Department of Veterans Affairs
Washington, DC 20420

VA Directive 6004
Transmittal Sheet
September 28, 2009

CONFIGURATION, CHANGE, AND RELEASE MANAGEMENT PROGRAMS

1. **REASON FOR ISSUE**: This Directive establishes Department of Veterans Affairs (VA) policy and responsibilities regarding Configuration, Change, and Release Management Programs for implementation across VA. This directive applies to all VA related components and information technology resources, including contracted Information Technology (IT) systems and services.

2. **SUMMARY OF CONTENTS/MAJOR CHANGES:** This directive establishes VA Configuration, Change, and Release Management Programs in accordance with Federal Information Security Management Act (FISMA) (P.L. 107-347, Title III of the E-Government Act), December 2002, which requires the Agency to establish and implement appropriate Department-wide VA Configuration, Change and Release Management Programs based upon Federal requirements and industry best practices.

3. **RESPONSIBLE OFFICE:** The Office of Information and Technology (OI&T) is responsible for the content of this policy and Process Document(s).

4. **RELATED DIRECTIVE:** VA Directive 6500, Information Security Program. Process documents related to the implementation of this Directive are in development.

5. **RESCISSIONS:** None.

CERTIFIED BY:

/s/
Roger Baker
Assistant Secretary for Information and Technology

BY DIRECTION OF THE SECRETARY VETERANS AFFAIRS:

/s/
Roger Baker
Assistant Secretary for Information and Technology

Distribution: Electronic Only.

CONFIGURATION, CHANGE, AND RELEASE MANAGEMENT PROGRAMS

1. PURPOSE:

The purpose of this Directive is to establish Department-wide Configuration, Change, and Release Management Programs in compliance with the Federal Information Security Management Act of 2002 (FISMA), 44 USC §3541-3549, and P.L. 107-347, Title III, and VA Directive and Handbook 6500, *Information Security Program*, to provide Configuration, Change, and Release Management processes utilizing industry standards to support information technology management across VA. This Directive applies to all VA related components and information technology resources, including contracted IT systems and services.

2. POLICY:

a. VA system owners will meet or exceed all Federal regulatory policies and procedures communicated to government agencies which affect Configuration, Change, and Release Management processes to be implemented on VA information technology assets. Configuration, Change, and Release Management Programs will be implemented and maintained by OI&T. These VA Programs are for all of VA's information systems under ownership, or contracted to vendors or third party servicers on behalf of the VA.

b. In support of VA policy, public law and other Federal guidance, each VA system owner must document, implement, and maintain Configuration, Change, and Release Management plans and processes. These processes will include the following:

(1) Documenting and maintaining the configuration baseline(s) applicable to the deployed system;

(2) Effectively managing and tracking all system configuration and associated document changes to maintain each operational system's authorized security posture, as well as the integrity, availability and maintainability of the system;

(3) Effectively planning to ensure the ability to reverse a deployment or implementation;

(4) Effectively tracking all system changes made, including installation of patches, to hardware, software, firmware, and documentation, through development, approval, testing, and controlled implementation of changes delivered into production environments; and

(5) Leveraging the risk management program in conjunction with the business owner so that proper risk-based decisions are made and documented throughout the development and system lifecycles in direct support of system security authorization efforts and VA policy.

c. Information systems are typically dynamic causing system state to change frequently as a result of upgrades to hardware, software, firmware or modifications to the surrounding environment in which a system resides. Industry standards to include Government Accounting Office (GAO), Office of Management and Budget (OMB) and several National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS), and Special Publications (SP) (800 Series regarding information and systems security) stress that information systems (e.g., general support systems, major applications, and minor applications) must document and assess the potential impact that proposed system changes may have on the operational processes and security posture of the system. IT best

industry practices recognize this as an essential aspect of effective system management, as well as being part of the continuous monitoring and maintenance of a system's security accreditation of Federal systems required by FISMA. These practices support optimum production system availability and include:

(1) Using standardized documented methods, processes, and procedures defined in the process document for all changes;

(2) Effectively tracking and communicating all system changes made to hardware, software, firmware, and documentation, through planning, approving, notifying, developing, testing, scheduling, and managing the release and implementation of changes;

(3) Making effective risk-based decisions to maintain each system's mission capability, authorized security posture and minimize risk. Risk-based decision making will equally involve IT and the business owner; and

(4) Effectively utilizing VA resources.

d. Change Control Boards (CCB) will be established as appropriate to ensure changes to the VA infrastructure, or contracted VA systems are reviewed and processed in accordance with established VA Configuration, Change, and Release Management processes and procedures. At the Department level, an Executive Change Control Board (ECCB) will be established to provide oversight for the implementation of these processes and to recommend improvements to this policy to the Assistant Secretary for OI&T.

e. ECCB Board membership will consist of Executive representation or designee in the following areas:

(1) Enterprise Operations and Field Development (EO&FD).

(2) Office of Enterprise Development (OED).

(3) Information Protection and Risk Management (IP&RM).

(4) Enterprise Strategy, Policy, Plans, & Programs (ESPPP).

(5) IT Resource Management (RM).

(6) Lines of business representatives (i.e., Veterans Health Administration, Veterans Benefits Administration, and National Cemetary Administration).

(7) Change Managers.

3. RESPONSIBILITIES

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

(1) Ensuring VA adopts Department-wide VA Configuration, Change, and Release Management Programs and otherwise complies with FISMA and other related Federal policies and requirements;

(2) Ensuring VA Configuration, Change, and Release Management Programs and related processes are integrated with strategic and operational planning processes;

(3) Ensuring Under Secretaries, Assistant Secretaries, and Other Key Officials support the VA Configuration, Change, and Release Management Programs with regard to information systems and services under their control; and

(4) Ensuring the Assistant Secretary for Information Technology, in coordination with VA Under-Secretaries, Assistant Secretaries, and Other Key Officials, reports on the effectiveness of the VA Configuration, Change, and Release Management Programs to Congress, OMB, Government Accountability Office (GAO), and other entities as required by law and Executive Branch direction.

b. **Under Secretaries and Assistant Secretaries:** These officials are responsible for providing expectations of the businesses needs, risks, and priorities in regards to Configuration, Change and Release Management with standing memberships in planning and governance activities to ensure a successful outcome of this Directive.

c. **Assistant Secretary for Information and Technology or VA Chief Information Officer (CIO)**: The VA CIO is responsible for:

(1) Issuing and approving policies, procedures and guidance for implementing and coordinating the VA Configuration, Change, and Release Management Programs within VA;

(2) Implementing the VA Configuration, Change, and Release Management Programs, as appropriate;

(3) Directing, monitoring, and enforcing implementation, maintenance and compliance with the VA Configuration, Change, and Release Management Programs; and

(4) Periodically testing and evaluating IT components to determine effectiveness and compliance with the VA Configuration, Change, and Release Management Programs.

d. **Deputy Assistant Secretary, Enterprise Operations and Field Development (DAS EO&FD) and Deputy Assistant Secretary, Office of Enterprise Development (DAS OED):** The DAS EO&FD and DAS OED are responsible for:

(1) Directing Configuration, Change, and Release Management activities across VA and for ensuring coordination among VA Deputy Assistant Secretaries as required to ensure full implementation of this policy;

(2) Ensuring adherence to this policy for applicable VA employees, contractor personnel and other non-Government employees; and

(3) Establishing reporting and other requirements associated with Configuration, Change, and Release Management to document the status of compliance with this policy.

e. **The VA Chief Information Security Officer (CISO):** The VA CISO shall establish, implement, communicate, and enforce minimum security configuration standards on all Departmental systems and networks that process, store, or communicate VA information.

f. **Executive Change Control Board (ECCB):** The ECCB shall be responsible for:

(1) Establishing a secure and sound configuration management framework ensuring definition and maintenance of configuration baselines and the identification, management and tracking of associated hardware, software and documentation configuration items for each VA system;

(2) Ensuring all changes to configuration items adhere to VA policy are documented, tested, and approved;

(3) Ensuring emergency change procedures are documented and approved by the CCB and that emergency change actions are documented, either prior to the change or immediately after the fact;

(4) Ensuring these change procedures maintain the operational system's authorized security posture, as well as the integrity, availability and maintainability of the system;

(5) Ensuring that VA Configuration, Change, and Release Management process documents are maintained as a Configuration Item (CI) component and placed under configuration management control;

(6) Coordinating with the other elements of the Service Line Management organization, as necessary, to ensure appropriate interface of management and control activities;

(7) Delegating authority, where appropriate, for approving changes to lower level boards; and

(8) Reporting on the effectiveness of the Configuration, Change, and Release Management activities to executive leadership.

g. All OI&T Employees and VA Contractors: These individuals are responsible for:

(1) Implementing Configuration, Change, and Release Management activities across VA;

(2) Ensuring coordination among other OI&T employees and contractors as required to ensure full implementation of this policy; and

(3) Ensuring communication with other VA offices as required, to establish and maintain coordination between business offices and OI&T.

4. REFERENCES

a. Best Practices for Rational Unified Process (RUP);

b. CMMI Continuous Representation (Model) v 1.1;

c. FISMA (P.L. 107-347, Title III), December 2002;

d. NIST FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*;

e. NIST FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*;

f. IEEE/EIA 12207, Industry *Implementation of International Standard*;

g. Information Technology Infrastructure Library (ITIL);

h. ISO 10007, *Quality Management Guidance for Configuration Management*, 2003;

i. ISO/IEC: ISO/IEC12207 *Standard for Information Technology Software Life Cycle Processes*, 1996;

j. ISO/IEC 12207, *International Standards Organization: Implementation of Information Technology—Software Life Cycle Processes*, 1998;

k. MIL-HDBK-61A (SE), *Military Handbook for Configuration Management Guidance*, 2001;

l. National Institute of Standards and Technology (NIST), Special Publication (SP) 800-12, *Introduction to Computer Security: The NIST Handbook*;

m. NIST SP 800-30, *Risk Management Guide for Information Technology Systems;*

n. NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems;*

o. NIST SP 800-40; *Creating a Patch and Vulnerability Management Program*

p. NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*;

q. NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*;

r. NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*;

s. NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*;

t. NIST SP 800-64, Revision 1, *Security Considerations in the Information System Development Life Cycle*;

u. NIST SP 800-65, *Integrating Security into the Capital Planning and Investment Control Process;*

v. NIST SP 800-70, *Security Configuration Checklists Program for IT Products -- Guidance for Checklists Users and Developers;*

w. OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources;*

x. OMB Circular A-130, Appendix III, *Transmittal Memorandum #4, Management of Federal Information Resources;*

y. Project Management Institute (PMI);

z. Project Management Institute (PMI);

aa. Service Transition Volume of the ITIL Lifecycle Publication Suite, authored by the UK Office of Government Commerce, JUN 2007; and

bb. VA Directive and Handbook 6500, *Information Security Program*.

5. DEFINITIONS:

a. **Authorization:** A formal declaration by a Designated Approving Authority (DAA) that an Information System (IS) is approved to operate in a particular security mode at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards.

b. **Certification:** Comprehensive evaluation of the technical and non-technical security features of an IS to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements.

c. **Change Management:** Change management provides standardized methods for implementing change in an IT infrastructure. Changes may also be introduced to reduce costs or improve services.

d. **Configuration Baseline:** The configuration management baseline is the starting point - an initial configuration entered in the Configuration Management Database (CMDB).

e. **Configuration Item:** Configuration items are individual elements to be added to the Configuration Management Database (CMDB) and assigned unique identifiers. They are standardized according to version, serial, and release, with appropriate nomenclature. Configuration items have three major attributes which are technical, ownership, and relationship.

f. **Configuration Management:** Configuration management is the process of identifying, controlling, verifying, and showing the relationship among all infrastructure components.

g. **Configuration Management Database (CMDB):** The repository that stores the identity of each component of the information infrastructure to include hardware, software, and documentation assets. Documentation is included in the database that is procedural, referential and instructional.

h. **General Support System:** Interconnected set of information resources under the same direct management control which share common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a Local Area Network (LAN) including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization.

i. **Information System (IS):** The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information. An IS can be a general support system or a major application.

j. **Major Application:** An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. ***Note:*** *All federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and*

should be treated as major. Adequate security for other applications should be provided by security of the system in which they operate.

k. **Major Change:** Major changes include: an increase in the sensitivity or criticality of a system; an increase in threat level; policy change, a change in operating system (base platform); a change to security relevant software; a change to hardware possibly affecting the security architecture; an increase in interconnection with other systems outside the accreditation boundary; or significant changes in the security requirements that apply to the system. When there is a major change to the system, VA officials with significant information and information system responsibilities must re-evaluate the sensitivity of the system, risks, and mitigation strategies.

l. **Release Management:** Release management is the process of introducing approved and tested release packages into the infrastructure in a planned and orderly manner.

m. **Service:** A software component participating in a service-oriented architecture that provides functionality or participates in realizing one or more capabilities.

n. **Service-Line Management (SLM):** A combination of trusted management and business planning techniques that can improve the way IT Service is delivered.

o. **System Owner:** An individual responsible for the proper technical and business functioning of an IT system. System owners have ultimate authority over the operation and maintenance of an IT system. System owners work with business managers to ensure that the system is providing the automation support required to perform their functions.