

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—

(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).