DEPARTMENT OF VETERANS AFFAIRS
Washington, DC 20420

VA DIRECTIVE 6500
Transmittal Sheet
September 20, 2012

MANAGING INFORMATION SECURITY RISK: VA INFORMATION SECURITY PROGRAM

1. REASON FOR ISSUE: To replace Department of Veterans Affairs (VA) Directive 6500, *Information Security Program*, dated August 4, 2006, with a policy that is consistent with VA's information security statutes, 38 United States Code (U.S.C) §§ 5722-5727; the Federal Information Security Management Act (FISMA), 44 U.S.C §§ 3541-3549; and Office of Management and Budget (OMB) Circular A-130, Appendix III, *Security of Federal Automated Information Resources*.

2. SUMMARY OF CONTENTS/MAJOR CHANGES: This Directive, in concert with VA Handbook 6500, establishes VA policy and responsibilities for incorporating National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach;* SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View;* and SP-800-53, *Recommended Security Controls for Federal Information Systems and Organizations,* requirements into VA's information system environment to ensure appropriate security for VA information technology assets that store, process, or transmit VA information.

3. RESPONSIBLE OFFICE: The Office of the Assistant Secretary for Information and Technology (OIT) (005), Office of Information Security (OIS) (005R), Office of Cyber Security (OCS) (005R2) is responsible for the content contained in this Directive.

4. RELATED HANDBOOKS: VA Handbook 6500*, Risk Management Framework for VA Information Systems – Tier 3, VA Information Security Program* and VA Handbook 6500.9, *Security Risk Management – Tier 1 and Tier 2, VA Information Security Program* (to be developed).

5. RESCISSIONS: VA Directive 6500, *Information Security Program*, August 4, 2006.

CERTIFIED BY:

/s/
Roger W. Baker
Assistant Secretary for Information and Technology

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/
Roger W. Baker
Assistant Secretary for Information and Technology

Distribution: Electronic Only

MANAGING INFORMATION SECURITY RISK
VA INFORMATION SECURITY PROGRAM

1. PURPOSE. The purpose of this Directive is to provide the framework for VA's Security Risk Management Program. VA Handbook 6500 and other VA security handbooks provide additional information, procedures/processes, and roles and responsibilities for achieving the goals and steps outlined in this Directive. Managing information security risks will:

a. Ensure that monitoring information system-related security risks is consistent with the Department of Veterans Affairs (VA) mission/business objectives and overall risk strategy established by VA leadership;

b. Support consistent, well-informed, and ongoing risk-based security decisions and maintain acceptable levels of risk through continuous monitoring, while assuring transparency of security and continuous risk management-related information, and reciprocity;

c. Ensure that information security requirements, including necessary security controls, are integrated into VA's enterprise architecture (EA) and system development life cycle (SDLC) processes; and

d. Achieve secure information and information systems within VA through the integration of appropriate risk mitigation strategies within the business operations/missions as well as within the systems.

2. BACKGROUND

a. The E-Government Act, Pub. L. 107-347, 116 Stat. 2899 (2002), recognized the importance of information and information systems to the economic and national security interests of the United States. Title III of the E-Government Act, Federal Information Security Management Act (FISMA), tasked all federal agencies with the responsibility of developing, documenting, and implementing agency-wide information security programs, and providing risk-based information security for the information and information systems that support their operations and assets. FISMA further tasked the National Institute of Standards and Technology (NIST) with the responsibility of developing security standards and guidelines to support these requirements. Of particular importance among the new or revised guidelines are NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*; NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View;* and NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*. SP 800-39 provides a broad-based, organizational view of risk management and provides guidance on developing and implementing the NIST Risk Management Framework (RMF). SP 800-37 addresses the implementation of the NIST RMF at the enterprise and system level and describes the structured six-step process of the RMF. SP 800-53 addresses the security controls that are required by Federal Information Processing Standards (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems* to implement information system security controls to mitigate security risks in a cost-effective manner to protect an agency's information and information systems

b. The NIST RMF promotes a common information security framework to support information security, improve risk management, and encourage collaboration. The RMF process emphasizes:

(1) Building information security capabilities into federal information systems through the application of state-of-the-practice management, operational, and technical security controls;

(2) Maintaining awareness of the security state of information systems on an ongoing basis through enhanced monitoring processes; and

(3) Providing essential information to senior leaders to facilitate decisions regarding the acceptance of risk to the agency, its operations and assets, individuals, and other organizations arising from the operations and use of information systems.

c. The RMF has the following characteristics:

(1) Promoting the concept of near real-time risk management and ongoing information system authorization through the implementation of robust continuous monitoring processes;

(2) Encouraging the use of automation to provide senior leaders the necessary information to make cost-effective, risk-based decisions with regard to an agency's information systems supporting their core mission and business functions;

(3) Integrating information security risk management principles into the EA and SDLC;

(4) Providing emphasis on the selection, implementation, assessment, and monitoring of security controls, and the authorization of information systems;

(5) Linking risk management processes at the information system level to risk-management-based business operations processes at the agency level through a risk executive function; and

(6) Establishing security responsibility and accountability for an agency's business operations processes and for the security controls deployed within its information systems and inherited by those systems (i.e., common controls).

3. POLICY

a. Information and information system risks exist in various forms throughout VA. To effectively address information and information system risks requires the implementation of comprehensive risk-management processes. The NIST RMF was designed to address risk-related concerns at all levels, including the organizational, business process/mission, and systems levels. To achieve the desired level of risk management, VA will institute a three-tiered approach, as described below, to risk management:

(1) Tier 1 – addresses risk from a VA perspective (risk executive function that includes representation from the three administrations) with the development of a comprehensive governance structure and VA-wide risk management strategy that includes:

(a) The techniques and methodologies the Office of Information and Technology (OIT) employs to assess information system-related security risks and other types of risk concerns to VA (i.e., program/acquisition risk, compliance and regulatory risk, financial risk, legal risk, operational risk, reputational risk, safety risk);

(b) The methods and procedures OIT uses to evaluate the significance of identified risks during the risk assessment process;

(c) The types and extent of risk mitigation measures OIT employs to address identified risks;

(d) The level of risk acceptable to VA (risk tolerance);

(e) Monitoring of risk on an ongoing basis by OIT given the inevitable changes to VA information systems and their environments of operation; and

(f) The degree and type of oversight OIT uses to ensure that the risk management strategy is being effectively carried out.

(2) Tier 2 – addresses risk from a mission and business process (administration-program office) perspective, is guided by the risk-based decisions at Tier 1, and includes:

(a) Defining the core mission and business processes for VA (including any derivative or related mission and business processes carried out by subordinate organizations);

(b) Prioritizing mission and business processes with respect to goals and objectives of VA;

(c) Defining the types of information that VA needs to successfully execute the stated mission and business processes and the information flows both internal and external to VA;

(d) Developing a VA-wide information protection strategy and incorporating high-level information security requirements into the core mission and business processes; and

(e) Specifying the degree of autonomy for subordinate organizations that VA permits for assessing, evaluating, mitigating, accepting, and monitoring risk.

(3) Tier 3 – addresses risk from an information system perspective and is guided by the risk decisions at Tiers 1 and 2. Risk decisions at Tiers 1 and 2 impact the ultimate selection and deployment of needed safeguards and countermeasures (i.e., management, operational and technical security controls) at the information system level.

b. VA Handbook 6500 provides additional procedures for implementation of each of VA's RMF steps. This Directive provides the overarching policy-based framework.

c. VA's RMF will provide a disciplined and structured process that integrates information security and risk management activities into the SDLC. The following RMF steps are used primarily in the development and operation of VA's information technology (IT) systems:

(1) ***Categorize*** the information system based on a potential impact analysis (using FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*), as follows:

(a) Categorize the information processed, stored, and transmitted by the information system;

(b) Categorize the information system, based on the results of the categorization of the information above;

(c) Document the security categorization of the system in the system's security plan;

(d) Describe the information system (including system boundary) and document the description in the security plan; and

(e) Register the information system in VA's Office of Information Security (OIS) approved system database - currently called Security Management and Reporting Tool.

(2) ***Select, tailor, and supplement*** an initial set of baseline security controls from VA Handbook 6500, Appendix F based on the security categorization of the system and an OIT assessment of risk and local conditions, as follows:

(a) Select the security controls for the information system and document the controls in the security plan;

(b) Develop a strategy for the continuous monitoring of security control effectiveness and any proposed or actual changes to the information system and its environment of operation; and

(c) Review and approve the security plan.

(3) ***Implement*** the security controls and describe how the controls are employed within the information system and its environment of operation, as follows:

(a) Implement and test the security controls specified in the security plan; and

(b) Document the security control implementation, as appropriate, in the security plan, providing a functional description of the control implementation (including planned inputs, expected behavior, and expected outputs).

(4) ***Assess*** the security controls using OIS-approved assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system, as follows:

(a) Develop, review, and approve a plan to assess the security controls;

(b) Assess the security controls in accordance with the assessment procedures defined in the security assessment plan;

(c) Prepare the security assessment report (SAR) documenting the issues, findings, and recommendations from the security controls assessment; and

(d) Conduct initial remediation actions on security controls based on the findings and recommendations of the SAR and reassess remediated control(s) as appropriate.

(5) ***Authorize*** information system operation based on an analysis of the residual risk posed by the operation of the information system to VA operations and assets, individuals, and other organizations, as follows:

(a) Prepare the plan of action and milestones (POA&M) based on the findings and recommendations of the SAR excluding any remediation actions taken;

(b) Assemble the OIS-approved security authorization package and submit the package to the authorizing official (AO) for adjudication; and

(c) Determine if the residual risk to VA operations (including mission, functions, image, or reputation) and assets, individuals, and other organizations is acceptable.

(6) ***Monitor*** the security controls in the information system on an ongoing basis, as follows:

(a) Determine the security impact of proposed or actual changes to the information system and its environment of operation;

(b) Assess a selected subset of the technical, management, and operational security controls employed within and inherited by the information system in accordance with VA-defined monitoring strategy;

(c) Conduct remediation actions based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in the POA&M;

(d) Update the security plan, SAR, and POA&M based on the results of the continuous monitoring process;

(e) Report the security status of the information system (including the effectiveness of security controls employed within and inherited by the system) to the AO and other appropriate VA officials on an ongoing basis in accordance with the monitoring strategy;

(f) Review the reported security status of the information system on an ongoing basis to determine whether the risk to VA operations and assets, individuals, and other organizations remains acceptable; and

(g) Implement an information system decommissioning strategy, when needed, which executes required actions when a system is removed from service.

4. RESPONSIBILITIES. Following are the responsibilities of agency officials under 38 United States Code (U.S.C) § 5723. Additional security roles and responsibilities for OIT and VA Offices are included in VA Handbook 6500.

a. **Secretary of Veterans Affairs**. 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 commensurate with the risk and magnitude of the potential harm to VA information (collected or maintained by or on behalf of VA) and information systems (used or operated by VA or by a contractor of an agency or other organization on behalf of VA) are implemented to protect against unauthorized access, use, disclosure, disruption, modification, or destruction;

(3) Ensuring that information security management processes are integrated with Department strategic and operational planning and daily business 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; and

(7) Ensuring that the Assistant Secretary for IT, in coordination with VA's Under Secretaries, Assistant Secretaries, and Other Key Officials, reports the effectiveness of VA's Information Security Program, including remedial actions, to Congress, Office of Management and Budget (OMB), and other entities as required by law and Executive Branch direction.

b. **Assistant Secretary for Information and Technology (IT).** The Assistant Secretary for IT, as VA's 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 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 individual's supervisor and ISO;

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

(9) 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;

(10) Ensuring that 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;

(11) Establishing the VA National Rules of Behavior (ROB) for appropriate use and protection of VA information as it is used to support VA missions and functions; and

(12) Establishing and providing supervision over an effective incident reporting system;

c. **Deputy Assistant Secretary (DAS) for Information Security.** In accordance with FISMA, the DAS for Information Security, as VA's Senior/Chief ISO, is responsible for carrying out the responsibilities of the Assistant Secretary for Information and Technology under FISMA, as described above.

d. **Office of Inspector General (OIG)**. In accordance with FISMA, VA OIG is responsible for the following:

(1) Conducting an annual audit of VA's 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; and

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

e. **VA Information Owners (Veterans Health Administration, Veterans Benefits Administration, National Cemetery Administration, and Staff Offices)**. Department information owners are responsible for the following:

(1) Providing assistance to the Assistant Secretary for Information and Technology in identifying the security requirements and appropriate level of security controls for the information system or systems where sensitive personal information is currently created, collected, processed, disseminated, stored or subject to disposal;

(2) Determining who has access to the system or systems containing sensitive personal information, including types of privileges and access rights based upon specific job duties and need to know;

(3) Assisting the Assistant Secretary for Information and Technology in the assessment of the common security controls for systems wherein their business information resides; and

(4) Providing assistance to Administration and Staff Office personnel involved in the development of new systems regarding the appropriate level of security controls necessary for processing and protecting their information.

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

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

(2) Ensuring information security controls that comprise activities that are under their day-to-day operational control or supervision are implemented;

(3) Providing a POA&M to the VA CIO on at least a quarterly basis detailing the status of actions being taken to correct and security compliance failure or policy violation.

(4) Complying with FISMA and other related information security laws and requirements in accordance with VA CIO orders to execute the appropriate security controls commensurate to responding to a VA Network Security Operations Center security bulletin. Such orders from 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 VA take immediate action to comply with orders from the VA CIO to (i) mitigate the impact of any potential security vulnerability, (ii) respond to a security incident, or (iii) implement the provisions of a Security Operations Center Bulletin or Alert. They shall ensure that their VA managers have all necessary authority and means to direct full compliance with such orders from the VA CIO;

(6) Ensuring the VA National ROB or the Contractor ROB is signed, as appropriate, and enforced by all VA system users to ensure appropriate use and protection of the information which is used to support VA mission and functions on an annual basis; and

(7) Assuming the responsibility to ensure that operating systems under their area of responsibility operate at an acceptable level of risk.

g. **Users of VA information systems or VA sensitive information**. These individuals are responsible for the following:

(1) Complying with all Department information security program policies, procedures, and practices.

(2) Completing VA security awareness training on at least an annual basis;

(3) Reporting security/privacy incident information to immediate supervisor, ISO and Privacy Officer after discovery or suspicion;

(4) Complying with orders from the Assistant Secretary for Information and Technology directing specific activities when a security/privacy incident occurs; and

(5) Signing an acknowledgement that they have read, understand, and agree to abide by the VA National ROB (or the Contractor ROB, as appropriate), on an annual basis.