Department of Veterans Affairs
Washington, DC 20420

VA DIRECTIVE 6500
Transmittal Sheet
August 4, 2006

INFORMATION SECURITY PROGRAM

1. REASON FOR ISSUE: To replace Department of Veterans Affairs (VA) Directive 6210, Automated Information Systems Security, dated January 30, 1997 with a policy which establishes the criteria for the Department-wide information security program.

2. SUMMARY OF CONTENTS/MAJOR CHANGES: This directive requires Department-wide compliance with the Federal Information Security Management Act of 2002, 44 U.S.C. §§ 3541-3549, and related information security issuances pertaining to the security of VA information and information systems administered by VA, or otherwise under the authority, control, or on behalf of VA. This directive applies to all VA Administrations and staff offices, and pertains to the security of all VA information and information systems, at all levels of sensitivity, and at any location or facility.

3. RESPONSIBLE OFFICE: Office of Cyber and Information Security (005S), Office of the Assistant Secretary for Information and Technology (005).

4. RELATED HANDBOOK: Under development.

5. RESCISSIONS: VA Directive and Handbook 6210, Automated Information Systems Security, dated January 30, 1997.

CERTIFIED BY:

/s/
Robert T. Howard
Senior Advisor to the Deputy Secretary
Supervisor, Office Information and Technology

/s/
R. James Nicholson
Secretary of Veterans Affairs

Distribution: Electronic Only

INFORMATION SECURITY PROGRAM

1. PURPOSE. The purpose of this policy is to establish a program to provide security for VA information and information systems commensurate to the risk of harm, and to communicate the responsibilities of the Secretary, Under Secretaries, Assistant Secretaries, other key officials, the Assistant Secretary for Information and Technology, the Associate Deputy Assistant Secretary (ADAS) for Cyber and Information Security, and the Inspector General (IG) as outlined in the Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. §§ 3541-3549, which was enacted as part of the E-Government Act of 2002, Pub. L. No. 107-347 (Dec. 17, 2002).

2. POLICY

a. The security of VA information and information systems is vital to the success of VA's mission. To that end, VA shall establish and maintain a comprehensive Department-wide information security program to provide for development and maintenance of cost-effective security controls needed to protect VA information, in any media or format, and VA information systems. The VA information security program shall include 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 VA employees, contractors, and all other users of sensitive VA information and VA information systems which identifies the information security risks associated with their activities and their responsibilities in complying with Department policies and procedures designed to reduce those risks.

(6) Periodic testing and evaluation of the effectiveness of security controls based on risk to include, at a minimum, 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, to include mitigating risks before substantial damage is done as well as notifying and consulting with the US-Computer Emergency Readiness Team in the Department of Homeland Security, law enforcement agencies, the VA IG, and other offices as appropriate.

(9) Plans and procedures to ensure continuity of operations for Department systems.

b. VA shall comply with the provisions of FISMA and other related information security requirements promulgated by the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) that define VA information system mandates.

3. RESPONSIBILITIES

a. **The Secretary of Veterans Affairs.** In accordance with FISMA, the Secretary is responsible for:

(1) Ensuring that VA adopts a Department-wide information security program and otherwise complies with FISMA and other related information security requirements.

(2) Ensuring that information security protections are commensurate with the risk and magnitude of the potential harm to VA 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 Under Secretaries, Assistant Secretaries, and Other Key Officials provide adequate security for the information and information systems under their control.

(5) Ensuring enforcement and compliance with the requirements imposed on VA under FISMA.

(6) Ensuring that VA has trained program and staff office personnel sufficient to assist in complying with all FISMA and other related information security requirements.

(7) Ensuring that the Assistant Secretary for Information and Technology, in coordination with VA Under Secretaries, Assistant Secretaries, and other key officials reports the effectiveness of the VA information security program, including remedial actions, to Congress, OMB, and other entities as required by law and Executive Branch direction.

b. **The Assistant Secretary for Information and Technology.** The Assistant Secretary for Information and Technology, as the VA Chief Information Officer (CIO), is responsible for:

(1) Establishing, maintaining and monitoring Department-wide information security policies, procedures, control techniques, training and inspection requirements as elements of the VA information security program.

(2) Issuing policies and handbooks to provide direction for implementing the elements of the information security program to all Department organizations.

(3) Approving all policies and procedures that are related to information security for those areas of responsibility that are currently under the management and the oversight of other Department organizations.

(4) Ordering and enforcing Department-wide compliance with and execution of any information security policy.

(5) Establishing minimum mandatory technical, operational, and management information security control requirements for each VA system, consistent with risk, the processes identified in NIST

standards, and the CIO's responsibilities to operate and maintain all Department systems currently creating, processing, collecting, or disseminating data on behalf of VA information owners.

(6) Establishing standards for access to VA information systems by organizations and individual employees, and to deny access as appropriate.

(7) Directing that any incidents of failure to comply with established information security policies be immediately reported to the CIO.

(8) Reporting any compliance failure or policy violation directly to the appropriate Under Secretary, Assistant Secretary, or other key official for appropriate disciplinary action.

(9) Reporting any compliance failure or policy violation directly to the appropriate Under Secretary, Assistant Secretary, or other key official along with taking the appropriate corrective action.

(10) Requiring any key official who is so notified to report back to the CIO regarding what action is to be taken in response to any compliance failure or policy violation reported by the CIO.

(11) Ensuring VA's facility CIOs and Information Security Officers (ISO) comply with all cyber security directives and mandates, and ensuring that these staff members have all necessary authority and means to direct full compliance with such directives and mandates relating to the acquisition, operation, maintenance, or use of information technology (IT) resources from all facility staff.

(12) Establishing the VA National Rules of Behavior for appropriate use and protection of the information which is used to support VA missions and functions.

(13) Establishing and providing supervision over an effective incident reporting system.

c. **The ADAS for Cyber and Information Security.** In accordance with FISMA, the ADAS for Cyber and Information Security, as VA's Senior ISO, is responsible for carrying out the responsibilities of the Assistant Secretary for Information and Technology under FISMA, as described above.

d. **VA Information Owners**. In accordance with the criteria of the Federated IT Management System, these officials are responsible for:

(1) Providing assistance to the VA CIO regarding the security requirements and appropriate level of security controls for the information system(s) where their information is currently created, collected, processed, disseminated, or subject to disposal.

(2) Determining who has access to the system(s) containing their information, to include types of privileges and access rights.

(3) Ensuring the VA National Rules of Behavior is signed on an annual basis and enforced by all system users to ensure appropriate use and protection of the information which is used to support VA missions and functions.

(4) Assisting the VA CIO in the identification and assessment of the common security controls for systems where their information resides.

(5) Providing assistance to Administration and staff office personnel involved in the development of new systems regarding the appropriate level of security controls for their information.

e. **Under Secretaries, Assistant Secretaries, and Other Key Officials.** In accordance with FISMA, these officials are responsible for:

(1) Implementing the policies, procedures, practices, and other countermeasures identified in the VA information security program that comprise activities that are under their day-to-day operational control or supervision.

(2) Periodically testing and evaluating information security controls that comprise activities that are under their day-to-day operational control or supervision to ensure effective implementation.

(3) Providing a Plan of Action and Milestones (POA&M) to the VA CIO 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 FISMA and other related information security laws and requirements in accordance with the VA CIO orders to execute the appropriate security controls commensurate to responding to a VA Security Operations Center (SOC) security bulletin. Such orders of the VA CIO shall supersede and take priority over all operational tasks and assignments, and shall be complied with immediately.

(5) Ensuring that all employees within their organizations take immediate action to comply with orders from the VA CIO to (a) mitigate the impact of any potential security vulnerability, (b) respond to a security incident, or (c) implement the provisions of a SOC Bulletin or Alert. They shall ensure that their organizational managers have all necessary authority and means to direct full compliance with such orders from the VA CIO.

(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 VA missions and functions on an annual basis.

f. **Users of VA information and information systems.** These individuals are responsible for:

(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 system or facility ISO and their immediate supervisor.

(4) Complying with orders from the VA CIO directing specific activities when a security incident occurs.

(5) Signing an acknowledgement that they have read, understand, and agree to abide by the VA National Rules of Behavior on an annual basis.

g. **The Inspector General**. In accordance with FISMA, the VA IG is responsible for:

(1) Conducting an annual audit of the VA information security program.

(2) Submitting an independent annual report to OMB on the status of VA's information security program, based on the results of the annual audit.

(3) Conducting investigations of complaints and referrals of violations as deemed appropriate by the Inspector General.

4. REFERENCES

a. E-Government Act of 2002, Pub. L. 107-347 (Dec. 17, 2002); to include Title III, the Federal Information Security Management Act (FISMA).

b. Executive Order 12958 – Classified National Security Information, as amended, 68 Fed. Reg. 15315 (Mar. 28, 2003).

c. Health Insurance Portability and Accountability Act (HIPAA) of 1996, P.L. 104-191 through 45 CFR Parts 160, 162 and 164 (2006), the unofficial version.

d. Memorandum from the Secretary of Veterans Affairs: Delegation of Authority and Power to VA CIO for the Establishment and Maintenance of Cyber Security Program, (June 28, 2006).

e. National Institute of Standards and Technology Act (15 U.S.C. 278g-3(a).

f. National Institute of Standards and Technology Computer Security Special Publication Series 800.

g. National Institute of Standards and Technology Federal Information Processing Standards (FIPS).

h. OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Systems, February 8, 1996.

i. Request for Advice Relating to the Federal Information Security Management Act (FISMA), 44 U.S.C. §§ 3541-3549, VAOPGADV 5-2004 (Apr. 7, 2004).

j. Responsibilities Regarding National Security and Non-National Security Information and Information Systems, VAOPGADV 12-2003 (Aug. 1, 2003).

k. OMB Memorandum M-02-01, Guidance for Preparing and Submitting Security Plans of Action and Milestones, October 17, 2001.

5. DEFINITIONS

a. **Availability.** Ensuring timely and reliable access to and use of information.

b. **Confidentiality.** Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

c. **Control Techniques.** Methods for guiding and controlling the operations of information systems to ensure adherence to FISMA and other related information security requirements.

d. **Federated IT Management System.** The organizational realignment of information technology operational and maintenance functions under the Assistant Secretary for Information and Technology approved by the Secretary of the Department of Veterans Affairs on March 22, 2006.

e. **Information Owner.** An information owner is the agency official with statutory or operational authority for specified information and responsibility for establishing the criteria for its creation, collection, processing, dissemination, or disposal. Information owner responsibilities extend to interconnected systems or groups of interconnected systems.

f. **Information Resources.** Information in any medium or form and its related resources, such as personnel, equipment, funds, and information technology.

g. **Information Security.** Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability.

h. **Information Security Requirements.** Information security requirements promulgated in accordance with law, or directed by the Secretary of Commerce and NIST, OMB, and, as to national security systems, the President.

i. **Information System.** Discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, whether automated or manual.

j. **Integrity.** Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

k. **National Security System.** 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 an Act of Congress or Executive Order to be kept classified in the interest of national defense or foreign policy.

l. **Plan of Action and Milestones (POA&M**). A POA&M, which is used as a basis for OMB quarterly reporting requirements, includes the following minimum information: (1) description of the security weakness; (2) identity of the office or organization responsible for resolving the weakness; (3) estimate of resources required to resolve the weakness by fiscal year; (4) scheduled completion date; (5) key milestones with estimated completion dates; (6) any changes to the original key milestone dates; (7) the source which identified the weakness (e.g., CIO audit, OIG audit); and (8) the status of efforts to correct the weakness (e.g., started, ongoing, completed).

m. **Security Incident.** An event that has, or could have, resulted in loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures.

n. **Subordinate Plan.** Also referred to as a system security plan, a subordinate plan 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.

o. **Training.** 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.

p. **VA National Rules of Behavior**. A set of Departmental rules that describes the responsibilities and expected behavior of personnel with regard to information system usage.

q. **VA Sensitive Data.** 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. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, records about individuals requiring protection under various confidentiality provisions such as the Privacy Act and the HIPAA Privacy Rule, and information that can be withheld under the Freedom of Information Act. Examples of VA sensitive information include individually-identifiable medical, benefits, and personnel information; financial, budgetary, research, quality assurance, confidential commercial, critical infrastructure, investigatory, and law enforcement information; information that is confidential and privileged in litigation, such as information protected by the deliberative process privilege, attorney work-product privilege, and the attorney-client privilege; and other information which, if released, could result in violation of law, harm, or unfairness to any individual or group, or could adversely affect the national interest or the conduct of Federal programs.