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—

(A) the Administration and facility of the Department responsible for processing or maintaining the sensitive personal information involved in the data breach; and

(B) the status of any remedial or corrective action with respect to 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) 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 that the Secretary determines is significant under paragraph (1), the Secretary shall provide the notice 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.

(3) Notice under paragraphs (1) and (2) 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.

(Added Pub. L. 109–461, title IX, § 902(a), Dec. 22, 2006, 120 Stat. 3457.)

§ 5727. Definitions

In this subchapter:

(1) AVAILABILITY.—The term ''availability'' means ensuring timely and reliable access to and use of information.

(2) CONFIDENTIALITY.—The term ''confidentiality'' means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

(3) CONTROL TECHNIQUES.—The term ''control techniques'' means methods for guiding and controlling the operations of information systems to ensure adherence to the provisions of subchapter III of chapter 35 of title 44 and other related information security requirements.

(4) DATA BREACH.—The term ''data breach'' means the loss, theft, or other unauthorized access, other than those incidental to the scope of employment, 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.

(5) DATA BREACH ANALYSIS.—The term ''data breach analysis'' means the process used to determine if a data breach has resulted in the misuse of sensitive personal information.

(6) FRAUD RESOLUTION SYSTEMS.—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.

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

(8) IDENTITY THEFT INSURANCE.—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 efforts to correct and ameliorate the effects and results of identity theft of the insured individual.

(9) INFORMATION OWNER.—The term ''information owner'' means an agency official with statutory or operational authority for specified information and responsibility for establishing the criteria for its creation, collection, processing, dissemination, or disposal, which responsibilities may extend to interconnected systems or groups of interconnected systems.

(10) INFORMATION RESOURCES.—The term ''information resources'' means information in any medium or form and its related resources, such as personnel, equipment, funds, and information technology.

(11) INFORMATION SECURITY.—The term ''information security'' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability.

(12) INFORMATION SECURITY REQUIREMENTS.—The term ''information security requirements'' means information security requirements promulgated in accordance with law, or directed by the Secretary of Commerce, the National Institute of Standards and Technology, and the Office of Management and Budget, and, as to national security systems, the President.

(13) INFORMATION SYSTEM.—The term ''information system'' means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, whether automated or manual.

(14) INTEGRITY.—The term ''integrity'' means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

(15) NATIONAL SECURITY SYSTEM.—The term ''national security system'' means an information system that is protected at all times by policies and procedures established for the processing, maintenance, use, sharing, dissemination or disposition of information that has been specifically authorized under criteria established by statute or Executive Order to be kept classified in the interest of national defense or foreign policy.

(16) PLAN OF ACTION AND MILESTONES.—The term ''plan of action and milestones'', means a plan used as a basis for the quarterly reporting requirements of the Office of Management and Budget that includes the following information:

(A) A description of the security weakness.

(B) The identity of the office or organization responsible for resolving the weakness.

(C) An estimate of resources required to resolve the weakness by fiscal year.

(D) The scheduled completion date.

(E) Key milestones with estimated completion dates.

(F) Any changes to the original key milestone date.

(G) The source that identified the weakness.

(H) The status of efforts to correct the weakness.

(17) PRINCIPAL CREDIT REPORTING AGENCY.—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)).

(18) SECURITY INCIDENT.—The term ''security incident'' means an event that has, or could have, resulted in loss or damage to Department assets, or sensitive information, or an action that breaches Department security procedures.

(19) SENSITIVE PERSONAL INFORMATION.—The term ''sensitive personal information'', with respect to an individual, means any information about the individual maintained by an agency, including the following:

(A) Education, financial transactions, medical history, and criminal or employment history.

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

(20) SUBORDINATE PLAN.—The term ''subordinate plan'', also referred to as a ''system security plan'', means a plan that defines the security controls that are either planned or implemented for networks, facilities, systems, or groups of systems, as appropriate, within a specific accreditation boundary.

(21) TRAINING.—The term ''training'' means a learning experience in which an individual is taught to execute a specific information security procedure or understand the information security common body of knowledge.

(22) VA NATIONAL RULES OF BEHAVIOR.—The term ''VA National Rules of Behavior'' means a set of Department rules that describes the responsibilities and expected behavior of personnel with regard to information system usage.

(23) VA SENSITIVE DATA.—The term ''VA sensitive data'' means all Department data, on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information and includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, and records about individuals requiring protection under applicable confidentiality provisions.

(Added Pub. L. 109–461, title IX, § 902(a), Dec. 22, 2006, 120 Stat. 3457; amended Pub. L. 111–275, title X, § 1001(m)(2), Oct. 13, 2010, 124 Stat. 2897.)

AMENDMENTS

2010—Par. (20). Pub. L. 111–275 substituted ''plan that defines'' for ''subordinate plan defines''.

§ 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.

(Added Pub. L. 109–461, title IX, § 902(a), Dec. 22, 2006, 120 Stat. 3460.)