(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