Pub. L. 102–54 amended section as in effect immediately before the enactment of Pub. L. 102–40 by substituting ''subpoena'' for ''subpena'' in section catchline and in two places in text.

SUBCHAPTER III—INFORMATION SECURITY

§ 5721. Purpose

The purpose of the Information Security Program is to establish a program to provide security for Department information and information systems commensurate to the risk of harm, and to communicate the responsibilities of the Secretary, Under Secretaries, Assistant Secretaries, other key officials, Assistant Secretary for Information and Technology, Associate Deputy Assistant Secretary for Cyber and Information Security, and Inspector General of the Department of Veterans Affairs as outlined in the provisions of subchapter III of chapter 35 of title 44 (also known as the ''Federal Information Security Management Act of 2002'', which was enacted as part of the E-Government Act of 2002 (Public Law 107–347)).

(Added Pub. L. 109–461, title IX, § 902(a), Dec. 22, 2006, 120 Stat. 3450.)

REFERENCES IN TEXT

The Federal Information Security Management Act of 2002, referred to in text, is the statutory short title for title III of Pub. L. 107–347, Dec. 17, 2002, 116 Stat. 2946, and for title X of Pub. L. 107–296, Nov. 25, 116 Stat. 2259. For complete classification of these Acts to the Code, see Short Title of 2002 Amendments note set out under section 101 of Title 44, Public Printing and Documents, Short Title note set out under section 101 of Title 6, Domestic Security, and Tables.

The E-Government Act of 2002, referred to in text, is Pub. L. 107–347, Dec. 17, 2002, 116 Stat. 2899. For complete classification of this Act to the Code, see Tables.

REGULATIONS

Pub. L. 109–461, title IX, § 902(c), Dec. 22, 2006, 120 Stat. 3460, provided that: ''Not later than one year after the date of the enactment of this Act [Dec. 22, 2006], the Secretary of Veterans Affairs shall prescribe regulations to carry out subchapter III of chapter 57 of title 38, United States Code, as added by subsection (a).''

§ 5722. Policy

(a) IN GENERAL.—The security of Department information and information systems is vital to the success of the mission of the Department. To that end, the Secretary shall establish and maintain a comprehensive Department-wide information security program to provide for the development and maintenance of cost-effective security controls needed to protect Department information, in any media or format, and Department information systems.

(b) ELEMENTS.—The Secretary shall ensure that the Department information security program includes the following elements:

(1) Periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the Department.

(2) Policies and procedures that—

(A) are based on risk assessments;

(B) cost-effectively reduce security risks to an acceptable level; and

(C) ensure that information security is addressed throughout the life cycle of each Department information system.

(3) Selection and effective implementation of minimum, mandatory technical, operational, and management security controls, or other compensating countermeasures, to protect the confidentiality, integrity, and availability of each Department system and its information.

(4) Subordinate plans for providing adequate security for networks, facilities, systems, or groups of information systems, as appropriate.

(5) Annual security awareness training for all Department employees, contractors, and all other users of VA sensitive data and Department information systems that identifies the information security risks associated with the activities of such employees, contractors, and users and the responsibilities of such employees, contractors, and users to comply with Department policies and procedures designed to reduce such risks.

(6) Periodic testing and evaluation of the effectiveness of security controls based on risk, including triennial certification testing of all management, operational, and technical controls, and annual testing of a subset of those controls for each Department system.

(7) A process for planning, developing, implementing, evaluating, and documenting remedial actions to address deficiencies in information security policies, procedures, and practices.

(8) Procedures for detecting, immediately reporting, and responding to security incidents, including mitigating risks before substantial damage is done as well as notifying and consulting with the US-Computer Emergency Readiness Team of the Department of Homeland Security, law enforcement agencies, the Inspector General of the Department, and other offices as appropriate.

(9) Plans and procedures to ensure continuity of operations for Department systems.

(c) COMPLIANCE WITH CERTAIN REQUIREMENTS.—The Secretary shall comply with the provisions of subchapter III of chapter 35 of title 44 and other related information security requirements promulgated by the National Institute of Standards and Technology and the Office of Management and Budget that define Department information system mandates.

(Added Pub. L. 109–461, title IX, § 902(a), Dec. 22, 2006, 120 Stat. 3450.)

§ 5723. Responsibilities

(a) SECRETARY OF VETERANS AFFAIRS.—In accordance with the provisions of subchapter III of chapter 35 of title 44, the Secretary is responsible for the following:

(1) Ensuring that the Department adopts a Department-wide information security program and otherwise complies with the provisions of subchapter III of chapter 35 of title 44 and other related information security requirements.

(2) Ensuring that information security protections are commensurate with the risk and

magnitude of the potential harm to Department information and information systems resulting from unauthorized access, use, disclosure, disruption, modification, or destruction.

(3) Ensuring that information security management processes are integrated with Department strategic and operational planning processes.

(4) Ensuring that the Under Secretaries, Assistant Secretaries, and other key officials of the Department provide adequate security for the information and information systems under their control.

(5) Ensuring enforcement and compliance with the requirements imposed on the Department under the provisions of subchapter III of chapter 35 of title 44.

(6) Ensuring that the Department has trained program and staff office personnel sufficient to assist in complying with all the provisions of subchapter III of chapter 35 of title 44 and other related information security requirements.

(7) Ensuring that the Assistant Secretary for Information and Technology, in coordination with the Under Secretaries, Assistant Secretaries, and other key officials of the Department report to Congress, the Office of Management and Budget, and other entities as required by law and Executive Branch direction on the effectiveness of the Department information security program, including remedial actions.

(8) Notifying officials other than officials of the Department of data breaches when required under this subchapter.

(9) Ensuring that the Assistant Secretary for Information and Technology 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 subchapter III of chapter 35 of title 44, including the management of all related mission applications, information resources, personnel, and infrastructure.

(10) Submitting 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, not later than March 1 each year, a report on the compliance of the Department with subchapter III of chapter 35 of title 44, with the information in such report displayed in the aggregate and separately for each Administration, office, and facility of the Department.

(11) Taking appropriate action to ensure that the budget for any fiscal year, as submitted by the President to Congress under section 1105 of title 31, sets forth separately the amounts required in the budget for such fiscal year for compliance by the Department with Federal law and regulations governing information security, including this subchapter and subchapter III of chapter 35 of title 44.

(12) Providing notice to the Director of the Office of Management and Budget, the Inspector General of the Department, and such other Federal agencies as the Secretary considers appropriate of a presumptive data breach of which notice is provided the Secretary under subsection (b)(16) if, in the opinion of the Assistant Secretary for Information and Technology, the breach involves the information of twenty or more individuals.

(b) ASSISTANT SECRETARY FOR INFORMATION AND TECHNOLOGY.—The Assistant Secretary for Information and Technology, as the Chief Information Officer of the Department, is responsible for the following:

(1) Establishing, maintaining, and monitoring Department-wide information security policies, procedures, control techniques, training, and inspection requirements as elements of the Department information security program.

(2) Issuing policies and handbooks to provide direction for implementing the elements of the information security program to all Department organizations.

(3) Approving all policies and procedures that are related to information security for those areas of responsibility that are currently under the management and the oversight of other Department organizations.

(4) Ordering and enforcing Department-wide compliance with and execution of any information security policy.

(5) Establishing minimum mandatory technical, operational, and management information security control requirements for each Department system, consistent with risk, the processes identified in standards of the National Institute of Standards and Technology, and the responsibilities of the Assistant Secretary to operate and maintain all Department systems currently creating, processing, collecting, or disseminating data on behalf of Department information owners.

(6) Establishing standards for access to Department information systems by organizations and individual employees, and to deny access as appropriate.

(7) Directing that any incidents of failure to comply with established information security policies be immediately reported to the Assistant Secretary.

(8) Reporting any compliance failure or policy violation directly to the appropriate Under Secretary, Assistant Secretary, or other key official of the Department for appropriate administrative or disciplinary action.

(9) Reporting any compliance failure or policy violation directly to the appropriate Under Secretary, Assistant Secretary, or other key official of the Department along with taking action to correct the failure or violation.

(10) Requiring any key official of the Department who is so notified to report to the Assistant Secretary with respect to an action to be taken in response to any compliance failure or policy violation reported by the Assistant Secretary.

(11) Ensuring that the Chief Information Officers and Information Security Officers of the Department comply with all cyber security directives and mandates, and ensuring that these staff members have all necessary authority and means to direct full compliance with such directives and mandates relating to

the acquisition, operation, maintenance, or use of information technology resources from all facility staff.

(12) Establishing the VA National Rules of Behavior for appropriate use and protection of the information which is used to support Department missions and functions.

(13) Establishing and providing supervision over an effective incident reporting system.

(14) Submitting to the Secretary, at least once every quarter, a report on any deficiency in the compliance with subchapter III of chapter 35 of title 44 of the Department or any Administration, office, or facility of the Department.

(15) Reporting immediately to the Secretary on any significant deficiency in the compliance described by paragraph (14).

(16) Providing immediate notice to the Secretary of any presumptive data breach.

(c) ASSOCIATE DEPUTY ASSISTANT SECRETARY FOR CYBER AND INFORMATION SECURITY.—In accordance with the provisions of subchapter III of chapter 35 of title 44, the Associate Deputy Assistant Secretary for Cyber and Information Security, as the Senior Information Security Officer of the Department, is responsible for carrying out the responsibilities of the Assistant Secretary for Information and Technology under the provisions of subchapter III of chapter 35 of title 44, as set forth in subsection (b).

(d) DEPARTMENT INFORMATION OWNERS.—In accordance with the criteria of the Centralized IT Management System, Department information owners are responsible for the following:

(1) Providing assistance to the Assistant Secretary for Information and Technology regarding the security requirements and appropriate level of security controls for the information system or systems where sensitive personal information is currently created, collected, processed, disseminated, or subject to disposal.

(2) Determining who has access to the system or systems containing sensitive personal information, including types of privileges and access rights.

(3) Ensuring the VA National Rules of Behavior is signed on an annual basis and enforced by all system users to ensure appropriate use and protection of the information which is used to support Department missions and functions.

(4) Assisting the Assistant Secretary for Information and Technology in the identification and assessment of the common security controls for systems where their information resides.

(5) Providing assistance to Administration and staff office personnel involved in the development of new systems regarding the appropriate level of security controls for their information.

(e) OTHER KEY OFFICIALS.—In accordance with the provisions of subchapter III of chapter 35 of title 44, the Under Secretaries, Assistant Secretaries, and other key officials of the Department are responsible for the following:

(1) Implementing the policies, procedures, practices, and other countermeasures identified in the Department information security program that comprise activities that are under their day-to-day operational control or supervision.

(2) Periodically testing and evaluating information security controls that comprise activities that are under their day-to-day operational control or supervision to ensure effective implementation.

(3) Providing a plan of action and milestones to the Assistant Secretary for Information and Technology on at least a quarterly basis detailing the status of actions being taken to correct any security compliance failure or policy violation.

(4) Complying with the provisions of subchapter III of chapter 35 of title 44 and other related information security laws and requirements in accordance with orders of the Assistant Secretary for Information and Technology to execute the appropriate security controls commensurate to responding to a security bulletin of the Security Operations Center of the Department, with such orders to supersede and take priority over all operational tasks and assignments and be complied with immediately.

(5) Ensuring that—

(A) all employees within their organizations take immediate action to comply with orders from the Assistant Secretary for Information and Technology to—

(i) mitigate the impact of any potential security vulnerability;

(ii) respond to a security incident; or

(iii) implement the provisions of a bulletin or alert of the Security Operations Center; and

(B) organizational managers have all necessary authority and means to direct full compliance with such orders from the Assistant Secretary.

(6) Ensuring the VA National Rules of Behavior is signed and enforced by all system users to ensure appropriate use and protection of the information which is used to support Department missions and functions on an annual basis.

(f) USERS OF DEPARTMENT INFORMATION AND INFORMATION SYSTEMS.—Users of Department information and information systems are responsible for the following:

(1) Complying with all Department information security program policies, procedures, and practices.

(2) Attending security awareness training on at least an annual basis.

(3) Reporting all security incidents immediately to the Information Security Officer of the system or facility and to their immediate supervisor.

(4) Complying with orders from the Assistant Secretary for Information and Technology directing specific activities when a security incident occurs.

(5) Signing an acknowledgment that they have read, understand, and agree to abide by the VA National Rules of Behavior on an annual basis.

(g) INSPECTOR GENERAL OF DEPARTMENT OF VETERANS AFFAIRS.—In accordance with the pro-

visions of subchapter III of chapter 35 of title 44, the Inspector General of the Department is responsible for the following:

(1) Conducting an annual audit of the Department information security program.

(2) Submitting an independent annual report to the Office of Management and Budget on the status of the Department information security program, based on the results of the annual audit.

(3) Conducting investigations of complaints and referrals of violations as considered appropriate by the Inspector General.

(Added Pub. L. 109–461, title IX, § 902(a), Dec. 22, 2006, 120 Stat. 3451; amended Pub. L. 111–275, title X, § 1001(m)(1), Oct. 13, 2010, 124 Stat. 2897.)

AMENDMENTS

2010—Subsec. (g)(2). Pub. L. 111–275 inserted ''the'' before ''Department''.

§ 5724. Provision of credit protection and other services

(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 or the Office of Inspector General of the Department 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 personal information involved in a data breach, the Secretary shall provide credit protection services in accordance with the regulations prescribed by the Secretary under this section.

(b) REGULATIONS.—Not later than 180 days after the date of the enactment of the Veterans Benefits, Health Care, and Information Technology Act of 2006, the Secretary shall prescribe interim regulations for the provision of the following in accordance with subsection (a)(2):

(1) Notification.
(2) Data mining.
(3) Fraud alerts.
(4) Data breach analysis.
(5) Credit monitoring.
(6) Identity theft insurance.
(7) Credit protection services.

(c) REPORT.—(1) 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 services provided pursuant to subsection (b).

(2) In the event of a data breach with respect to sensitive personal information processed or maintained by the Secretary that is the sensitive personal information of a member of the Army, Navy, Air Force, or Marine Corps or a civilian officer or employee of the Department of Defense, the Secretary shall submit the report required under paragraph (1) to the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives in addition to the Committees on Veterans' Affairs of the Senate and House of Representatives.

(Added Pub. L. 109–461, title IX, § 902(a), Dec. 22, 2006, 120 Stat. 3455.)

REFERENCES IN TEXT

The date of the enactment of the Veterans Benefits, Health Care, and Information Technology Act of 2006, referred to in subsec. (b), is the date of enactment of Pub. L. 109–461, which was approved Dec. 22, 2006.

§ 5725. 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 pursuant to section 5724(b) of this title.

(Added Pub. L. 109–461, title IX, § 902(a), Dec. 22, 2006, 120 Stat. 3456.)

§ 5726. Reports and notice to Congress on 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—