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, operational, 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, infor-