended—

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

(2) by striking the period and inserting "; and" at the end of paragraph (8); and

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

"(9) procedures for notifying individuals whose sensitive personal information is compromised consistent with policies, procedures, and standards established under section 3543(a)(9) of this title.".

(d) SENSITIVE PERSONAL INFORMATION DEFINITION.—Section 3542(b) of title 44, United States Code, is amended by adding at the end the following new paragraph:

"(4) The term 'sensitive personal information' means any information contained in a record, as defined in section 552a(4) of title 5.".

SEC. 3. UNDER SECRETARY FOR INFORMATION SERVICES.

(a) UNDER SECRETARY.—Chapter 3 of title 38, United States Code, is amended by inserting after section 307 the following new section:

"§ 307A. Under Secretary for Information Services

"(a) UNDER SECRETARY.—There is in the Department an Under Secretary for Information Services, who is appointed by the President, by and with the advice and consent of the Senate. The Under Secretary shall be the head of the Office of Information Services and shall perform such functions as the Secretary shall prescribe.

"(b) SERVICE AS CHIEF INFORMATION OFFICER.—Notwithstanding any other provision of law, the Under Secretary for Information Services shall serve as the Chief Information Officer of the Department under section 310 of this title.".

(b) CLERICAL AMENDMENT.—The table of sections at the beginning of such chapter is amended by inserting after the item relating to section 307 the following new item:

"307A. Under Secretary for Information Services.".

(c) CONFORMING AMENDMENT.—Section 308(b) of such title is amended by striking paragraph (5) and redesignating paragraphs (6) through (11) as paragraphs (5) through (10), respectively.

SEC. 4. DEPARTMENT OF VETERANS AFFAIRS INFORMATION SECURITY.

(a) INFORMATION SECURITY.—Chapter 57 of title 38, United States Code, is amended by adding at the end the following new subchapter:

"SUBCHAPTER III—INFORMATION SECURITY

"§ 5721. Definitions

"For the purposes of this subchapter:

"(1) The term 'sensitive personal information' means the name, address, or telephone number of an individual, in combination with any of the following:

"(A) The Social Security number of the individual.

"(B) The date of birth of the individual.

"(C) Any information not available as part of the public record regarding the individual's military service or health.

"(D) Any financial account or other financial information relating to the individual.

"(E) The driver's license number or equivalent State identification number of the individual.

"(F) The deoxyribonucleic acid profile or other unique biometric data of the individual, including the fingerprint, voice print, retina or iris image, or other unique physical representation of the individual.

"(2) The term 'data breach' means the loss, theft, or other unauthorized access to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data.

"(3) The term 'data breach analysis' means the identification of any misuse of sensitive personal information involved in a data breach.

"(4) The term 'fraud resolution services' means services to assist an individual in the process of recovering and rehabilitating the credit of the individual after the individual experiences identity theft.

"(5) The term 'identity theft' has the meaning given such term under section 603 of the Fair Credit Reporting Act (15 U.S.C. 1681a).

"(6) The term 'identity theft insurance' means any insurance policy that pays benefits for costs, including travel costs, notary fees, and postage costs, lost wages, and legal fees and expenses associated with the identity theft of the insured individual.

"(7) The term 'principal credit reporting agency' means a consumer reporting agency as described in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)).

"§ 5722. Office of the Under Secretary for Information Services

"(a) DEPUTY UNDER SECRETARIES.—The Office of the Under Secretary for Information Services shall consist of the following:

"(1) The Deputy Under Secretary for Information Services for Security, who shall serve as the Senior Information Security Officer of the Department.

"(2) The Deputy Under Secretary for Information Services for Operations and Management.

"(3) The Deputy Under Secretary for Information Services for Policy and Planning.

"(b) APPOINTMENTS.—Appointments under subsection (a) shall be made by the Secretary, notwithstanding the limitations of section 709 of this title.

"(c) QUALIFICATIONS.—At least one of positions established and filled under subsection (a) shall be filled by an individual who has at least five years of continuous service in the Federal civil service in the executive branch immediately preceding the appointment of the individual as a Deputy Under Secretary. For purposes of determining such continuous service of an individual, there shall be excluded any service by such individual in a position—

"(1) of a confidential, policy-determining, policy-making, or policy-advocating character;

"(2) in which such individual served as a noncareer appointee in the Senior Executive Service, as such term is defined in section 3132(a)(7) of title 5; or

"(3) to which such individual was appointed by the President.

"§ 5723. Information security management

"(a) RESPONSIBILITIES OF CHIEF INFORMATION OFFICER.—To support the economical, efficient, and effective execution of subtitle III of chapter 35 of title 44, and policies and plans of the Department, the Secretary shall ensure that the Chief Information Officer of the Department has the authority and control necessary to develop, approve, implement, integrate, and oversee the policies, procedures, processes, activities, and systems of the Department relating to that subtitle, including the management of all related mission applications, information resources, personnel, and infrastructure.

"(b) ANNUAL COMPLIANCE REPORT.—Not later than March 1 of each year, the Secretary shall submit to the Committees on Veterans' Affairs of the Senate and House of Representatives, the Committee on Government Reform of the House of Representatives, and the Committee on Homeland Security and Governmental Affairs of the Senate, a report on the Department's compliance with subtitle III of chapter 35 of title 44. The information in such report shall be displayed in the aggregate and separately for each Administration, office, and facility of the Department.

"(c) REPORTS TO SECRETARY OF COMPLIANCE DEFICIENCIES.—(1) At least once every month, the Chief Information Officer shall report to the Secretary any deficiency in the compliance with subtitle III of chapter 35 of title 44 of the Department or any Administration, office, or facility of the Department.

"(2) The Chief Information Officer shall immediately report to the Secretary any significant deficiency in such compliance.

"(d) DATA BREACHES.—(1) The Chief Information Officer shall immediately provide notice to the Secretary of any data breach.

"(2) Immediately after receiving notice of a data breach under paragraph (1), the Secretary shall provide notice of such breach to the Director of the Office of Management and Budget, the Inspector General of the Department, and, if appropriate, the Federal Trade Commission and the United States Secret Service.

"(e) BUDGETARY MATTERS.—When the budget for any fiscal year is submitted by the President to Congress under section 1105 of title 31, the Secretary shall submit to Congress a report that identifies amounts requested for Department implementation and remediation of and compliance with this subchapter and subtitle III of chapter 35 of title 44. The report shall set forth those amounts both for each Administration within the Department and for the Department in the aggregate and shall identify, for each such amount, how that amount is aligned with and supports such implementation and compliance.

"§ 5724. Congressional reporting and notification of data breaches

"(a) QUARTERLY REPORTS.—(1) Not later than 30 days after the last day of a fiscal quarter, the Secretary shall submit to the Committees on Veterans' Affairs of the Senate and House of Representatives a report on any data breach with respect to sensitive personal information processed or maintained by the Department that occurred during that quarter.

"(2) Each report submitted under paragraph (1) shall identify, for each data breach covered by the report, the Administration and facility of the Department responsible for processing or maintaining the sensitive personal information involved in the data breach.

"(b) NOTIFICATION OF SIGNIFICANT DATA BREACHES.—(1) In the event of a data breach with respect to sensitive personal information processed or maintained by the Secretary that the Secretary determines is significant, the Secretary shall provide notice of such breach to the Committees on Veterans' Affairs of the Senate and House of Representatives.

"(2) Notice under paragraph (1) shall be provided promptly following the discovery of such a data breach and the implementation of any measures necessary to determine the scope of the breach, prevent any further breach or unauthorized disclosures, and reasonably restore the integrity of the data system.

"§ 5725. Data breaches

"(a) INDEPENDENT RISK ANALYSIS.—(1) In the event of a data breach with respect to sensitive personal information that is processed or maintained by the Secretary, the Secretary shall ensure that, as soon as possible after the data breach, a non-Department entity conducts an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach.

"(2) If the Secretary determines, based on the findings of a risk analysis conducted under paragraph (1), that a reasonable risk exists for the potential misuse of sensitive information involved in a data breach, the Secretary shall provide credit protection services in accordance with section 5726 of this title.

"(b) NOTIFICATION.—(1) In the event of a data breach with respect to sensitive personal information that is processed or maintained by the Secretary, the Secretary shall provide to an individual whose sensitive personal information is involved in that breach notice of the data breach—

"(A) in writing; or

"(B) by email, if—

"(i) the Department's primary method of communication with the individual is by email; and

"(ii) the individual has consented to receive such notification.

"(2) Notice provided under paragraph (1) shall—

"(A) describe the circumstances of the data breach and the risk that the breach could lead to misuse, including identity theft, involving the sensitive personal information of the individual;

"(B) describe the specific types of sensitive personal information that was compromised as a part of the data breach;

"(C) describe the actions the Department is taking to remedy the data breach;

"(D) inform the individual that the individual may request a fraud alert and credit security freeze under this section;

"(E) clearly explain the advantages and disadvantages to the individual of receiving fraud alerts and credit security freezes under this section; and

"(F) includes such other information as the Secretary determines is appropriate.

"(3) The notice required under paragraph (1) shall be provided promptly following the discovery of a data breach and the implementation of any measures necessary to determine the scope of the breach, prevent any further breach or unauthorized disclosures, and reasonably restore the integrity of the data system.

"(c) REPORT.—For each data breach with respect to sensitive personal information processed or maintained by the Secretary, the Secretary shall promptly submit to the Committees on Veterans' Affairs of the Senate and House of Representatives a report containing the findings of any independent risk analysis conducted under subsection (a)(1), any determination of the Secretary under subsection (a)(2), and a description of any credit protection services provided under section 5726 of this title.

"(d) FINAL DETERMINATION.—Notwithstanding sections 511 and 7104(a) of this title, any determination of the Secretary under subsection (a)(2) with respect to the reasonable risk for the potential misuse of sensitive information involved in a data breach is final and conclusive and may not be reviewed by any other official, administrative body, or court, whether by an action in the nature of mandamus or otherwise.

"(e) FRAUD ALERTS.—(1) In the event of a data breach with respect to sensitive personal information that is processed or maintained by the Secretary, the Secretary shall arrange, upon the request of an individual whose sensitive personal information is involved in the breach to a principal credit reporting agency with which the Secretary has entered into a contract under section 5726(d) and at no cost to the individual, for the principal credit reporting agency to provide fraud alert services for that individual for a period of not less than one year, beginning on the date of such request, unless the individual requests that such fraud alert be removed before the end of such period, and the agency receives appropriate proof of the identity of the individual for such purpose.

"(2) The Secretary shall arrange for each principal credit reporting agency referred to in paragraph (1) to provide any alert requested under such subsection in the file of the individual along with any credit score generated in using that file, for a period of not less than one year, beginning on the date of such request, unless the individual requests that such fraud alert be removed before the end of such period, and the agency receives appropriate proof of the identity of the individual for such purpose.

"(f) CREDIT SECURITY FREEZE.—(1) In the event of a data breach with respect to sensitive personal information that is processed or maintained by the Secretary, the Secretary shall arrange, upon the request of an individual whose sensitive personal information is involved in the breach and at no cost to the individual, for each principal credit reporting agency to apply a security freeze to the file of that individual for a period of not less than one year, beginning on the date of such request, unless the individual requests that such security freeze be removed before the end of such period, and the agency receives appropriate proof of the identity of the individual for such purpose.

"(2) The Secretary shall arrange for a principal credit reporting agency applying a security freeze under paragraph (1)—

"(A) to send a written confirmation of the security freeze to the individual within five business days of applying the freeze;

"(B) to refer the information regarding the security freeze to other consumer reporting agencies;

"(C) to provide the individual with a unique personal identification number or password to be used by the individual when providing authorization for the release of the individual's credit for a specific party or period of time; and

"(D) upon the request of the individual, to temporarily lift the freeze for a period of time specified by the individual, beginning not later than three business days after the date on which the agency receives the request.

"§ 5726. Provision of credit protection services

"(a) COVERED INDIVIDUAL.—For purposes of this section, a covered individual is an individual whose sensitive personal information that is processed or maintained by the Department (or any third-party entity acting on behalf of the Department) is involved, on or after August 1, 2005, in a data breach for which the Secretary determines a reasonable risk exists for the potential misuse of sensitive personal information under section 5725(a)(2) of this title.

"(b) NOTIFICATION.—(1) In addition to any notice required under subsection 5725(b) of this title, the Secretary shall provide to a covered individual notice in writing that—

"(A) the individual may request credit protection services under this section;

"(B) clearly explains the advantages and disadvantages to the individual of receiving credit protection services under this section;

"(C) includes a notice of which principal credit reporting agency the Secretary has entered into a contract with under subsection (d), and information about requesting services through that agency;

"(D) describes actions the individual can or should take to reduce the risk of identity theft; and

"(E) includes such other information as the Secretary determines is appropriate.

"(2) The notice required under paragraph (1) shall be made as promptly as possible and without unreasonable delay following the discovery of a data breach for which the Secretary determines a reasonable risk exists for the potential misuse of sensitive personal information under section 5725(a)(2) of this title and the implementation of any measures necessary to determine the scope of the breach, prevent any further breach or unauthorized disclosures, and reasonably restore the integrity of the data system.

"(3) The Secretary shall ensure that each notification under paragraph (1) includes a form or other means for readily requesting the credit protection services

under this section. Such form or other means may include a telephone number, email address, or Internet website address.

"(c) AVAILABILITY OF SERVICES THROUGH OTHER GOVERNMENT AGENCIES.—If a service required to be provided under this section is available to a covered individual through another department or agency of the Government, the Secretary and the head of that department or agency may enter into an agreement under which the head of that department or agency agrees to provide that service to the covered individual.

"(d) CONTRACT WITH CREDIT REPORTING AGENCY.—Subject to the availability of appropriations and notwithstanding any other provision of law, the Secretary shall enter into contracts or other agreements as necessary with one or more principal credit reporting agencies in order to ensure, in advance, the provision of credit protection services under this section and fraud alerts and security freezes under section 5725 of this title. Any such contract or agreement may include provisions for the Secretary to pay the expenses of such a credit reporting agency for the provision of such services.

"(e) DATA BREACH ANALYSIS.—The Secretary shall arrange, upon the request of a covered individual and at no cost to the individual, to provide data breach analysis for the individual for a period of not less than one year, beginning on the date of such request.

"(f) PROVISION OF CREDIT MONITORING SERVICES AND IDENTITY THEFT INSURANCE.—During the one-year period beginning on the date on which the Secretary notifies a covered individual that the individual's sensitive personal information is involved in a data breach, the Secretary shall arrange, upon the request of the individual and without charge to the individual, for the provision of credit monitoring services to the individual. Credit monitoring services under this subsection shall include each of the following:

"(1) One copy of the credit report of the individual every three months.

"(2) Fraud resolution services for the individual.

"(3) Identity theft insurance in a coverage amount that does not exceed $30,000 in aggregate liability for the insured.

"§ 5727. Contracts for data processing or maintenance

"(a) CONTRACT REQUIREMENTS.—If the Secretary enters into a contract for the performance of any Department function that requires access to sensitive personal information, the Secretary shall require as a condition of the contract that—

"(1) the contractor shall not, directly or through an affiliate of the contractor, disclose such information to any other person unless the disclosure is lawful and is expressly permitted under the contract;

"(2) the contractor, or any subcontractor for a subcontract of the contract, shall promptly notify the Secretary of any data breach that occurs with respect to such information.

"(b) LIQUIDATED DAMAGES.—Each contract subject to the requirements of subsection (a) shall provide for liquidated damages to be paid by the contractor to the Secretary in the event of a data breach with respect to any sensitive personal information processed or maintained by the contractor or any subcontractor under that contract.

"(c) PROVISION OF CREDIT PROTECTION SERVICES.—Any amount collected by the Secretary under subsection (b) shall be deposited in or credited to the Department account from which the contractor was paid and shall remain available for obligation without fiscal year limitation exclusively for the purpose of providing credit protection services in accordance with section 5726 of this title.

"§ 5728. Authorization of appropriations

"There are authorized to be appropriated to carry out this subchapter such sums as may be necessary for each fiscal year.".

(b) CLERICAL AMENDMENT.—The table of sections at the beginning of such chapter is amended by adding at the end the following new items:

"SUBCHAPTER III—INFORMATION SECURITY

"5721. Definitions.
"5722. Office of the Under Secretary for Information Services.
"5723. Information security management.
"5724. Congressional reporting and notification of data breaches.
"5725. Data breaches.
"5726. Provision of credit protection services.
"5727. Contracts for data processing or maintenance.
"5728. Authorization of appropriations.".

(c) DEADLINE FOR REGULATIONS.—Not later than 60 days after the date of the enactment of this Act, the Secretary of Veterans Affairs shall publish regulations to

carry out subchapter III of chapter 57 of title 38, United States Code, as added by subsection (a).

SEC. 5. REPORT ON FEASIBILITY OF USING PERSONAL IDENTIFICATION NUMBERS FOR IDENTIFICATION.

Not later than 180 days after the date of the enactment of this Act, the Secretary of Veterans Affairs shall submit to Congress a report containing the assessment of the Secretary with respect to the feasibility of using personal identification numbers instead of Social Security numbers for the purpose of identifying individuals whose sensitive personal information (as that term is defined in section 5721 of title 38, United States Code, as added by section 4) is processed or maintained by the Secretary.

SEC. 6. DEADLINE FOR APPOINTMENTS.

(a) DEADLINE.—Not later than 180 days after the date of the enactment of this Act—

(1) the President shall nominate an individual to serve as the Under Secretary of Veterans Affairs for Information Services under section 307A of title 38, United States Code, as added by section 3; and

(2) the Secretary of Veterans Affairs shall appoint an individual to serve as each of the Deputy Under Secretaries of Veterans Affairs for Information Services under section 5722 of such title, as added by section 4.

(b) REPORT.—Not later than 30 days after the date of the enactment of this Act, and every 30 days thereafter until the appointments described in subsection (a) are made, the Secretary of Veterans Affairs shall submit to Congress a report describing the progress of such appointments.

SEC. 7. INFORMATION SECURITY EDUCATION ASSISTANCE PROGRAM.

(a) PROGRAM REQUIRED.—Title 38, United States Code, is amended by inserting after chapter 78 the following new chapter:

"CHAPTER 79—INFORMATION SECURITY EDUCATION ASSISTANCE PROGRAM

"Sec.
"7901. Programs; purpose.
"7902. Scholarship program.
"7903. Education debt reduction program.
"7904. Preferences in awarding financial assistance.
"7905. Requirement of honorable discharge for veterans receiving assistance.
"7906. Regulations.
"7907. Termination.

"§ 7901. Programs; purpose

"(a) IN GENERAL.—To encourage the recruitment and retention of Department personnel who have the information security skills necessary to meet Department requirements, the Secretary shall carry out programs in accordance with this chapter to provide financial support for education in computer science and electrical and computer engineering at accredited institutions of higher education.

"(b) TYPES OF PROGRAMS.—The programs authorized under this chapter are as follows:

"(1) Scholarships for pursuit of doctoral degrees in computer science and electrical and computer engineering at accredited institutions of higher education.

"(2) Education debt reduction for Department personnel who hold doctoral degrees in computer science and electrical and computer engineering at accredited institutions of higher education.

"§ 7902. Scholarship program

"(a) AUTHORITY.—(1) Subject to the availability of appropriations, the Secretary shall establish a scholarship program under which the Secretary shall, subject to subsection (d), provide financial assistance in accordance with this section to a qualified person—

"(A) who is pursuing a doctoral degree in computer science or electrical or computer engineering at an accredited institution of higher education; and

"(B) who enters into an agreement with the Secretary as described in subsection (b).

"(2)(A) Except as provided under subparagraph (B), the Secretary may provide financial assistance under this section to an individual for up to five years.

"(B) The Secretary may waive the limitation under subparagraph (A) if the Secretary determines that such a waiver is appropriate.

"(3)(A) The Secretary may award up to five scholarships for any academic year to individuals who did not receive assistance under this section for the preceding academic year.

"(B) Not more than one scholarship awarded under subparagraph (A) may be awarded to an individual who is an employee of the Department when the scholarship is awarded.

"(b) SERVICE AGREEMENT FOR SCHOLARSHIP RECIPIENTS.—(1) To receive financial assistance under this section an individual shall enter into an agreement to accept and continue employment in the Department for the period of obligated service determined under paragraph (2).

"(2) For the purposes of this subsection, the period of obligated service for a recipient of financial assistance under this section shall be the period determined by the Secretary as being appropriate to obtain adequate service in exchange for the financial assistance and otherwise to achieve the goals set forth in section 7901(a) of this title. In no event may the period of service required of a recipient be less than the period equal to two times the total period of pursuit of a degree for which the Secretary agrees to provide the recipient with financial assistance under this section. The period of obligated service is in addition to any other period for which the recipient is obligated to serve on active duty or in the civil service, as the case may be.

"(3) An agreement entered into under this section by a person pursuing an doctoral degree shall include terms that provide the following:

"(A) That the period of obligated service begins on a date after the award of the degree that is determined under the regulations prescribed under section 7906 of this title.

"(B) That the individual will maintain satisfactory academic progress, as determined in accordance with those regulations, and that failure to maintain such progress constitutes grounds for termination of the financial assistance for the individual under this section.

"(C) Any other terms and conditions that the Secretary determines appropriate for carrying out this section.

"(c) AMOUNT OF ASSISTANCE.—(1) The amount of the financial assistance provided for an individual under this section shall be the amount determined by the Secretary as being necessary to pay—

"(A) the tuition and fees of the individual; and

"(B) $1500 to the individual each month (including a month between academic semesters or terms leading to the degree for which such assistance is provided or during which the individual is not enrolled in a course of education but is pursuing independent research leading to such degree) for books, laboratory expenses, and expenses of room and board.

"(2) In no case may the amount of assistance provided for an individual under this section for an academic year exceed $50,000.

"(3) In no case may the total amount of assistance provided for an individual under this section exceed $200,000.

"(4) Notwithstanding any other provision of law, financial assistance paid an individual under this section shall not be considered as income or resources in determining eligibility for, or the amount of benefits under, any Federal or federally assisted program.

"(d) REPAYMENT FOR PERIOD OF UNSERVED OBLIGATED SERVICE.—(1) An individual who receives financial assistance under this section shall repay to the Secretary an amount equal to the unearned portion of the financial assistance if the individual fails to satisfy the requirements of the service agreement entered into under subsection (b), except in certain circumstances authorized by the Secretary.

"(2) The Secretary may establish, by regulations, procedures for determining the amount of the repayment required under this subsection and the circumstances under which an exception to the required repayment may be granted.

"(3) An obligation to repay the Secretary under this subsection is, for all purposes, a debt owed the United States. A discharge in bankruptcy under title 11 does not discharge a person from such debt if the discharge order is entered less than five years after the date of the termination of the agreement or contract on which the debt is based.

"(e) WAIVER OR SUSPENSION OF COMPLIANCE.—The Secretary shall prescribe regulations providing for the waiver or suspension of any obligation of a individual for service or payment under this section (or an agreement under this section) whenever noncompliance by the individual is due to circumstances beyond the control of the individual or whenever the Secretary determines that the waiver or suspension of compliance is in the best interest of the United States.

"(f) INTERNSHIPS.—(1) The Secretary may offer a compensated internship to an individual for whom financial assistance is provided under this section during a period between academic semesters or terms leading to the degree for which such assistance is provided. Compensation provided for such an internship shall be in addition to the financial assistance provided under this section.

"(2) An internship under this subsection shall not be counted toward satisfying a period of obligated service under this section.

"(g) INELIGIBILITY OF INDIVIDUALS RECEIVING CERTAIN EDUCATION ASSISTANCE PAYMENTS.—An individual who receives a payment of educational assistance under chapter 30, 31, 32, 34, or 35 of this title or chapter 1606 or 1607 of title 10 for a month in which the individual is enrolled in a course of education leading to a doctoral degree in information security is not eligible to receive financial assistance under this section for that month.

"§ 7903. Education debt reduction program

"(a) AUTHORITY.—(1) Subject to the availability of appropriations, the Secretary shall establish an education debt reduction program under which the Secretary shall make education debt reduction payments under this section to qualified individuals eligible under subsection (b) for the purpose of reimbursing such individuals for payments by such individuals of principal and interest on loans described in paragraph (2) of that subsection.

"(2)(A) For each fiscal year, the Secretary may accept up to five individuals into the program established under paragraph (1) who did not receive such a payment during the preceding fiscal year.

"(B) Not more than one individual accepted into the program for a fiscal year under subsection (A) shall be a Department employee as of the date on which the individual is accepted into the program.

"(b) ELIGIBILITY.—An individual is eligible to participate in the program under this section if the individual—

"(1) has completed a doctoral degree in computer science or electrical or computer engineering at an accredited institution of higher education during the five-year period preceding the date on which the individual is hired;

"(2) is an employee of the Department who serves in a position related to information security (as determined by the Secretary); and

"(3) owes any amount of principal or interest under a loan, the proceeds of which were used by or on behalf of that individual to pay costs relating to a doctoral degree in computer science or electrical or computer engineering at an accredited institution of higher education.

"(c) AMOUNT OF ASSISTANCE.—(1) Subject to paragraph (2), the amount of education debt reduction payments made to an individual under this section may not exceed $82,500 over a total of five years, of which not more than $16,500 of such payments may be made in each year.

"(2) The total amount payable to an individual under this section for any year may not exceed the amount of the principal and interest on loans referred to in subsection (b)(3) that is paid by the individual during such year.

"(d) PAYMENTS.—(1) The Secretary shall make education debt reduction payments under this section on an annual basis.

"(2) The Secretary shall make such a payment—

"(A) on the last day of the one-year period beginning on the date on which the individual is accepted into the program established under subsection (a); or

"(B) in the case of an individual who received a payment under this section for the preceding fiscal year, on the last day of the one-year period beginning on the date on which the individual last received such a payment.

"(3) Notwithstanding any other provision of law, education debt reduction payments under this section shall not be considered as income or resources in determining eligibility for, or the amount of benefits under, any Federal or federally assisted program.

"(e) PERFORMANCE REQUIREMENT.—The Secretary may make education debt reduction payments to an individual under this section for a year only if the Secretary determines that the individual maintained an acceptable level of performance in the position or positions served by the individual during the year.

"(f) NOTIFICATION OF TERMS OF PROVISION OF PAYMENTS.—The Secretary shall provide to an individual who receives a payment under this section notice in writing of the terms and conditions that apply to such a payment.

"(g) COVERED COSTS.—For purposes of subsection (b)(3), costs relating to a course of education or training include—

"(1)) tuition expenses; and

"(2) all other reasonable educational expenses, including fees, books, and laboratory expenses;

"§ 7904. Preferences in awarding financial assistance

"In awarding financial assistance under this chapter, the Secretary shall give a preference to qualified individuals who are otherwise eligible to receive the financial assistance in the following order of priority:

"(1) Veterans with service-connected disabilities.

"(2) Veterans.

"(3) Persons described in section 4215(a)(1)(B) of this title.

"(4) Individuals who received or are pursuing degrees at institutions designated by the National Security Agency as Centers of Academic Excellence in Information Assurance Education.

"(5) Citizens of the United States.

"§ 7905. Requirement of honorable discharge for veterans receiving assistance

"No veteran shall receive financial assistance under this chapter unless the veteran was discharged from the Armed Forces under honorable conditions.

"§ 7906. Regulations

"The Secretary shall prescribe regulations for the administration of this chapter.

"§ 7907. Termination

"The authority of the Secretary to make a payment under this chapter shall terminate on July 31, 2017.".

(b) GAO REPORT.—Not later than three years after the date of the enactment of this Act, the Comptroller General shall submit to Congress a report on the scholarship and education debt reduction programs under chapter 79 of title 38, United States Code, as added by subsection (a).

(c) APPLICABILITY OF SCHOLARSHIPS.—Section 7902 of title 38, United States Code, as added by subsection (a), shall apply with respect to financial assistance provided for an academic semester or term that begins on or after August 1, 2007.

(d) CLERICAL AMENDMENT.—The tables of chapters at the beginning of such title, and at the beginning of part V of such title, are amended by inserting after the item relating to chapter 78 the following new item:

"79. Information Security Education Assistance Program ..... 7901".

INTRODUCTION

The reported bill reflects the Committee's consideration of H.R. 5455, H.R. 5464, H.R. 5467, H.R. 5490, H.R. 5577, H.R. 5588, H.R. 5636, H.R. 5783, and H.R. 5835, as amended.

On May 23, 2006, the Honorable John T. Salazar introduced H.R. 5455, the Veterans' Identity Protection Act, which would require the Secretary of Veterans Affairs to provide free credit monitoring and credit reports for veterans and others affected by the theft of veterans' personal data, and to ensure that such persons are appropriately notified of such thefts.

On May 24, 2006, the Honorable Marsha Blackburn introduced H.R. 5464, which would require that veterans be notified that their data was stolen, and that the veteran could request a free credit report every three months for the next year, and have a year of credit monitoring.

On May 24, 2006, the Honorable Thelma D. Drake introduced H.R. 5467, which would amend title 38, United States Code, to establish criminal penalties for the unauthorized disclosure of records containing personal information about veterans.

On May 25, 2006, the Honorable Darlene Hooley introduced H.R. 5487, which would require the Secretary of Veterans Affairs to take certain actions to mitigate the effects of the breach of data that occurred in May 2006.

On May 25, 2006, the Honorable Robert E. Andrews introduced H.R. 5490, which would require the Secretary of Veterans Affairs to establish a personal identification number for each veteran in order to help preserve the confidentiality of the Department of Veterans Affairs' information on veterans.

On May 25, 2006, the full Committee held a hearing with the Secretary of Veterans Affairs and the Inspector General of the De-

partment of Veterans Affairs to review the loss of sensitive information of veterans.

On June 8, 2006, full Committee Chairman Steve Buyer and Committee on Appropriations' Subcommittee on Military Quality of Life and Veterans Affairs Chairman James T. Walsh held a business roundtable with information technology experts from private sector companies, including the Goldman Sachs Group; EMC Corporation; VISA; Citigroup Inc.; TriWest Healthcare Alliance; and the American Bankers Association.

On June 9, 2006, the Honorable Shelley Moore Capito introduced H.R. 5577, which would enhance protection of records of the Department of Veterans Affairs containing personal identifying information that is required by law to be confidential and privileged from disclosure except as authorized by law.

On June 12, 2006, the Honorable John T. Salazar and the Honorable Lane Evans introduced H.R. 5588, the Comprehensive Veterans' Data Protection and Identity Theft Prevention Act of 2006, which would require the Secretary of Veterans Affairs to protect sensitive personal information of veterans, to ensure that veterans are appropriately notified of any breach of data security with respect to such information, and to provide free credit monitoring and credit reports for veterans and others affected by any such breach of data security.

On June 14, 2006, the full Committee held an oversight hearing on information security at the Department of Veterans Affairs.

On June 16, 2006, the Honorable Kay Granger introduced H.R. 5636, the Social Security Number Privacy and Protection Act, to reduce the risk of identity theft by limiting the use of social security account numbers on certain Government-issued identification cards and Government documents.

On June 20, 2006, the Subcommittees on Disability Assistance and Memorial Affairs and Economic Opportunity held a joint hearing on data security at the Veterans Benefits Administration.

On June 21, 2006, the Subcommittee on Health held an oversight hearing on safeguarding veterans' medical information within the Veterans Health Administration.

On June 22, 2006, the full Committee held an oversight hearing on the academic and legal implications of VA's data loss.

On June 28, 2006, the full Committee held a hearing on what VA IT organizational structures would have best prevented VA's failures in information management.

On June 29, 2006, the full Committee held a hearing with the Secretary of Veterans Affairs on the progress of the Department of Veterans Affairs in mitigating the nation's second largest data breach.

On July 13, 2006, the Honorable Brian P. Bilbray introduced H.R. 5783, the Comprehensive Credit Services for Veterans Act of 2006, which would amend title 38, United States Code, to improve the security of sensitive personal data processed or maintained by the Secretary of Veterans Affairs.

On July 18, 2006, the full Committee held a legislative hearing on draft legislation to review proposals and draft legislation the Committee was preparing as a response to the recent theft of the personal information of 26.5 million veterans and 2.2 million active duty and reserve component service members and their spouses,

which included provisions and concepts from H.R. 5464, H.R. 5467, H.R. 5487, H.R. 5577, H.R. 5588, and H.R. 5783.

On July 19, 2006, the Chairman and Acting Ranking Member, the Honorable Steve Buyer and the Honorable Bob Filner, respectively, along with Mr. Michael Bilirakis, Mr. Lane Evans, Mr. Cliff Stearns, Mr. Luis V. Gutierrez, Mr. Dan Burton, Ms. Corrine Brown of Florida, Mr. Henry E. Brown, Jr., of South Carolina, Mr. Michael H. Michaud, Mr. Jeff Miller of Florida, Ms. Stephanie Herseth, Mr. John Boozman, Mr. Ted Strickland, Mr. Jeb Bradley, Mr. Silvestre Reyes, Mrs. Ginny Brown-Waite, Ms. Shelley Berkley, Mr. Brian P. Bilbray, Mr. John T. Salazar, Mr. Tom Davis of Virginia, Mr. Henry A. Waxman, Mr. James T. Walsh, Mr. Chet Edwards, Mr. John D. Dingell, and Ms. Janice D. Schakowsky introduced H.R. 5835, the Veterans Information and Credit Security Act of 2006.

On July 20, 2006, the full Committee met to markup H.R. 5835, and ordered it reported favorably with an amendment in the nature of a substitute to the House by unanimous voice vote.

SUMMARY OF THE REPORTED BILL

H.R. 5835, as amended, would:

1. Establish federal agency data breach notification requirements including the provision of enforcement authority to the Chief Information Officer of the Department of Veterans Affairs.

2. Create a new Under Secretary of Information Services at the Department of Veterans Affairs, who would also serve as the Chief Information Officer.

3. Create the Office of the Under Secretary for Information Security, which would contain three Deputy Under Secretaries appointed by the Secretary:

   a. Deputy Under Secretary for Security, who would also serve as the Senior Information Security Officer of the Department,

   b. Deputy Under Secretary for Operations and Management, and

   c. Deputy Under Secretary for Policy and Planning.

4. Define the responsibilities of the Under Secretary for Information Services under the Federal Information Security Management Act of 2002 (FISMA), which would include regular reporting of compliance or noncompliance with FISMA to the Secretary and Congress.

5. Provide reporting and notification guidelines by the Secretary of Veterans Affairs to Congress in the event of a data security breach.

6. Require an independent analysis of any data breaches to determine the level of risk associated for the potential misuse of any sensitive personal information involved in the data breach, and provide notification to affected individuals which would include:

   a. the availability of fraud alerts at the request of the individual, and

   b. the availability of a credit security freeze at the request of the individual.

7. Permit the Secretary of Veterans Affairs to have final determination with respect to the reasonable risk for the potential mis-

use of sensitive information involved in a data breach based on the risk analysis performed.

8. Allow remediation of identity theft, in the event the Secretary determines a reasonable risk exists for the potential misuse of the breached data, for a veteran or other individual whose sensitive personal information was compromised due to a data security breach at the Department, through the availability of credit protection services and, upon the request of that individual, fraud resolution services including;

a. a definition of the covered individual,

b. notification in writing or by email that the individual's sensitive personal information was part of a security breach,

c. the availability of services through other government entities,

d. contracting with credit reporting agencies,

e. the availability of a data breach analysis, and

f. credit monitoring services and identity theft insurance.

9. Require, as a condition of contracting with the Department of Veterans Affairs for the processing or maintenance of sensitive personal information, that a contractor not disclose such information to any other person, unless the disclosure is lawful and is expressly permitted under the contract. Should a breach occur by either the contractor or the subcontractor, liquidated damages would be incurred by the contractor. Monies collected from contractors as liquidated damages would be used to provide credit protection services to covered individuals affected by the data breach for which the penalty is paid.

10. Provide for an appropriation of such funds as may be necessary for each fiscal year for credit protection services.

11. Require a report by the Department of Veterans Affairs on the feasibility of using personal identification numbers instead of social security numbers for the purpose of identifying individuals whose sensitive personal information is processed or maintained by the Secretary. The report is to be submitted to Congress no later than 180 days after the date of enactment.

12. Set a deadline for appointments under this Act of not later than 180 days after enactment, with a report of not later than 30 days after the date of the enactment, and every 30 days thereafter until the appointments are made, from the Secretary describing the progress of the appointments.

13. Create a scholarship program for up to five new scholarships each year at VA for recruitment of personnel who are in pursuit of a doctoral degree in information security, computer engineering, or electrical engineering at an accredited institution of higher learning. The recipients would be required to agree to a period of obligated service at the Department as determined by the Secretary, not less than two years for every one year of school tuition paid, and repayment would be required in the event an individual voluntarily terminates service prior to the end of the period of obligated service.

14. Provide for repayment of education debts for five individuals each year who hold doctoral degrees in information security, computer engineering, or electrical engineering from an accredited institution of higher learning (only one may be a current employee of the Department). Debt reduction payments made to individuals

under this section would not exceed $82,500 over a total of 5 years of participation, or $16,500 per year in the program.

15. Authorize the Secretary of Veterans Affairs to give preference in the award of either the scholarships or the repayment program to individuals who are: service-disabled veterans, veterans, surviving spouses of veterans who have died of a service-connected disability, or spouses of veterans who are 100-percent permanently and totally disabled; or individuals who have received or are pursuing a degree at a Center of Academic Excellence in Information Assurance Education.

16. Require the Government Accountability Office (GAO) to report on the education programs 3 years after date of enactment.

BACKGROUND AND DISCUSSION

Federal Agency Data Breach Notification.—Section 2 of the bill would provide enforcement authority under the Federal Information Security Management Act of 2002 (FISMA). The Committee found in its investigation of the data breach of May 3, 2006, the intent of Congress should be clarified with regard to the extent to which FISMA would authorize the Department Secretary or the Chief Information Officer to enforce compliance with FISMA at the Department. This language was written in cooperation with the Committee on Government Reform and would strengthen the Secretary and the CIO's authority and enforcement under FISMA for all government agencies. This section also would require timely notification to individuals whose sensitive personal information was included in a breach of data at the agency. The Committee strongly urges the Department of Veterans Affairs to follow the guidelines set forth in the Federal Information Security Management Act of 2002 (FISMA) to ensure the protection of veterans' personal information. The Committee also expects that the Secretary would consider compliance with FISMA when evaluating an employee's performance for providing merit bonuses, consistent with the Secretary's goal of working to make VA the "gold standard" in information security.

Under Secretary for Information Services.—Section 3 of the bill would create a new appointment-level Under Secretary for Information Services at the Department of Veterans Affairs. This Under Secretary would direct the Office of Information Services, and also serve as the Chief Information Officer of the Department of Veterans Affairs. The Committee intends that the Under Secretary for Information Services and Chief Information Officer would serve on the VA/DoD Joint Executive Council, just as the current Assistant Secretary for Information and Technology and Chief Information Officer does. The Committee also determined that, consistent with private sector practices, the Department would be better served by an Under Secretary appointee who would be in charge of all IT related services for the Department. In the private sector the CIO is often a corporate vice president.

Department of Veterans Affairs Information Security.—Section 4 of the bill would create the Office of the Under Secretary for Information Services. In the Office of Information Services, there would be three Deputy Under Secretaries: (1) Deputy Under Secretary for Security, who would also serve as the Chief Information Security Officer of the Department; (2) Deputy Under Secretary for Oper-

ations and Management; who would oversee day to day information technology operations within the Department of Veterans Affairs, and (3) Deputy Under Secretary for Policy and Planning who would provide policy guidelines and development planning for IT related issues at the Department.

The section would also identify the responsibilities of the Chief Information Officer, and would require an annual report to be submitted to the House and Senate Committees on Veterans' Affairs, the House Committee on Government Reform and the Senate Committee on Homeland Security and Governmental Affairs on the Department's compliance under FISMA. The information would be for each Administration, office or facility of the Department.

The Chief Information Officer would be required to report at least monthly to the Secretary any deficiency in the compliance of FISMA of the Department or any Administration, office, or facility of the Department. Should a significant deficiency in compliance be found at the Department or in any Administration, office or facility of the Department, the Chief Information Officer would be required to immediately report this to the Secretary.

With respect to data breaches that may occur at the Department or at any Administration, office or facility of the Department, the Chief Information Officer would immediately provide notice of said breach to the Secretary. The Secretary would then provide notice of the breach to the Director of the Office of Management and Budget, the Inspector General of the Department, and if appropriate, the Federal Trade Commission and the United States Secret Service.

Under section 5725(b)(1) the Department would be required to notify the individual whose sensitive personal information was part of the data breach. The Committee suggests that under this section the Department develop a mechanism through the Veterans Integrated Service Networks to notify the veterans of the data breach and provide an explanation of the services provided under this legislation.

Report on Feasibility of Using Personal Identification Numbers for Identification.—Section 5 of the bill would require a report from the Secretary of Veterans Affairs to Congress, containing the assessment of the Secretary with respect to the feasibility of using personal identification numbers instead of Social Security numbers for the purpose of identifying individuals whose sensitive personal information is processed or maintained by the Secretary. Currently, social security numbers are maintained in the same database as all other veteran information, and used by claims processors to access files at the Department. Prior to 1973, a special C-file number was assigned to veterans claims and cases, and was used as the primary identifier for veterans information at the Department. The Committee seeks to determine the feasibility of changing to a system of identifiers which would not require the use of a Social Security Number stored within the veterans' primary record in order to protect the veterans personal identifying information.

Deadline for Appointments.—Section 6 of the bill would require the Under Secretary for Information Services, and the Deputy Under Secretaries under the Office of Information Services to be appointed not later than 180 days after the enactment of the Act. Thirty days after enactment of this act, the Secretary would be re-

quired to report to Congress on the progress of the appointments, and then every 30 days until all appointments are made.

Information Security Education Assistance Program.—Section 7 of the bill would require VA to establish a financial assistance program that would include no more than five scholarships and five debt reduction payment programs per year through July 31, 2017 for individuals in pursuit of, or having received, a doctoral degree in computer science, electrical engineering, or computer engineering, in an effort to assist VA with recruiting new personnel with expertise in cyber security. The Committee intends for VA to broadly interpret the areas of doctoral degrees to include any disciplines in the information security systems arena. Finally, the Committee expects VA to give preference to service-disabled veterans, veterans, surviving spouses of veterans who have died of a service-connected disability or spouses of veterans who are 100 percent permanently and totally disabled, and individuals who have received or are pursuing a degree at a Center of Academic Excellence in Information Assurance Education. The education assistance program was specifically drafted into the legislation in order to provide the Secretary with a recruiting and retention tool to obtain the most qualified individuals in the area of information technology and information security to work at the Department.

SECTION-BY-SECTION ANALYSIS

Section 1 of the bill would provide that this Act may be cited as the "Veterans Identity and Credit Security Act of 2006."

Section 2(a) of the bill would amend section 3543(a) of title 44, United States Code, by (1) striking "and" at the end of paragraph (7); (2) striking the period and inserting "; and" at the end of paragraph (8); and (3) adding at the end the following new paragraph: "(9) establishing policies, procedures, and standards for agencies to follow in the event of a breach of data security involving the disclosure of sensitive personal information in violation of section 552a of title 5, United States Code, including a requirement for timely notice to be given to those individuals whose sensitive personal 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 of identity theft, fraud, or other unlawful conduct regarding such individual.

Section 2(b) of the bill would amend section 3544(a)(3) of title 44, United States Code, 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".

Section 2(c) of the bill would amend section 3544(b) of title 44, United States Code, (1) by striking "and" at the end of paragraph (7); (2) by striking the period and inserting "; and" at the end of paragraph (8); and by adding at the end the following new paragraph: (9) procedures for notifying individuals whose sensitive personal information is compromised consistent with policies, procedures, and standards established under section 3543(a)(9) of this title."

Section 2(d) of the bill would amend section 3542(b) of title 44, United States Code, by defining the term 'sensitive personal information' as any information contained in a record, as defined in section 552a(4) of title 5, United States Code.

Section 3 of the bill would amend Chapter 3 of title 38, United States Code, by inserting after section 307 the following new section: "§ 307A. Under Secretary for Information Services".

New section 307A(a) of the bill would create the Under Secretary for Information Services, who is appointed by the President by and with the advice and consent of the Senate. The Under Secretary would be the head of the Office of Information Services and will perform such functions as the Secretary prescribes.

New section 307A(b) of the bill would specify that the Under Secretary for Information Services serve as the Chief Information Officer of the Department under section 310 of title 38, United States Code, notwithstanding any other provision of law.

Section 3(b) of the bill would make clerical amendments.

Section 3(c) of the bill would make conforming amendments.

Section 4(a) of the bill would amend Chapter 57 of title 38, United States Code, by adding a new Subchapter III—Information Security:

New section 5721(1) of the bill would define the term 'sensitive personal information' as the name, address, or telephone number of an individual, in combination with any of the following: (A) the Social Security number of the individual, (B) the date of the birth of the individual, (C) any information not available as part of the public record regarding the individual's military service or health, (D) any financial account or other financial information relating to the individual, (E) the driver's license number or equivalent State identification number of the individual, (F) the deoxyribonucleic acid profile or other unique biometric data of the individual, including the fingerprint, voice print, retina or iris image, or other unique physical representation of the individual.

New section 5721(2) of the bill would define the term 'data breach' to mean the loss, theft, or other unauthorized access to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data.

New section 5721(3) of the bill would define the term 'data breach analysis' to mean the identification of any misuse of sensitive personal information involved in a data breach.

New section 5721(4) of the bill would define the term 'fraud resolution services' to mean services to assist an individual in the process of recovering and rehabilitating the credit of the individual after the individual experiences identity theft.

New section 5721(5) of the bill would define the term 'identity theft' as the meaning given under section 603 of the Fair Credit Reporting Act (15 U.S.C. 168Ia).

New section 5721(6) of the bill would define the term 'identity theft insurance' as any insurance policy that pays benefits for costs, including travel costs, notary fees, postage costs, lost wages, and legal fees and expenses associated with the identity of the insured individual.

New section 5721(7) of the bill would define the term 'principal credit reporting agency' as a consumer reporting agency as described in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)).

New section 5722(a) of the bill would provide that the Office of the Under Secretary for Information Services consist of the fol-

lowing: (I) the Deputy Under Secretary for Information Services for Security, who shall serve as the Senior Information Security Officer of the Department, (2) the Deputy Under Secretary for Information Services for Operations and Management, (3) the Deputy Under Secretary for Information Services for Policy and Planning.

New section 5722(b) of the bill would provide that appointments under new section 5722(a) be made by the Secretary, notwithstanding the limitations of section 709 of title 38, United States Code.

New section 5722(c) of the bill would provide that at least one of the positions established and filled under new section 5722(a) be filled by an individual who has at least five years of continuous service in the Federal civil service in the executive branch immediately preceding the appointment of the individual as a Deputy Under Secretary. For purposes of determining such continuous service of an individual, there shall be excluded any service by such individual in a position (1) of a confidential, policy-determining, policy-making, or policy-advocating character; (2) in which such individual served as a non-career appointee in the Senior Executive Service, as defined in section 3132(a)(7) of title 5, United States Code; or (3) to which such individual was appointed by the President.

New section 5723(a) would provide for the responsibilities of the Chief Information Officer. The Secretary shall ensure that the Chief Information Officer, in order to support the economical, efficient, and effective execution of subtitle III of chapter 35 of title 44, United States Code, have the authority and control necessary to develop, approve, implement, integrate, and oversee the policies, procedures, processes, activities, and systems of the Department relating to that subtitle, including the management of all related mission applications, information resources, personnel, and infrastructure.

New section 5723(b) of the bill would require the Secretary to submit a report, not later than March 1 of each year, to the Committees on Veterans' Affairs of the Senate and House of Representatives, the Committee on Government Reform of the House of Representatives, and the Committee on Homeland Security and Governmental Affairs of the Senate, on the Department's compliance with subtitle III of chapter 35 of title 44, United States Code. The information in such report shall be displayed in the aggregate and separately for each Administration, office, and facility of the Department.

New section 5723(c)(1) of the bill would require the Chief Information Officer to submit a report, at least once every month, to the Secretary noting any deficiency in the compliance with subtitle III of chapter 35 of title 44, United States Code, of the Department or any Administration, office, or facility of the Department.

New section 5723(c)(2) of the bill would require the Chief Information Officer to immediately report to the Secretary any significant deficiency in such compliance.

New section 5723(d)(1) of the bill would require the Chief Information Officer to immediately provide notice to the Secretary any data breach.

New section 5723(d)(2) of the bill would require the Secretary, after receiving notice of a date breach under paragraph (1), to pro-

vide notice of such breach to the Director of the Office of Management and Budget, the Inspector General of the Department, and, if appropriate, the Federal Trade Commission and the United States Secret Service.

New section 5723(e) of the bill would require the Secretary, when the budget for any fiscal year is submitted by the President to Congress under section 1105 of title 31, United States Code, to submit to Congress a report that identifies amounts requested for Department implementation and remediation of, and compliance with, this subchapter and subtitle III of chapter 35 of title 44, United States Code. The report shall set forth those amounts both for each Administration within the Department and for the Department in the aggregate and shall identify, for each such amount, how that amount is aligned with and supports such implementation and compliance.

New section 5724(a)(I) of the bill would require the Secretary to submit a report, not later than 30 days after the last day of a fiscal quarter, to the Committees on Veterans' Affairs of the Senate and the House of Representatives, on any data breach with respect to sensitive personal information processed or maintained by the Department that occurred during that quarter.

New section 5724(2) of the bill would require that each report submitted under paragraph (1) identify, for each data breach covered by the report, the Administration and facility of the Department responsible for processing or maintaining the sensitive personal information involved in the data breach.

New section 5724(b)(1) of the bill would require the Secretary, in the event of a data breach with respect to sensitive personal information and which the Secretary determines is significant, to provide notice to the Committees' on Veterans' Affairs of the Senate and House of Representatives.

New section 5724(b)(2) of the bill would require the Secretary, pursuant to paragraph (1), to provide prompt notice following the discovery of such a data breach and the implementation of any measures necessary to determine the scope of the breach, prevent any further breach or unauthorized disclosures, and reasonably restore the integrity of the data system.

New section 5725(a)(1) of the bill would require that, in the event of a data breach with respect to sensitive personal information that is processed or maintained by the Secretary, the Secretary shall ensure that, as soon as possible after the data breach, a non Department entity conducts an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach.

New section 5725(a)(2) of the bill would require the Secretary to provide credit protection services in accordance with section 5726 of title 38, United States Code, in the event of a data breach with respect to sensitive personal information that is processed or maintained by the Secretary.

New section 5725(b)(1) of the bill would require the Secretary to provide to an individual whose sensitive personal information is involved in a data breach, notice (A) in writing; or (B) by e-mail, if (i) the Department's primary method of communication with the in-

dividual is by email; and (ii) if the individual has consented to receive such notification.

New section 5725(b)(2) of the bill would provide that notice under paragraph (1) shall describe the circumstances of the data breach and the risk that the breach could lead to misuse, including identity theft, involving the sensitive personal information of the individual; describe the specific types of sensitive personal information that was compromised as a part of the data breach; describe the actions the Department is taking to remedy the data breach; inform the individual that the individual may require a fraud alert and credit security freeze under this section; clearly explain the advantages and disadvantages to the individual of receiving fraud alerts and credit security freezes under this section; and include other such information as the Secretary determines is appropriate.

New section 5725(b)(3) of the bill would require the notice under paragraph (1) to be provided promptly following the discovery of a data breach and the implementation of any measures necessary to determine the scope of the breach, prevent any further breach or unauthorized disclosures, and reasonably restore the integrity of the data system.

New section 5725(c) of the bill would require the Secretary to promptly report, with respect to sensitive personal information processed or maintained by the Secretary, to the Committees on Veterans' Affairs of the Senate and House of Representatives, findings of any independent risk analysis conducted under subsection (a)(1), any determination of the Secretary under subsection (a)(2), and a description of any credit protection services provided under section 5726 of title 38, United States Code.

New section 5725(d) of the bill would provide that, notwithstanding sections 511 and 7104(a) of title 38, United States Code, any determination of the Secretary under subsection (a)(2) with respect to the reasonable risk for the potential misuse of sensitive information involved in a data breach is final and conclusive and may not be reviewed by any other official, administrative body, or court, whether by an action in the nature of mandamus or otherwise.

New section 5725(e)(1) of the bill would require the Secretary, in the event of a data breach with respect to sensitive personal information that is processed or maintained by the Secretary, to arrange, upon the request of an individual whose sensitive personal information is involved in the breach to a principal credit reporting agency with which the Secretary has entered into a contract under section 5726(d) and at no cost to the individual, for the principal credit reporting agency to provide fraud alert services for that individual for a period of not less than one year, beginning on the date of such request, unless the individual requests that such fraud alert be removed before the end of such period, and the agency receives appropriate proof of the identity of the individual for such purpose.

New section 5725(e)(2) of the bill would require the Secretary to arrange for each principal credit reporting agency referred to in paragraph (2) to provide any alert requested under such subsection in the file of the individual along with any credit score generated in using that file, for a period of not less than one year, beginning on the date of such request, unless the individual requests that

such fraud alert be removed before the end of such period, and the agency receives appropriate proof of the identity of the individual for such purpose.

New section 5725(f)(1) of the bill would require the Secretary to arrange, in the event of a data breach with respect to sensitive personal information that is processed or maintained by the Secretary, upon request of an individual whose sensitive personal information is involved in the breach and at no cost to the individual, for each principal credit reporting agency to apply a security freeze to the file of that individual for a period not less than one year, beginning on the date of such request, unless the individual requests that such security freeze be removed before the end of such period, and the agency receives appropriate proof of the identity of the individual for such purpose.

New section 5725(f)(2) of the bill would require the Secretary to arrange for a principal credit reporting agency applying a security freeze under paragraph (1) to (A) send written confirmation of the security freeze to the individual within five business days of applying the freeze; (B) refer the information regarding the security freeze to other consumer reporting agencies; (C) provide the individual with a unique personal identification number or password to be used by the individual when providing authorization for the release of the individual's credit for a specific party or period of time; and (D) upon request of the individual, to temporarily lift the freeze for a period of time specified by the individual, beginning not later than three business days after the date on which the agency receives the request.

New section 5726(a) of the bill would provide credit protection services to a covered individual, who, for the purposes of this section, is an individual whose sensitive personal information is processed or maintained by the Department (or any third-party entity acting on behalf of the Department) whose sensitive personal information is involved, on or after August 1,2005, in a data breach for which the Secretary determines a reasonable risk exists for the potential misuse of sensitive personal information under section 5725(a)(2) of title 38, United States Code.

New section 5726(b)(1) of the bill would require the Secretary to provide, in writing, notification of credit protection services, in addition to any notice required under subsection 5725(b), to a covered individual that (A) the individual may request credit protection services under this section; (B) clearly explains the advantages and disadvantages to the individual of receiving credit protection services under this section; (C) includes a notice of which principal credit reporting agency the Secretary has entered into a contract with under subsection (d), and information about requesting services through that agency; (D) describes actions the individual can or should take to reduce the risk of identity theft; and (E) includes such other information as the Secretary determines is appropriate.

New section 5726(b)(2) of the bill would require that the required notice under paragraph (1) be made as promptly as possible and without reasonable delay following the discovery of a data breach for which the Secretary determines a reasonable risk exists for the potential misuse of sensitive personal information under section 5725(a)(2) of this title and the implementation of any measures necessary to determine the scope of the breach, prevent any further

breach or unauthorized disclosures, and reasonably restore the integrity of the data system.

New section 5726(b)(3) of the bill would require the Secretary to ensure that each notification under paragraph (1) includes a form or other means for readily requesting the credit protection services under this section. Such form or other means may include a telephone number, email address, or Internet website address.

New section 5726(c) of the bill would provide for the availability of services through other government agencies. If a service required under this section is available to a covered individual through another department or agency of the Government, the Secretary and the head of that department or agency may enter in to an agreement under which the head of that department or agency agrees to provide that service to the covered individual.

New section 5726(d) of the bill would require, subject to the availability of appropriations and not withstanding any other provision of law, that the Secretary shall enter into contracts or other agreements as necessary with one or more principal credit reporting agencies in order to ensure, in advance, the provision of credit protection services under this section and fraud alerts and security freezes under section 5725 of this title. Any such contract or agreement may include provisions for the Secretary to pay the expenses of such a credit reporting agency for the provision of such services.

New section 5726(e) of the bill would require the Secretary, upon request of the individual and at no cost to the individual, to provide data breach analysis for the individual for a period of not less than one year, beginning on the date of such request.

New section 5726(f) of the bill would require the Secretary to arrange, during the one-year period beginning on the date on which the Secretary notifies a covered individual that the individual's sensitive personal information is involved in a data breach, for the provision of credit monitoring services to the individual upon the request of the individual and without charge to the individual. Credit monitoring services under this subsection shall include: (1) one copy of the credit report of the individual every three months, (2) fraud resolution services for the individual, and (3) identity theft insurance in a coverage amount that does not exceed $30,000 in aggregate liability for the insured.

New section 5727(a) of the bill would require that if the Secretary enters into any contract for the performance of any Department function that requires access to sensitive personal information that (1) the contractor not, directly or through an affiliate of the contractor, disclose such information to any other person unless the disclosure is lawful and is expressly permitted under contract, and (2) the contractor or any subcontractor for a subcontract of the contract, promptly notify the Secretary of any data breach that occurs with respect to such information.

New section 5727(b) of the bill would require each contract subject to the requirements of subsection (a) to provide liquidated damages to be paid by the contractor to the Secretary in the event of a data breach with respect to any sensitive personal information processed or maintained by the contractor or any subcontractor under that contract.

New section 5727(c) of the bill would require any amount collected by the Secretary under subsection (b) be deposited in or

credited to the Department account from which the contractor is paid and remain available for obligation without fiscal year limitation exclusively for the purpose of providing credit protection services in accordance with section 5726 of title 38, United States Code.

New section 5728 of the bill would authorize such sums as may be necessary for each fiscal year to be appropriated to carry out this subchapter.

Section 4(b) of the bill would make clerical amendments.

Section 4(c) of the bill would require the Secretary of Veterans Affairs to publish regulations to carry out subchapter III of chapter 57, title 38, United States Code, as added by subsection (a), not later than 60 days after the enactment of this Act.

Section 5 of the bill would require the Secretary to submit to Congress a report containing the assessment of the Secretary on the feasibility of using personal identification numbers instead of Social Security numbers for the purpose of identifying individuals whose sensitive personal information, as defined in section 5721 of title 38, United States Code, is processed or maintained by the Secretary, not later than 180 days after enactment of this Act.

Section 6(a)(1) of the bill would require the President to nominate an individual to serve as Under Secretary for Information Services under section 307A of title 38, United States Code, not later than 180 days after enactment of this Act.

New section 6(a)(2) of the bill would require the Secretary of Veterans Affairs to appoint an individual to serve as each of the Deputy Under Secretaries of Veterans Affairs for Information Services under section 5722 of title 38, United States Code, not later than 180 days after enactment of this Act.

New section 6(b) of the bill would require the Secretary of Veterans Affairs to submit to Congress a report describing the progress of appointments described in subsection (a), not later than 30 days after enactment of this Act, and every 30 days after until the appointments are made.

Section 7(a) of the bill would add a new chapter 79, "Information Security Education Assistance Program," to title 38, United States Code. The following sections would be added to title 38, United States Code.

New section 7901(a) of the bill would require the Secretary to provide financial support for education in computer science, and electrical and computer engineering at accredited institutions of higher education to encourage the recruitment and retention of personnel who have information security skills necessary to meet the Department's needs.

New section 7901(b) of the bill would authorize programs for scholarships for the pursuit of doctoral degrees in computer science, and electrical and computer engineering from accredited institutions of higher education or education debt reduction for Department personnel who hold doctoral degrees in computer science, or electrical and computer engineering from accredited institutions of higher education.

New section 7902(a)(1) of the bill would require the Secretary to establish a scholarship program, subject to the availability of appropriations, to provide financial assistance to individuals who are pursuing a doctoral degree in computer science, and electrical and computer engineering at accredited institutions of higher education

and enter into an agreement with the Secretary as described in the new subsection 7902(b).

New section 7902(a)(2) of the bill would allow the Secretary to provide the scholarship to an individual for up to five years unless the Secretary determines that a waiver is necessary.

New section 7902(a)(3) of the bill would allow the Secretary to award up to five scholarships per academic year to individuals who did not receive the scholarship the preceding year. One of the five scholarships each year may be awarded to a current VA employee.

New section 7902(b) of the bill would require any individual who receives financial assistance from the scholarship to enter into an agreement to accept and continue employment with VA for a period of obligated service to be determined by the Secretary that would not be less than 2 years of service for every one year of financial assistance. The period of obligated service would begin on a date after the individual receives a degree. The individual would be required to maintain a satisfactory academic progress, as determined by the Secretary, or the assistance would be terminated. The Secretary would have the authority to determine any other appropriate terms and conditions for carrying out the scholarship.

New section 7902(c) of the bill would allow the amount of financial assistance under the scholarship program to not exceed $50,000 per academic year or a total amount of assistance of $200,000. The scholarship would be used for tuition and fees of the individual and $1500 would be awarded to the individual each month the individual is pursuing a course of study, independent research and between semesters for books, laboratory expenses, and room and board. The assistance awarded under this new section would not be considered as income or resources when determining eligibility for and Federal or federally assisted programs.

New section 7902(d) of the bill would require any individual who receives the scholarship to repay the Secretary if the individual fails to satisfy the requirements of the service agreement entered into with the Secretary according to subsection 7902(b). The Secretary would be authorized to make regulations with regard to the repayment policy of the scholarship. The repayment obligation would be a debt owed to the United States and a discharge in bankruptcy under title 11, United States Code, would not discharge the individual's debt if the debt is entered into in less than five years after the termination of the agreement of contract.

New section 7902(e) of the bill would require the Secretary to prescribe regulations for a waiver or suspension policy for service or payment if the Secretary determines the individual is noncompliant due to circumstances beyond their control.

New section 7902(f) of the bill would authorize the Secretary to offer compensated internships to individuals receiving the scholarship between semesters. Any internship performed would not count towards obligated service.

New section 7902(g) of the bill would prohibit any individual who receives education benefits under chapters 30, 31, 32, 34, or 35 of title 38, United States Code, or from 1606 or 1607 of title 10, United States Code, to receive the scholarship.

New section 7903(a)(1) of the bill would require the Secretary to establish a debt reduction program, subject to the availability of appropriations, to provide financial assistance to individuals who

received a doctoral degree in computer science, and electrical and computer engineering at accredited institutions of higher education for the individuals to make payments to the principal and interest on loans described in 7903(b).

New section 7903(a)(2) of the bill would allow the Secretary to accept up to five individuals into the program per year who did not receive a payment the preceding year. One of the five scholarships each year may be awarded to a current VA employee.

New section 7903(b) of the bill would require any individual who participates in the program to have completed a doctoral degree in computer science, and electrical and computer engineering at accredited institutions of higher education during the five years preceding the date the individual is hired, be an employee in a position related to information security, and owes principal or interest on a loan which was used to pay the costs of achieving the doctoral degree.

New section 7903(c) of the bill would limit the amount of financial assistance under the scholarship program to $16,500 per year or a total amount of assistance of $82,500 over 5 years. The total amount paid to the individual would not exceed the amount of principal and interest on the loans that the individual pays during the year.

New section 7309(d) of the bill would require the Secretary to make the debt reduction payments on an annual basis on the last day of the one-year period beginning on the date the individual was accepted into the program, or if the individual received the payment the previous year, the individual would receive the payment on the last day of the one-year period beginning on the date of the last payment. The assistance awarded under this new section would not be considered as income or resources when determining eligibility for federal or federally assisted programs.

New section 7309(e) of the bill would authorize the Secretary to make payments under the debt reduction program to an individual only if the individual maintains an acceptable level of performance in the position or positions during the year after acceptance in the program.

New section 7309(f) of the bill would require the Secretary to notify any individual accepted into the debt reduction program of the terms and conditions of the program in writing.

New section 7309(g) of the bill would authorize payment to individuals accepted into the debt reduction program for loans associated with tuition expenses and all other reasonable educational expenses, including fees, books, and laboratory expenses.

New section 7904 of the bill would require the Secretary to give preference for the financial assistance programs to qualified individuals who are: service-disabled veterans; veterans; surviving spouses of veterans who have died of a service-connected disability, or spouses of veterans who are 100 percent permanently and totally disabled; individuals who have received or are pursuing a degree at a Center of Academic Excellence in Information Assurance Education; or citizens of the United States.

New section 7905 of the bill would require that any veteran who receives financial assistance through this new chapter 79 of title 38, United States Code be discharged from the Armed Forces under honorable conditions.

New section 7906 would require the Secretary to prescribe regulations for the new chapter 79 of title 38, United States Code.

New section 7907 of the bill would terminate the new financial assistance programs on July 31, 2017.

New section 7(b) of the bill would require the Comptroller General to submit a report to Congress on the scholarship and debt reduction programs under the new chapter 79 of title 39, United States Code no later than 3 years after date of enactment.

New section 7(c) of the bill would require scholarship payments under the new chapter 79 of title 38, United States Code to apply to academic semesters or terms beginning on or after August 31, 2007.

New section 7(d) of the bill would make clerical amendments.

LETTERS REGARDING JURISDICTION OF THE COMMITTEE ON GOVERNMENT REFORM

TOM DAVIS, VIRGINIA,
CHAIRMAN

CHRISTOPHER SHAYS, CONNECTICUT
DAN BURTON, INDIANA
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. McHUGH, NEW YORK
JOHN L. MICA, FLORIDA
GIL GUTKNECHT, MINNESOTA
MARK E. SOUDER, INDIANA
STEVEN C. LaTOURRETTE, OHIO
TODD RUSSELL PLATTS, PENNSYLVANIA
CHRIS CANNON, UTAH
JOHN J. DUNCAN, JR., TENNESSEE
CANDICE MILLER, MICHIGAN
MICHAEL R. TURNER, OHIO
DARRELL ISSA, CALIFORNIA
JON C. PORTER, NEVADA
KENNY MARCHANT, TEXAS
LYNN A. WESTMORELAND, GEORGIA
PATRICK T. McHENRY, NORTH CAROLINA
CHARLES W. DENT, PENNSYLVANIA
VIRGINIA FOXX, NORTH CAROLINA
JEAN SCHMIDT, OHIO
VACANCY

ONE HUNDRED NINTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
FACSIMILE (202) 225–3974
MINORITY (202) 225–5051
TTY (202) 225–6852

http://reform.house.gov

HENRY A. WAXMAN, CALIFORNIA,
RANKING MINORITY MEMBER

TOM LANTOS, CALIFORNIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
CAROLYN B. MALONEY, NEW YORK
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
DANNY K. DAVIS, ILLINOIS
WM. LACY CLAY, MISSOURI
DIANE E. WATSON, CALIFORNIA
STEPHEN F. LYNCH, MASSACHUSETTS
CHRIS VAN HOLLEN, MARYLAND
LINDA T. SANCHEZ, CALIFORNIA
C.A. DUTCH RUPPERSBERGER, MARYLAND
BRIAN HIGGINS, NEW YORK
ELEANOR HOLMES NORTON, DISTRICT OF COLUMBIA

BERNARD SANDERS, VERMONT,
INDEPENDENT

September 12, 2006

The Honorable Steve Buyer
Chairman
House Committee on Veterans Affairs
335 Cannon House Office Building
Washington, D.C. 20515

Dear Mr. ~~Chairman~~: Steve

On July 20, 2006, the House Veterans' Affairs Committee reported H.R. 5835, the "Veterans Identity and Credit Security Act of 2006." As you know, the bill includes provisions within the jurisdiction of the Committee on Government Reform including Section 2 of the bill regarding federal agency data breach notification amendments under the Federal Information Security Management Act (FISMA).

In the interest of moving this important legislation forward, I agreed to waive sequential consideration of this bill by the Committee on Government Reform. However, I do so only with the understanding that this procedural route would not be construed to prejudice the Committee on Government Reform's jurisdictional interest and prerogatives on this bill or any other similar legislation. I understand this will not be considered as precedent for consideration of matters of jurisdictional interest to my Committee in the future.

I respectfully request your support for the appointment of outside conferees from the Committee on Government Reform should this bill or a similar bill be considered in a conference with the Senate. Finally, I request that you include this letter and your response in the *Congressional Record* during consideration of the legislation on the House floor.

Thank you for your attention to these matters.

Sincerely,

Tom Davis

cc: The Honorable J. Dennis Hastert, Speaker
The Honorable Henry A. Waxman, Ranking Member
The Honorable John V. Sullivan, Parliamentarian

REPUBLICANS

STEVE BUYER, INDIANA, CHAIRMAN

MICHAEL BILIRAKIS, FLORIDA
TERRY EVERETT, ALABAMA
CLIFF STEARNS, FLORIDA
DAN BURTON, INDIANA
JERRY MORAN, KANSAS
RICHARD H. BAKER, LOUISIANA
HENRY E. BROWN, Jr., SOUTH CAROLINA
JEFF MILLER, FLORIDA
JOHN BOOZMAN, ARKANSAS
JEB BRADLEY, NEW HAMPSHIRE
GINNY BROWN-WAITE, FLORIDA
MICHAEL R. TURNER, OHIO
JOHN CAMPBELL, CALIFORNIA
BRIAN P. BILBRAY, CALIFORNIA

JAMES M. LARIVIERE
STAFF DIRECTOR

U.S. House of Representatives

COMMITTEE ON VETERANS' AFFAIRS

ONE HUNDRED NINTH CONGRESS
335 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
http://veterans.house.gov

DEMOCRATS

LANE EVANS, ILLINOIS, RANKING

BOB FILNER, CALIFORNIA
LUIS V. GUTIERREZ, ILLINOIS
CORRINE BROWN, FLORIDA
VIC SNYDER, ARKANSAS
MICHAEL H. MICHAUD, MAINE
STEPHANIE HERSETH, SOUTH DAKOTA
TED STRICKLAND, OHIO
DARLENE HOOLEY, OREGON
SILVESTRE REYES, TEXAS
SHELLEY BERKLEY, NEVADA
TOM UDALL, NEW MEXICO
JOHN T. SALAZAR, COLORADO

JAMES H. HOLLEY
DEMOCRATIC STAFF DIRECTOR

September 12, 2006

The Honorable Tom Davis
Chairman
House Committee on Government Reform
2157 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Davis:

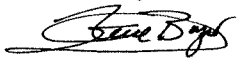
I am writing regarding your committee's jurisdictional interest in H.R. 5835, the Veterans Identity and Credit Security Act of 2006, and would appreciate your cooperation in waiving consideration of the bill by the Committee on Government Reform in order to allow expedited consideration of the legislation next week under suspension of the rules.

I acknowledge your committee's jurisdictional interest in section 2 of H.R. 5835, as ordered reported by the Committee on Veterans' Affairs. Any decision by the Committee on Government Reform to forego further action on the bill will not prejudice the Committee on Government Reform with respect to its jurisdictional prerogatives on this or similar legislation. I will support your request for an appropriate number of conferees should there be a House-Senate conference on this or similar legislation.

Finally, I will include a copy of this letter and your response in the *Congressional Record* when the legislation is considered by the House.

Thank you for your assistance.

Sincerely,



Steve Buyer
Chairman

cc: The Honorable J. Dennis Hastert, Speaker
The Honorable Lane Evans, Ranking Member
The Honorable Bob Filner, Acting Ranking Member
The Honorable Henry A. Waxman, Ranking Member, HCGR
The Honorable John V. Sullivan, Parliamentarian

PERFORMANCE GOALS AND OBJECTIVES

The reported bill would establish the position of Under Secretary for Information Services, and would provide for an Office of Information Services within the Department of Veterans Affairs. It would strengthen the Federal Information Security Management Act of 2002, to provide the Department's Chief Information Officer improved enforcement authority over information management, and require certain notification and credit services for veterans affected by data breaches. Performance goals and objectives are established in VA's annual performance plans and are subject to the Committee's regular oversight. In addition, the Committee on Government Reform conducts regular oversight of the Department's conformance with FISMA regulations.

STATEMENTS OF THE VIEWS OF THE ADMINISTRATION

STATEMENT OF HON. GORDON H. MANSFIELD, DEPUTY SECRETARY, DEPARTMENT OF VETERANS AFFAIRS

Mr. Chairman and Members of the Committee,

I am pleased to provide the Department's views on eight bills, all intended to protect the personal privacy of veterans and others affected by the May 3, 2006 theft of computer equipment containing veterans' personal data. While you had also invited our views on a draft bill your staff shared last week, I regret that time has not permitted us have cleared positions on its many provisions. We will supply those for the record once the necessary executive-branch coordination is completed.

Initially, I wish to point out that the eight bills covered in my testimony were introduced before the stolen computer hardware was recovered. As you know, the FBI has concluded with a high degree of confidence that, based upon its forensic examination and other evidence developed during its investigation, the veterans data were not accessed or compromised prior to their recovery. That development has eliminated the need for much of what is proposed in the legislation, and while we understand the concerns that engendered these eight bills we do not support their enactment.

H.R. 5455

H.R. 5455, the "Veterans Identity Protection Act of 2006," would require the Department of Veterans Affairs to: (1) provide notification to each individual whose personal' information was included in the recent data breach; (2) provide to any of these individuals a free one-year credit monitoring service; (3) provide a copy of that individual's credit report once annually during the two year period following the termination of the credit monitoring services; and (4) certify in writing to Congress that any individual whose personal information has been compromised due to data security lapses at the Department has been appropriately notified in writing.

The Secretary has already taken proactive and aggressive steps to notify all individuals whose personal information was potentially at risk as a result of the May 3 data theft, Also, the recovery of the data, apparently uncompromised, eliminates the need to offer credit monitoring or additional free credit reports at this time.

In addition, the Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 et seq., requires each of the three major credit bureaus to provide, upon request, a free copy of an individual's credit report once every twelve months and upon the individual's placement of an initial fraud alert on his or her credit file. Therefore, an individual who places an initial fraud alert could make a request to each of the three credit bureaus and receive up to six free credit reports annually. The Department's website at *http://www.va.gov*. documents the actions taken by the Secretary in this regard and advises veterans how to place a fraud alert with, and obtain free credit reports from, the credit bureaus. For these reasons, H.R. 5455 is unnecessary.

H.R. 5464

H.R. 5464, the "Veterans Identity Protection Act," would require VA to: (1) provide detailed notification to each veteran whose personal information was included in the data breach; and (2) include a form for the veteran to elect to receive a free credit report once every three months for the year following notification and free credit monitoring for that year also. The bill also would limit the funds available to Office of the Secretary to 90 percent of the funds otherwise available if the 16 information security recommendations of VA's Inspector General are not fully implemented by January 1, 2007. The bill would limit the funds otherwise available to the Office of the Secretary by 10 percent in subsequent fiscal years, after January 1, 2007, for any information security recommendation not fully implemented.

VA supports the underlying intent of H.R. 5464, but cannot support the bill. In addition to the actions already discussed, VA is taking steps to implement the 16 information security recommendations. The Secretary has established an Information Security Task Force composed of senior officials and has hired a Special Advisor on Information Security. Working together with the Chief Information Officer of the Department, these individuals will implement the recommendations. For these reasons, we believe that H.R. 5464 too is unnecessary.

H.R. 5467

H.R. 5467, the "Veterans Identity Security Act of 2006," would establish criminal penalties for knowingly disclosing without authorization records containing personal information about veterans. The bill would amend title 38, United States Code, by adding a new section 5706 applicable to officers, employees, contractors, and volunteers of the Department who disclose personal information without lawful

authorization. The bill defines personal information as "name, date of birth, address, phone number, Social Security number, and (if applicable) disability rating." Penalties range from fines to imprisonment for up ten years when there is intent to sell, transfer, or use the personal information for commercial advantage, personal gain or malicious harm.

VA has no objection to the intent of H.R. 5467 but has several technical suggestions for improving its drafting and coverage. We would be happy to discuss these with Committee staff at its convenience.

H.R. 5487

H.R. 5487, the "Veterans' ID Theft Protection Act of 2006," would also require VA to notify any person affected by the breach, but also to notify consumer reporting agencies and appropriate third parties who may be required to act in a manner to further protect affected persons from fraud or identity theft. The notice specifications must include details of the breach, current safeguards of personal information, contact information for the Department, information provided by the Federal Trade Commission (FTC) regarding identity theft, information on obtaining a copy of a consumer's credit report free of charge and other information regarding placing a fraud alert on one's file and contact information for the FTC. The bill also would require the Department to offer affected persons free credit monitoring service, at their request, for not less than six months, and to take prompt and reasonable measures to repair the data breach that would improve the data security policies and procedures.

For reasons already discussed, H.R. 5487 is unnecessary.

H.R. 5490

H.R. 5490, the "Veterans Identification Protection Act," would require the Department of Veterans Affairs to: (1) provide a four-digit personal identification number (PIN) for each veteran who receives or applies for VA benefits, and (2) take steps to provide that any entity entering into a commercial transaction with a veteran that "includes the extension to the veteran of credit, a loan, or any other thing of value" shall verify the veteran's identity through the PIN established. Any entity that is required to so verify a veteran's identity, but fails to, would be liable to that individual for all attorney fees and injuries incurred by that individual resulting from that failure.

VA does not support H.R. 5490. VA understands that the current level of security as recommended by the National Institute of Standards and Technology and other security experts requires a PIN number with more than four digits. However, even if the bill were amended in this regard, VA would be opposed to the requirement that the Secretary provide, assign, monitor, or validate any universal PIN number exclusively for the use of veterans in commercial enterprises. The bill is unclear about the commercial en-

terprises to be covered. For example, there is no distinction made between commercial activities with a VA involvement (such as a home loan guarantee) and other commercial activities a veteran may be involved with that have no VA connection.

H.R. 5577

H.R. 5577, the "Veterans Identity Protection Act of 2006," is intended to enhance the protection from disclosure of VA records containing personal identifying information that is required by law to be confidential and privileged.

It would require the Department to establish an Office of Identity Protection, administered by a Director who shall be appointed by the Secretary. The Office would notify each individual whose personal information has been lost or compromised, provide him or her with one credit report every six months for three years at no charge, offer a 24-hour toll-free telephone number and a web site to provide information regarding credit reporting services, ensure that active-duty military personnel have access to credit reporting services, make information available on possible fraudulent consumer credit or reporting services that may be targeted at affected veterans and service members and notify the Department of Justice and the FTC immediately when personal data in VA records may have been compromised. Furthermore, the Act would require the VA Inspector General (IG) to conduct a study of the data-security practices at VA and submit a report not later than six months after the date of the law's enactment to the Senate and House Committees on Veterans' Affairs. Finally the Act would impose criminal penalties of a fine or imprisonment on any VA employee who removes records from VA custody without proper authorization.

VA supports the underlying purposes of H.R. 5577, but cannot support the bill. In addition to the ameliorative actions already discussed, VA has provided a toll-free telephone number and a section on the Department's web site with information for those individuals seeking assistance, and established an Information Security Task Force to improve data security. While the Information Security Task Force will consider administrative alignments to enhance data security protections, there does not appear to be a need for a separate administrative Office of Identity Protection at this time. And, as already noted, FCRA already provides up to three free credit reports annually, and up to another three annually when an initial fraud alert is placed. For these reasons, we do not believe that these provisions are necessary.

The requirement for the VA IG to report on the Department's progress in implementing data security improvements within six months after the law's enactment would not allow sufficient time for the Department to address corrective actions before the report must be submitted. Furthermore, the VA Inspector General regularly issues

reports about data security practices within VA in Federal Information Security Management Act (FISMA) audits and consolidated financial statement audits performed annually. There does not appear to be a need for additional reports in this area.

In addition, the criminal penalty provision is not sufficiently specific for enforcement purposes. In particular, the bill does not specify whether "remove from the custody of VA," refers to removal from the "custody of a VA employee" or any removal from a "VA worksite." H.R. 5577 also does not consider the reality that files leave the worksite every day for legitimate purposes, nor does it identify the specific part of title 18 that would provide for the fines imposed for such action. We could support enactment of the additional criminal penalties in H.R. 5467 if those provisions were amended as discussed above.

H.R. 5588

H.R. 5588, the "Comprehensive Veterans" Data Protection and Identity Theft Prevention Act of 2006," would require the Secretary of Veterans Affairs to: (1) issue policies and procedures to safeguard sensitive personal information before the end of the 90-day period beginning on the date of the enactment of the Act; (2) notify the Secret Service, VA IG, Senate and House Committees on Veterans' Affairs, the FTC, and the affected individual of any breach: (3) place fraud alerts or security freezes in the credit file of affected individuals; (4) provide affected individuals with credit monitoring services; and (5) establish the position of an Ombudsman for Data Security within the Department to provide information and assistance to such individuals.

In light of the ameliorative actions outlined above, VA does not believe that H.R. 5588 is necessary and does not support enactment.

H.R. 5636

H.R. 5636, the "Social Security Numbers Privacy and Protection Act," would require: (1) the alteration of selective service reminder mailback cards; and (2) the elimination and prohibition of social security account numbers from Medicare, Medicaid, and SCHIP- and VA-issued health care identification cards by the end of the two-year period after the enactment of the Act.

VA supports alternative methods for the identification of veterans for the purpose of providing health care or other benefits available under Title 38. To that end, VA has already removed the social security numbers from the Veterans Identification Cards known as VIC cards and is therefore already in compliance with the bill. With respect to Medicare, Medicaid, and SCHIP programs, the Department of Health and Human Services advises us that instituting a new number for use on the identity cards used for these programs would entail substantial expense and require a substantially longer time than allowed by the bill.

They are continuing to work on these efforts. Therefore, we believe that enactment of H.R. 5636 would not be productive.

CONCLUSION

As I have indicated, VA already has implemented many of the provisions of the various bills that provide, among other things, stronger safeguards to protect against data breaches within the Department. VA is strongly committed to providing all available protections to the safety and security of personal information of all veterans' and their beneficiaries. As we continue to work on improvements in our systems and procedures, we will be pleased to work with your Committee in fostering methods to achieve a level of information security that is responsible and necessary.

CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

The following letter was received from the Congressional Budget Office concerning the cost of the reported bill:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, July 28, 2006.

Hon. STEVE BUYER,
Chairman, Committee on Veterans' Affairs,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 5835, the Veterans Identity and Credit Security Act of 2006.

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

Sincerely,

DONALD B. MARRON,
Acting Director.

Enclosure.

H.R. 5835—Veterans Identity and Credit Security Act of 2006

Summary: H.R. 5835 would create a new Office of the Under Secretary for Information Services within the Department of Veterans Affairs (VA). The bill also would require VA to notify affected individuals when sensitive, personal information held by VA is lost, stolen, or otherwise compromised. Additionally, if the Secretary of VA determines there is a risk that the compromised information could be used in a criminal manner, VA would be required to provide services to alleviate any loss those individuals might suffer. Furthermore, H.R. 5835 would require contractors to pay damages to VA if the compromised information was under the contractors' control and would allow VA to spend those receipts without further appropriation action. Finally, the bill would allow VA to provide scholarships and pay school debts for individuals pursuing a doctoral degree in computer science or related fields who agree to work for VA.

CBO estimates that implementing H.R. 5835 would cost $5 million in 2007 and about $50 million over the 2007–2011 period, assuming appropriation of the estimated amounts. However, if VA were to experience another data breach similar to the recent incident involving personal information on 17 million individuals, the cost could be as much as $1 billion. Under the bill, VA would be authorized to collect and spend certain receipts, but CBO estimates that the net effect of those receipts on the federal budget would be insignificant.

H.R. 5835 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. 5835 is shown in the following table. The costs of this legislation fall within budget function 700 (veterans benefits and services).

	By fiscal year, in millions of dollars—					
	2006	2007	2008	2009	2010	2011
CHANGES IN SPENDING SUBJECT TO APPROPRIATION						
Credit-Protection Services:						
Estimated Authorization Level	0	9	10	10	10	11
Estimated Outlays	0	5	9	10	10	11
Scholarships and Debt Reduction:						
Estimated Authorization Level	0	(*)	1	1	1	1
Estimated Outlays	0	(*)	1	1	1	1
Total Changes in Spending Under H.R. 5835:						
Estimated Authorization Level	0	9	11	11	11	12
Estimated Outlays	0	5	10	11	11	12

Note.—* = less than $500,000.

Basis of estimate: For the purposes of this estimate, CBO assumes that the bill will be enacted near the start of fiscal year 2007 and that the estimated amounts will be appropriated for each year.

Spending subject to appropriation

Assuming appropriation of the estimated amounts, implementing H.R. 5835 would cost $5 million in 2007 and about $50 million over the 2007–2011 period, CBO estimates. This spending would be for credit-protection services for certain veterans and for scholarships and debt-reduction grants provided to current and future VA employees.

Credit-Protection Services. H.R. 4835 would require VA to notify individuals and provide them with certain services when their sensitive, personal information is lost, stolen, or otherwise compromised, while in VA's possession. All of those services would be provided at no cost to those individuals. Initially, VA would have to:

- Notify all affected individuals of the lost or compromised data,
- Inform those individuals of the steps VA is taking to remedy the problem,
- Explain to each individual the advantages and disadvantages of requesting a fraud alert and a credit security freeze from the major credit-reporting agencies, and

- Contract with the credit-reporting agencies to implement a security freeze of the file of each affected individual who requests it.

If the Secretary of VA determines there is a reasonable risk that the compromised data could be misused, the department would have to provide an additional notification detailing the availability of credit-protection services. Under the bill, VA would contract with one of the principal credit-reporting agencies to provide affected individuals credit-protection services that include:

- A credit report every three months,
- Services to assist in rehabilitating the individual's credit in the event of identity theft, and
- Identity theft insurance of up to $30,000 that would cover the damages of identity theft, including travel costs, legal fees, and lost wages.

Based on publicly available information on the recent loss of personal information by government agencies (including VA), CBO estimates that VA could be expected to experience an average of three incidents a year in which sensitive, personal information is compromised in some manner. Excluding the incident that occurred on May 3, 2006, when a computer with information on more than 17 million people was stolen, the average number of people affected by a data breach has been about 50,000. Based on information from VA, CBO expects that the cost of notifying individuals in the event of such data breaches would generally be less than $500,000 a year.

Using information from a Federal Trade Commission survey report on identity theft, CBO estimates that 10 percent to 15 percent of those individuals who have their personal information compromised might have problems with identity theft and experience a loss. CBO estimates that, in 2007, such a loss would, on average, amount to about $450. Thus, CBO estimates that requiring VA to provide insurance and fraud-resolution services to individuals who have had their personal information compromised would cost about $10 million a year, on average, assuming appropriation of the necessary amounts. CBO projects that outlays would be $5 million in 2007 and about $45 million over the 2007–2011 period. (If VA were to experience another data breach where information for more than 17 million people were to be compromised, the cost for such an incident could be as high as $1 billion.)

Scholarship and Debt Reduction. H.R. 5835 also would establish programs that would improve VA's ability to recruit employees with skills in information security. The bill would allow VA to pay tuition, fees, and a monthly stipend of $1,500 for individuals who are pursuing a doctoral degree in computer science or a related field. Under the bill, VA could provide the assistance for up to five years if those individuals agreed to work at VA for twice as long as they received such assistance. VA could offer up to five new scholarships each year and could provide up to $50,000 a year or $200,000 per scholarship for each individual.

In addition, H.R. 5835 would allow VA to establish an education debt-reduction program as a recruitment tool to attract individuals who completed a doctoral program in computer science or a related field within the previous five years. The bill would allow VA to pay up to $16,500 a year for five years to eligible employees for repay-

ment of loans related to their doctoral degree. VA would be authorized to make such payments to an additional five individuals each year.

Based on the amounts specified in the bill, CBO estimates that implementing these provisions would cost less than $500,000 in 2007 and about $4 million over the 2007–2011 period, assuming appropriation of the necessary amounts.

Direct spending

Section 4 of the bill would require that VA contractors who have access to sensitive personal information pay damages to VA in the event the personal data is compromised. Damages paid to VA would be credited to the appropriation account under which the contract was paid and would be available without fiscal year limitation to pay for credit-protection services. Because VA would be able to spend the funds collected under this section, CBO estimates that enacting the bill would have no significant net effect on direct spending in any year over the 2007–2016 period.

Intergovernmental and private-sector impact: H.R. 5835 contains no intergovernmental or private-sector mandates as defined in UMRA and would not affect the budgets of state, local, or tribal governments.

Estimated prepared by: Federal Costs: Sam Papenfuss. Impact on State, Local, and Tribal Governments: Melissa Merrell. Impact on the Private Sector: Allison Percy.

Estimate approved by: Robert A. Sunshine, Assistant Director for Budget Analysis.

STATEMENT OF FEDERAL MANDATES

The preceding Congressional Budget Office (CBO) cost estimate states that H.R. 5835, as amended, does not contain any intergovernmental and private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA), Public Law 104–4.

STATEMENT OF CONSTITUTIONAL AUTHORITY

Pursuant to Article I, section 8 of the United States Constitution, the reported bill is authorized by Congress' power to "provide for the common Defense and general Welfare of the United States."

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):

CHAPTER 35 OF 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 "sensitive personal information" means any information contained in a record, as defined in section 552a(4) of title 5.

* * * * * * *

§ 3543. Authority and functions of the Director

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

(1) * * *

* * * * * * *

(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) * * *

* * * * * * *

(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*

(9) establishing policies, procedures, and standards for agencies to follow in the event of a breach of data security involving the disclosure of sensitive personal information in violation of section 552a of title 5, including a requirement for timely notice to be given to those individuals whose sensitive personal 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 of identity theft, fraud, or other unlawful conduct regarding such individual.

* * * * * * *

§ 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) * * *

* * * * * * *

(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) * * *

* * * * * * *

(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**[**.**]***; and*

(9) procedures for notifying individuals whose sensitive personal information is compromised consistent with policies, procedures, and standards established under section 3543(a)(9) of this title.

* * * * * * *

TITLE 38, UNITED STATES CODE

* * * * * * *

PART I—GENERAL PROVISIONS

Chapter		Sec.
1.	General	101

* * * * * * *

PART V—BOARDS, ADMINISTRATIONS, AND SERVICES

71.	Board of Veterans' Appeals	7101

* * * * * * *

79.	*Information Security Education Assistance Program*	*7901*

* * * * * * *

PART I—GENERAL PROVISIONS

* * * * * * *

CHAPTER 3—DEPARTMENT OF VETERANS AFFAIRS

Sec.
301. Department.

* * * * * * *

307A. Under Secretary for Information Services.

* * * * * * *

§ 307A. Under Secretary for Information Services

(a) UNDER SECRETARY.—There is in the Department an Under Secretary for Information Services, who is appointed by the President, by and with the advice and consent of the Senate. The Under Secretary shall be the head of the Office of Information Services and shall perform such functions as the Secretary shall prescribe.

(b) SERVICE AS CHIEF INFORMATION OFFICER.—Notwithstanding any other provision of law, the Under Secretary for Information Services shall serve as the Chief Information Officer of the Department under section 310 of this title.

§ 308. Assistant Secretaries; Deputy Assistant Secretaries

(a) * * *

(b) The Secretary shall assign to the Assistant Secretaries responsibility for the administration of such functions and duties as the Secretary considers appropriate, including the following functions:

(1) * * *

* * * * * * *

[(5) Information management functions as required by section 3506 of title 44.**]**

[(6)**]** *(5)* Capital facilities and real property program functions.

[(7)**]** *(6)* Equal opportunity functions.

[(8)**]** *(7)* Functions regarding the investigation of complaints of employment discrimination within the Department.

[(9)**]** *(8)* Functions regarding intergovernmental, public, and consumer information and affairs.

[(10)**]** *(9)* Procurement functions.

[(11)**]** *(10)* Operations, preparedness, security, and law enforcement functions.

* * * * * * *

PART IV—GENERAL ADMINISTRATIVE PROVISIONS

* * * * * * *

CHAPTER 57—RECORDS AND INVESTIGATIONS

SUBCHAPTER I —RECORDS

Sec.
5701. Confidential nature of claims.

* * * * * * *

SUBCHAPTER III—INFORMATION SECURITY

5721. Definitions.
5722. Office of the Under Secretary for Information Services.
5723. Information security management.
5724. Congressional reporting and notification of data breaches.
5725. Data breaches.
5726. Provision of credit protection services.
5727. Contracts for data processing or maintenance.
5728. Authorization of appropriations.

* * * * * * *

SUBCHAPTER III—INFORMATION SECURITY

§ 5721. Definitions

For the purposes of this subchapter:

(1) The term "sensitive personal information" means the name, address, or telephone number of an individual, in combination with any of the following:

(A) The Social Security number of the individual.

(B) The date of birth of the individual.

(C) Any information not available as part of the public record regarding the individual's military service or health.

(D) Any financial account or other financial information relating to the individual.

(E) The driver's license number or equivalent State identification number of the individual.

(F) The deoxyribonucleic acid profile or other unique biometric data of the individual, including the fingerprint, voice print, retina or iris image, or other unique physical representation of the individual.

(2) The term "data breach" means the loss, theft, or other unauthorized access to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data.

(3) The term "data breach analysis" means the identification of any misuse of sensitive personal information involved in a data breach.

(4) The term "fraud resolution services" means services to assist an individual in the process of recovering and rehabilitating the credit of the individual after the individual experiences identity theft.

(5) The term "identity theft" has the meaning given such term under section 603 of the Fair Credit Reporting Act (15 U.S.C. 1681a).

(6) The term "identity theft insurance" means any insurance policy that pays benefits for costs, including travel costs, notary fees, and postage costs, lost wages, and legal fees and expenses associated with the identity theft of the insured individual.

(7) The term "principal credit reporting agency" means a consumer reporting agency as described in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)).

§ 5722. Office of the Under Secretary for Information Services

(a) DEPUTY UNDER SECRETARIES.—The Office of the Under Secretary for Information Services shall consist of the following:

(1) The Deputy Under Secretary for Information Services for Security, who shall serve as the Senior Information Security Officer of the Department.

(2) The Deputy Under Secretary for Information Services for Operations and Management.

(3) The Deputy Under Secretary for Information Services for Policy and Planning.

(b) APPOINTMENTS.—Appointments under subsection (a) shall be made by the Secretary, notwithstanding the limitations of section 709 of this title.

(c) QUALIFICATIONS.—At least one of positions established and filled under subsection (a) shall be filled by an individual who has at least five years of continuous service in the Federal civil service in the executive branch immediately preceding the appointment of the individual as a Deputy Under Secretary. For purposes of determining such continuous service of an individual, there shall be excluded any service by such individual in a position—

(1) of a confidential, policy-determining, policy-making, or policy-advocating character;

(2) in which such individual served as a noncareer appointee in the Senior Executive Service, as such term is defined in section 3132(a)(7) of title 5; or

(3) to which such individual was appointed by the President.

§ 5723. Information security management

(a) RESPONSIBILITIES OF CHIEF INFORMATION OFFICER.—To support the economical, efficient, and effective execution of subtitle III of chapter 35 of title 44, and policies and plans of the Department, the Secretary shall ensure that the Chief Information Officer of the Department has the authority and control necessary to develop, approve, implement, integrate, and oversee the policies, procedures, processes, activities, and systems of the Department relating to that subtitle, including the management of all related mission applications, information resources, personnel, and infrastructure.

(b) ANNUAL COMPLIANCE REPORT.—Not later than March 1 of each year, the Secretary shall submit to the Committees on Veterans' Affairs of the Senate and House of Representatives, the Committee on Government Reform of the House of Representatives, and the Committee on Homeland Security and Governmental Affairs of the Senate, a report on the Department's compliance with subtitle III of chapter 35 of title 44. The information in such report shall be displayed in the aggregate and separately for each Administration, office, and facility of the Department.

(c) REPORTS TO SECRETARY OF COMPLIANCE DEFICIENCIES.—(1) At least once every month, the Chief Information Officer shall report to the Secretary any deficiency in the compliance with subtitle III of chapter 35 of title 44 of the Department or any Administration, office, or facility of the Department.

(2) The Chief Information Officer shall immediately report to the Secretary any significant deficiency in such compliance.

(d) DATA BREACHES.—(1) The Chief Information Officer shall immediately provide notice to the Secretary of any data breach.

(2) Immediately after receiving notice of a data breach under paragraph (1), the Secretary shall provide notice of such breach to the Director of the Office of Management and Budget, the Inspector General of the Department, and, if appropriate, the Federal Trade Commission and the United States Secret Service.

(e) BUDGETARY MATTERS.—When the budget for any fiscal year is submitted by the President to Congress under section 1105 of title 31, the Secretary shall submit to Congress a report that identifies amounts requested for Department implementation and remediation of and compliance with this subchapter and subtitle III of chapter 35 of title 44. The report shall set forth those amounts both for each Administration within the Department and for the Department in the aggregate and shall identify, for each such amount, how that

amount is aligned with and supports such implementation and compliance.

§ 5724. Congressional reporting and notification of data breaches

(a) QUARTERLY REPORTS.—(1) Not later than 30 days after the last day of a fiscal quarter, the Secretary shall submit to the Committees on Veterans' Affairs of the Senate and House of Representatives a report on any data breach with respect to sensitive personal information processed or maintained by the Department that occurred during that quarter.

(2) Each report submitted under paragraph (1) shall identify, for each data breach covered by the report, the Administration and facility of the Department responsible for processing or maintaining the sensitive personal information involved in the data breach.

(b) NOTIFICATION OF SIGNIFICANT DATA BREACHES.—(1) In the event of a data breach with respect to sensitive personal information processed or maintained by the Secretary that the Secretary determines is significant, the Secretary shall provide notice of such breach to the Committees on Veterans' Affairs of the Senate and House of Representatives.

(2) Notice under paragraph (1) shall be provided promptly following the discovery of such a data breach and the implementation of any measures necessary to determine the scope of the breach, prevent any further breach or unauthorized disclosures, and reasonably restore the integrity of the data system.

§ 5725. Data breaches

(a) INDEPENDENT RISK ANALYSIS.—(1) In the event of a data breach with respect to sensitive personal information that is processed or maintained by the Secretary, the Secretary shall ensure that, as soon as possible after the data breach, a non-Department entity conducts an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach.

(2) If the Secretary determines, based on the findings of a risk analysis conducted under paragraph (1), that a reasonable risk exists for the potential misuse of sensitive information involved in a data breach, the Secretary shall provide credit protection services in accordance with section 5726 of this title.

(b) NOTIFICATION.—(1) In the event of a data breach with respect to sensitive personal information that is processed or maintained by the Secretary, the Secretary shall provide to an individual whose sensitive personal information is involved in that breach notice of the data breach—

(A) in writing; or

(B) by email, if—

(i) the Department's primary method of communication with the individual is by email; and

(ii) the individual has consented to receive such notification.

(2) Notice provided under paragraph (1) shall—

(A) describe the circumstances of the data breach and the risk that the breach could lead to misuse, including identity theft, involving the sensitive personal information of the individual;

(B) describe the specific types of sensitive personal information that was compromised as a part of the data breach;

(C) describe the actions the Department is taking to remedy the data breach;

(D) inform the individual that the individual may request a fraud alert and credit security freeze under this section;

(E) clearly explain the advantages and disadvantages to the individual of receiving fraud alerts and credit security freezes under this section; and

(F) includes such other information as the Secretary determines is appropriate.

(3) The notice required under paragraph (1) shall be provided promptly following the discovery of a data breach and the implementation of any measures necessary to determine the scope of the breach, prevent any further breach or unauthorized disclosures, and reasonably restore the integrity of the data system.

(c) REPORT.—For each data breach with respect to sensitive personal information processed or maintained by the Secretary, the Secretary shall promptly submit to the Committees on Veterans' Affairs of the Senate and House of Representatives a report containing the findings of any independent risk analysis conducted under subsection (a)(1), any determination of the Secretary under subsection (a)(2), and a description of any credit protection services provided under section 5726 of this title.

(d) FINAL DETERMINATION.—Notwithstanding sections 511 and 7104(a) of this title, any determination of the Secretary under subsection (a)(2) with respect to the reasonable risk for the potential misuse of sensitive information involved in a data breach is final and conclusive and may not be reviewed by any other official, administrative body, or court, whether by an action in the nature of mandamus or otherwise.

(e) FRAUD ALERTS.—(1) In the event of a data breach with respect to sensitive personal information that is processed or maintained by the Secretary, the Secretary shall arrange, upon the request of an individual whose sensitive personal information is involved in the breach to a principal credit reporting agency with which the Secretary has entered into a contract under section 5726(d) and at no cost to the individual, for the principal credit reporting agency to provide fraud alert services for that individual for a period of not less than one year, beginning on the date of such request, unless the individual requests that such fraud alert be removed before the end of such period, and the agency receives appropriate proof of the identity of the individual for such purpose.

(2) The Secretary shall arrange for each principal credit reporting agency referred to in paragraph (1) to provide any alert requested under such subsection in the file of the individual along with any credit score generated in using that file, for a period of not less than one year, beginning on the date of such request, unless the individual requests that such fraud alert be removed before the end of such period, and the agency receives appropriate proof of the identity of the individual for such purpose.

(f) CREDIT SECURITY FREEZE.—(1) In the event of a data breach with respect to sensitive personal information that is processed or maintained by the Secretary, the Secretary shall arrange, upon the request of an individual whose sensitive personal information is involved in the breach and at no cost to the individual, for each principal credit reporting agency to apply a security freeze to the file of that individual for a period of not less than one year, beginning on the date of such request, unless the individual requests that such security freeze be removed before the end of such period, and the agency receives appropriate proof of the identity of the individual for such purpose.

(2) The Secretary shall arrange for a principal credit reporting agency applying a security freeze under paragraph (1)—

(A) to send a written confirmation of the security freeze to the individual within five business days of applying the freeze;

(B) to refer the information regarding the security freeze to other consumer reporting agencies;

(C) to provide the individual with a unique personal identification number or password to be used by the individual when providing authorization for the release of the individual's credit for a specific party or period of time; and

(D) upon the request of the individual, to temporarily lift the freeze for a period of time specified by the individual, beginning not later than three business days after the date on which the agency receives the request.

§ 5726. Provision of credit protection services

(a) COVERED INDIVIDUAL.—For purposes of this section, a covered individual is an individual whose sensitive personal information that is processed or maintained by the Department (or any third-party entity acting on behalf of the Department) is involved, on or after August 1, 2005, in a data breach for which the Secretary determines a reasonable risk exists for the potential misuse of sensitive personal information under section 5725(a)(2) of this title.

(b) NOTIFICATION.—(1) In addition to any notice required under subsection 5725(b) of this title, the Secretary shall provide to a covered individual notice in writing that—

(A) the individual may request credit protection services under this section;

(B) clearly explains the advantages and disadvantages to the individual of receiving credit protection services under this section;

(C) includes a notice of which principal credit reporting agency the Secretary has entered into a contract with under subsection (d), and information about requesting services through that agency;

(D) describes actions the individual can or should take to reduce the risk of identity theft; and

(E) includes such other information as the Secretary determines is appropriate.

(2) The notice required under paragraph (1) shall be made as promptly as possible and without unreasonable delay following the discovery of a data breach for which the Secretary determines a reasonable risk exists for the potential misuse of sensitive personal information under section 5725(a)(2) of this title and the implementa-

tion of any measures necessary to determine the scope of the breach, prevent any further breach or unauthorized disclosures, and reasonably restore the integrity of the data system.

(3) The Secretary shall ensure that each notification under paragraph (1) includes a form or other means for readily requesting the credit protection services under this section. Such form or other means may include a telephone number, email address, or Internet website address.

(c) AVAILABILITY OF SERVICES THROUGH OTHER GOVERNMENT AGENCIES.—If a service required to be provided under this section is available to a covered individual through another department or agency of the Government, the Secretary and the head of that department or agency may enter into an agreement under which the head of that department or agency agrees to provide that service to the covered individual.

(d) CONTRACT WITH CREDIT REPORTING AGENCY.—Subject to the availability of appropriations and notwithstanding any other provision of law, the Secretary shall enter into contracts or other agreements as necessary with one or more principal credit reporting agencies in order to ensure, in advance, the provision of credit protection services under this section and fraud alerts and security freezes under section 5725 of this title. Any such contract or agreement may include provisions for the Secretary to pay the expenses of such a credit reporting agency for the provision of such services.

(e) DATA BREACH ANALYSIS.—The Secretary shall arrange, upon the request of a covered individual and at no cost to the individual, to provide data breach analysis for the individual for a period of not less than one year, beginning on the date of such request.

(f) PROVISION OF CREDIT MONITORING SERVICES AND IDENTITY THEFT INSURANCE.—During the one-year period beginning on the date on which the Secretary notifies a covered individual that the individual's sensitive personal information is involved in a data breach, the Secretary shall arrange, upon the request of the individual and without charge to the individual, for the provision of credit monitoring services to the individual. Credit monitoring services under this subsection shall include each of the following:

(1) One copy of the credit report of the individual every three months.

(2) Fraud resolution services for the individual.

(3) Identity theft insurance in a coverage amount that does not exceed $30,000 in aggregate liability for the insured.

§ 5727. Contracts for data processing or maintenance

(a) CONTRACT REQUIREMENTS.—If the Secretary enters into a contract for the performance of any Department function that requires access to sensitive personal information, the Secretary shall require as a condition of the contract that—

(1) the contractor shall not, directly or through an affiliate of the contractor, disclose such information to any other person unless the disclosure is lawful and is expressly permitted under the contract;

(2) the contractor, or any subcontractor for a subcontract of the contract, shall promptly notify the Secretary of any data breach that occurs with respect to such information.

(b) LIQUIDATED DAMAGES.—Each contract subject to the requirements of subsection (a) shall provide for liquidated damages to be paid by the contractor to the Secretary in the event of a data breach with respect to any sensitive personal information processed or maintained by the contractor or any subcontractor under that contract.

(c) PROVISION OF CREDIT PROTECTION SERVICES.—Any amount collected by the Secretary under subsection (b) shall be deposited in or credited to the Department account from which the contractor was paid and shall remain available for obligation without fiscal year limitation exclusively for the purpose of providing credit protection services in accordance with section 5726 of this title.

§ 5728. Authorization of appropriations

There are authorized to be appropriated to carry out this subchapter such sums as may be necessary for each fiscal year.

* * * * * * *

PART V—BOARDS, ADMINISTRATIONS, AND SERVICES

Chapter	Sec.
71. Board of Veterans' Appeals	7101
* * * * * * *	
79. Information Security Education Assistance Program	*7901*
* * * * * * *	

CHAPTER 79—INFORMATION SECURITY EDUCATION ASSISTANCE PROGRAM

Sec.
7901. Programs; purpose.
7902. Scholarship program.
7903. Education debt reduction program.
7904. Preferences in awarding financial assistance.
7905. Requirement of honorable discharge for veterans receiving assistance.
7906. Regulations.
7907. Termination.

§ 7901. Programs; purpose

(a) IN GENERAL.—To encourage the recruitment and retention of Department personnel who have the information security skills necessary to meet Department requirements, the Secretary shall carry out programs in accordance with this chapter to provide financial support for education in computer science and electrical and computer engineering at accredited institutions of higher education.

(b) TYPES OF PROGRAMS.—The programs authorized under this chapter are as follows:

(1) Scholarships for pursuit of doctoral degrees in computer science and electrical and computer engineering at accredited institutions of higher education.

(2) Education debt reduction for Department personnel who hold doctoral degrees in computer science and electrical and computer engineering at accredited institutions of higher education.

§ 7902. Scholarship program

(a) AUTHORITY.—(1) Subject to the availability of appropriations, the Secretary shall establish a scholarship program under which the Secretary shall, subject to subsection (d), provide financial assistance in accordance with this section to a qualified person—

(A) who is pursuing a doctoral degree in computer science or electrical or computer engineering at an accredited institution of higher education; and

(B) who enters into an agreement with the Secretary as described in subsection (b).

(2)(A) Except as provided under subparagraph (B), the Secretary may provide financial assistance under this section to an individual for up to five years.

(B) The Secretary may waive the limitation under subparagraph (A) if the Secretary determines that such a waiver is appropriate.

(3)(A) The Secretary may award up to five scholarships for any academic year to individuals who did not receive assistance under this section for the preceding academic year.

(B) Not more than one scholarship awarded under subparagraph (A) may be awarded to an individual who is an employee of the Department when the scholarship is awarded.

(b) SERVICE AGREEMENT FOR SCHOLARSHIP RECIPIENTS.—(1) To receive financial assistance under this section an individual shall enter into an agreement to accept and continue employment in the Department for the period of obligated service determined under paragraph (2).

(2) For the purposes of this subsection, the period of obligated service for a recipient of financial assistance under this section shall be the period determined by the Secretary as being appropriate to obtain adequate service in exchange for the financial assistance and otherwise to achieve the goals set forth in section 7901(a) of this title. In no event may the period of service required of a recipient be less than the period equal to two times the total period of pursuit of a degree for which the Secretary agrees to provide the recipient with financial assistance under this section. The period of obligated service is in addition to any other period for which the recipient is obligated to serve on active duty or in the civil service, as the case may be.

(3) An agreement entered into under this section by a person pursuing an doctoral degree shall include terms that provide the following:

(A) That the period of obligated service begins on a date after the award of the degree that is determined under the regulations prescribed under section 7906 of this title.

(B) That the individual will maintain satisfactory academic progress, as determined in accordance with those regulations, and that failure to maintain such progress constitutes grounds for termination of the financial assistance for the individual under this section.

(C) Any other terms and conditions that the Secretary determines appropriate for carrying out this section.

(c) AMOUNT OF ASSISTANCE.—(1) The amount of the financial assistance provided for an individual under this section shall be the amount determined by the Secretary as being necessary to pay—

(A) the tuition and fees of the individual; and

(B) $1500 to the individual each month (including a month between academic semesters or terms leading to the degree for which such assistance is provided or during which the individual is not enrolled in a course of education but is pursuing independent research leading to such degree) for books, laboratory expenses, and expenses of room and board.

(2) In no case may the amount of assistance provided for an individual under this section for an academic year exceed $50,000.

(3) In no case may the total amount of assistance provided for an individual under this section exceed $200,000.

(4) Notwithstanding any other provision of law, financial assistance paid an individual under this section shall not be considered as income or resources in determining eligibility for, or the amount of benefits under, any Federal or federally assisted program.

(d) REPAYMENT FOR PERIOD OF UNSERVED OBLIGATED SERVICE.—(1) An individual who receives financial assistance under this section shall repay to the Secretary an amount equal to the unearned portion of the financial assistance if the individual fails to satisfy the requirements of the service agreement entered into under subsection (b), except in certain circumstances authorized by the Secretary.

(2) The Secretary may establish, by regulations, procedures for determining the amount of the repayment required under this subsection and the circumstances under which an exception to the required repayment may be granted.

(3) An obligation to repay the Secretary under this subsection is, for all purposes, a debt owed the United States. A discharge in bankruptcy under title 11 does not discharge a person from such debt if the discharge order is entered less than five years after the date of the termination of the agreement or contract on which the debt is based.

(e) WAIVER OR SUSPENSION OF COMPLIANCE.—The Secretary shall prescribe regulations providing for the waiver or suspension of any obligation of a individual for service or payment under this section (or an agreement under this section) whenever noncompliance by the individual is due to circumstances beyond the control of the individual or whenever the Secretary determines that the waiver or suspension of compliance is in the best interest of the United States.

(f) INTERNSHIPS.—(1) The Secretary may offer a compensated internship to an individual for whom financial assistance is provided under this section during a period between academic semesters or terms leading to the degree for which such assistance is provided. Compensation provided for such an internship shall be in addition to the financial assistance provided under this section.

(2) An internship under this subsection shall not be counted toward satisfying a period of obligated service under this section.

(g) INELIGIBILITY OF INDIVIDUALS RECEIVING CERTAIN EDUCATION ASSISTANCE PAYMENTS.—An individual who receives a payment of educational assistance under chapter 30, 31, 32, 34, or 35 of this title or chapter 1606 or 1607 of title 10 for a month in which the individual is enrolled in a course of education leading to a doctoral degree in information security is not eligible to receive financial assistance under this section for that month.

§ 7903. Education debt reduction program

(a) AUTHORITY.—(1) Subject to the availability of appropriations, the Secretary shall establish an education debt reduction program under which the Secretary shall make education debt reduction payments under this section to qualified individuals eligible under subsection (b) for the purpose of reimbursing such individuals for payments by such individuals of principal and interest on loans described in paragraph (2) of that subsection.

(2)(A) For each fiscal year, the Secretary may accept up to five individuals into the program established under paragraph (1)who did not receive such a payment during the preceding fiscal year.

(B) Not more than one individual accepted into the program for a fiscal year under subsection (A) shall be a Department employee as of the date on which the individual is accepted into the program.

(b) ELIGIBILITY.—An individual is eligible to participate in the program under this section if the individual—

(1) has completed a doctoral degree a doctoral degree in computer science or electrical or computer engineering at an accredited institution of higher education during the five-year period preceding the date on which the individual is hired;

(2) is an employee of the Department who serves in a position related to information security (as determined by the Secretary); and

(3) owes any amount of principal or interest under a loan, the proceeds of which were used by or on behalf of that individual to pay costs relating to a doctoral degree in computer science or electrical or computer engineering at an accredited institution of higher education.

(c) AMOUNT OF ASSISTANCE.—(1) Subject to paragraph (2), the amount of education debt reduction payments made to an individual under this section may not exceed $82,500 over a total of five years, of which not more than $16,500 of such payments may be made in each year.

(2) The total amount payable to an individual under this section for any year may not exceed the amount of the principal and interest on loans referred to in subsection (b)(3) that is paid by the individual during such year.

(d) PAYMENTS.—(1) The Secretary shall make education debt reduction payments under this section on an annual basis.

(2) The Secretary shall make such a payment—

(A) on the last day of the one-year period beginning on the date on which the individual is accepted into the program established under subsection (a); or

(B) in the case of an individual who received a payment under this section for the preceding fiscal year, on the last day of the one-year period beginning on the date on which the individual last received such a payment.

(3) Notwithstanding any other provision of law, education debt reduction payments under this section shall not be considered as income or resources in determining eligibility for, or the amount of benefits under, any Federal or federally assisted program.

(e) PERFORMANCE REQUIREMENT.—The Secretary may make education debt reduction payments to an individual under this section for a year only if the Secretary determines that the individual main-

tained an acceptable level of performance in the position or positions served by the individual during the year.

(f) NOTIFICATION OF TERMS OF PROVISION OF PAYMENTS.—The Secretary shall provide to an individual who receives a payment under this section notice in writing of the terms and conditions that apply to such a payment.

(g) COVERED COSTS.—For purposes of subsection (b)(3), costs relating to a course of education or training include—

(1)) tuition expenses; and

(2) all other reasonable educational expenses, including fees, books, and laboratory expenses;

§ 7904. Preferences in awarding financial assistance

In awarding financial assistance under this chapter, the Secretary shall give a preference to qualified individuals who are otherwise eligible to receive the financial assistance in the following order of priority:

(1) Veterans with service-connected disabilities.

(2) Veterans.

(3) Persons described in section 4215(a)(1)(B) of this title.

(4) Individuals who received or are pursuing degrees at institutions designated by the National Security Agency as Centers of Academic Excellence in Information Assurance Education.

(5) Citizens of the United States.

§ 7905. Requirement of honorable discharge for veterans receiving assistance

No veteran shall receive financial assistance under this chapter unless the veteran was discharged from the Armed Forces under honorable conditions.

§ 7906. Regulations

The Secretary shall prescribe regulations for the administration of this chapter.

§ 7907. Termination

The authority of the Secretary to make a payment under this chapter shall terminate on July 31, 2017.

* * * * * * *

○