ational 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 provisions 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—

(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).