AMENDMENTS

1991—Pub. L. 102–40 renumbered section 3311 of this title as this section.

Pub. L. 102–54 amended section as in effect immediately before the enactment of Pub. L. 102–40 by substituting ''subpoenas'' for ''subpenas'' in section catchline and amending text generally. Prior to amendment, text read as follows: ''For the purposes of the laws administered by the Veterans' Administration, the Administrator, and those employees to whom the Administrator may delegate such authority, to the extent of the authority so delegated, shall have the power to issue subpenas for and compel the attendance of witnesses within a radius of one hundred miles from the place of hearing, to require the production of books, papers, documents, and other evidence, to take affidavits, to administer oaths and affirmations, to aid claimants in the preparation and presentation of claims, and to make investigations and examine witnesses upon any matter within the jurisdiction of the Veterans' Administration. Any person required by such subpena to attend as a witness shall be allowed and paid the same fees and mileage as are paid witnesses in the district courts of the United States.''

§ 5712. Validity of affidavits

Any such oath, affirmation, affidavit, or examination, when certified under the hand of any such employee by whom it was administered or taken and authenticated by the seal of the Department, may be offered or used in any court of the United States and without further proof of the identity or authority of such employee shall have like force and effect as if administered or taken before a clerk of such court.

(Pub. L. 85–857, Sept. 2, 1958, 72 Stat. 1237, § 3312; renumbered § 5712, Pub. L. 102–40, title IV, § 402(b)(1), May 7, 1991, 105 Stat. 238; Pub. L. 102–83, § 4(a)(3), (4), Aug. 6, 1991, 105 Stat. 404.)

AMENDMENTS

1991—Pub. L. 102–40 renumbered section 3312 of this title as this section.

Pub. L. 102–83 substituted ''Department'' for ''Veterans' Administration''.

§ 5713. Disobedience to subpoena

In case of disobedience to any such subpoena, the aid of any district court of the United States may be invoked in requiring the attendance and testimony of witnesses and the production of documentary evidence, and such court within the jurisdiction of which the inquiry is carried on may, in case of contumacy or refusal to obey a subpoena issued to any officer, agent, or employee of any corporation or to any other person, issue an order requiring such corporation or other person to appear or to give evidence touching the matter in question; and any failure to obey such order of the court may be punished by such court as a contempt thereof.

(Pub. L. 85–857, Sept. 2, 1958, 72 Stat. 1237, § 3313; renumbered § 5713, Pub. L. 102–40, title IV, § 402(b)(1), May 7, 1991, 105 Stat. 238; Pub. L. 102–54, § 14(d)(6)(A), (B), June 13, 1991, 105 Stat. 286.)

AMENDMENTS

1991—Pub. L. 102–40 renumbered section 3313 of this title as this section.

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, oper-

ational, 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.