CONFIGURATION, CHANGE AND RELEASE MANAGEMENT PROGRAMS

1. **REASON FOR ISSUE**: This updated directive establishes the 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 information technology (IT) hardware, software and communications components and IT resources, including contracted IT systems and services.

2. **SUMMARY OF CONTENTS/MAJOR CHANGES:** This directive establishes VA Configuration, Change and Release Management Programs in accordance with the Federal Information Security Modernization Act of 2014 (FISMA), 44 U.S.C. § 3551-3559 (Pub. L. 113-283), 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. Major changes include new terminology, change integration with Office of Information and Technology (OIT) Agile and processes.

3. **RESPONSIBLE OFFICE:** Office of Information and Technology (OIT) (005), Infrastructure Operations (IO), Enterprise Change, Release and Configuration Management.

4. **RELATED DIRECTIVE:** VA Directive 6500, VA Cybersecurity Program, dated February 24, 2021.

5. **RESCISSION:** VA Directive 6004, Configuration, Change and Release Management Programs, dated September 28, 2009.

CERTIFIED BY:

/s/
Guy T. Kiyokawa
Assistant Secretary for
Enterprise Integration

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/
Kurt DelBene
Assistant Secretary for
Office of Information and Technology
and Chief Information Officer

CONFIGURATION, CHANGE AND RELEASE MANAGEMENT PROGRAMS

TABLE OF CONTENTS

CONFIGURATION, CHANGE AND RELEASE MANAGEMENT PROGRAMS

1. INTRODUCTION AND PURPOSE.

a. The Department of Veterans Affairs (VA), Office of Information and Technology (OIT) established formal Change Control and Release Management guidance via the “Office of Information and Technology Release Management Program” (VAIQ 7399362) memorandum (memo) published on November 8, 2013. Since then, both programs, along with Service Configuration Management (SCM) in OIT, have evolved into mature enterprise programs that are closely integrated with the IT Service Management (ITSM) Suite. Today, one will find standardized processes, controls, communications and guidance designed to be used by the entire enterprise. OIT shall use this directive along with its process document and related work instructions to adequately manage all IT change, configuration and release activities required by this directive.

b. The purpose of this directive is to establish/maintain Department-wide Configuration, Change and Release Management Programs in compliance with the Federal Information Security Modernization Act of 2014 (FISMA), 44 U.S.C. § 3551-3559 (Pub. L. 113-283), VA Directive 6500, VA Cybersecurity Program, the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Rev 5 Security and Privacy Controls for Federal Information Systems and Organizations and NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems. This directive applies to all VA-related IT hardware, software and communication components and IT resources, including contracted IT systems and services.

2. POLICY.

a. VA System Owners (see Definitions) and contractors shall 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 IT assets. Configuration, Change and Release Management Programs will be implemented and maintained by OIT. These VA Programs are for all VA Information Systems (IS) 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, communicate, implement and maintain a system Configuration Management Plan (CMP) outlining their Configurations, Change and Release practices. These processes will include the following:

(1) Document and maintain the information system configuration baseline(s) applicable to the deployed system.

(2) Document and maintain the business and technical ownership of Configuration Items (CIs) in a Configuration Management Database (CMDB) through service and information system baseline management responsibilities supporting on-going service delivery by ensuring configuration information is identified, base-lined and controlled as changes occur. (See Section 3: Responsibilities of this directive).

(3) Log any change to a production environment CI in the OIT ITSM system—through automation or manually. Each change must be approved, scheduled and communicated to all affected stakeholders. A Change Request is the only approved mechanism by which official approval of a change is recognized and only approved change requests and release records shall populate OIT maintenance and deployment calendars. Approvals are documented within the change and release records per specific groups designated for each record.

(4) Compliance through increased accountability and traceability of CI attribute and relationship changes via participation in SCM Program activities involving continuous validation and certification of CIs and Mapped Application Services.

(5) Manage and track all system configuration and associated document changes to maintain each operating system's authorized security posture, as well as the integrity, availability, maintainability and confidentiality of the system.

(6) Plan to ensure the ability to reverse a deployment or implementation.

(7) Maintain test results of all production change requests. If pre-deployment and post-deployment validation testing cannot be conducted, make sure change owner keeps a written record of why the testing could not be completed and any mitigating factors. Test results need not be placed in the change record but should be available for any auditing purposes or tied to a release record.

(8) Track all system changes made, including installation of patches to hardware, software and firmware through development, testing and approval. Pre-Implementation and Post Deployment test results must be documented and kept for at least one (1) year in case needed for Inspector General (IG) audits. This is further documented in currently published work instructions.

(9) Leverage risk and impact management in conjunction with the business owner to ensure 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.

(10) Upload of the completed and approved CMP into the Enterprise Mission Assurance Support Service (eMASS) system, by the IS owner or system steward, per the Office of Information Security (OIS) Authorization Requirements Standard Operating Procedures (SOP).

c. Information Systems are typically dynamic, causing system operational status to change frequently because of upgrades to hardware, software, firmware, or modifications to the surrounding environment in which a system resides. Industry standards to include U.S. Government Accountability Office (GAO), Office of Management and Budget (OMB) and several NIST, Federal Information Processing Standards (FIPS) and SP (800 series regarding IS security) stress that IS (e.g., information systems and hosted 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 industry best 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) Use of standardized documented methods, processes and procedures defined in process documentation.

(2) Tracking and communicating all production system changes made to hardware, software and firmware and through planning, approving, notifying, developing, testing, scheduling and managing the release and implementation of change requests through the OIT-approved Change, Release system. If change induces new risks to system security posture, The OIS, Information Security Risk Management (ISRM) must be notified for review of change before final approval.

(3) Making effective risk-based decisions, per the ServiceNow Change Risk Survey to maintain each system's mission capability and authorized security posture and to minimize risk. Risk-based decision-making will equally involve IT and the business owners. An evaluation of whether a Security Impact Analysis (SIA) is required during the risk analysis. ISRM should be consulted for high or critical security impacts, requiring an SIA before change approval.

(4) Use of VA IT Governance and ITSM Tool resources.

d. Configuration Control Boards (CCB) will be established at the product level, 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 enterprise Change Advisory Board (CAB) is

established to provide oversight for the implementation of these processes and to recommend improvements to this policy to the Assistant Secretary for OIT.

3. RESPONSIBILITIES.

a. **Under Secretaries, Assistant Secretaries and Other Key Officials** shall:

(1) Provide guidance concerning the business needs, risks and priorities regarding Configuration, Change and Release Management with standing memberships in planning and governance activities related to change control and configuration management to ensure a successful outcome of this directive.

(2) Support the VA Configuration, Change and Release Management Programs regarding information systems and services under their control.

(3) Report on the effectiveness of the VA Configuration, Change and Release Management Programs to Congress, OMB, GAO and other entities as required by Federal regulations.

b. **Assistant Secretary for Information and Technology/Chief Information Officer (CIO).** The VA CIO shall:

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

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

(3) Issue and approve policies, procedures and guidance for implementing and coordinating the VA Configuration, Change and Release Management Programs within VA.

(4) Implement the VA Configuration, Change and Release Management Programs, as appropriate.

(5) Direct, communicate and enforce, compliance with the VA Configuration, Change and Release Management Programs.

(6) Annually test and evaluate IT components to determine effectiveness and compliance with the VA Configuration, Change and Release Management Programs.

c. **Deputy Chief Information Officer (DCIO), Infrastructure Operations** shall:

(1) Direct Configuration, Change and Release Management activities across VA and establish coordination among VA Deputy Assistant Secretaries as required to ensure full implementation of this policy.

(2) Ensure adherence to this directive for applicable VA employees, contractor personnel and other non-Government employees.

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

(4) Ensure the Continuous Integration, Continuous Delivery and Continuous Deployment of DSO Services is documented along with the change process.

d. **VA Chief Information Security Officer (CISO)** shall: implement a VA-wide cybersecurity program that establishes an organization, mission and system-level change management processes in accordance with NIST guidelines.

e. **Enterprise Change Advisory Board (CAB)** shall:

(1) Establish a secure configuration management framework ensuring definition and maintenance of information system configuration baselines and the identification, management and tracking of associated hardware, software and documentation Configuration Items (CIs) for each VA system.

(2) Ensure all production changes to CIs adhere to VA policy are documented, tested and approved.

(3) Ensure emergency change requests are documented either prior to the change or immediately after the fact.

(4) Ensure these change procedures maintain the operational system’s authorized security posture, as well as the integrity, availability, maintainability and confidentiality of the system.

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

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

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

f. **Configuration Control Boards (CCB)** shall:

(1) Provide a group comprised of change owners, technical points of contact, business representatives and any other change stakeholders at the change group level. The CCB groups should meet at least weekly to review and approve standard and lower risk normal changes. CCB's are subordinate to the enterprise CAB and can escalate their changes to the CAB for final adjudication and approval, if needed.

(2) Evaluate and provide joint initial technical and business approvals on change requests. Ensure pre-production testing is properly executed and documented by attaching test plans and test results to the change request. If testing cannot be completed, attach a justification as to why testing could not be completed and any mitigating factors, per NIST 800-53 CM-3.

(3) CCBs are organized and meet at change group levels that are lower in authority and scope to the enterprise CAB which covers the review and approval of critical and high-risk normal change adjudication.

(4) CCB groups will help deconflict any changes they own against the enterprise change calendar, use the appropriate maintenance windows and avoid blackout windows when scheduling any normal system maintenance via change control.

g. **System Owners**. System Owners are responsible for the accuracy of their mapped application services and will follow established procedures for updates to make configuration data available in response to information requests or reporting needs. System Owners shall:

(1) Implement Configuration, Change and Release Management activities across VA.

(2) Ensure coordination among OIT employees and contractors as required to ensure full implementation of this policy.

(3) Ensure communication with other VA offices as required, to establish and maintain coordination between business offices and OIT. System Owners are typically change request owners as well. Change Owners are responsible for communicating all upcoming maintenance and deployment activities that tie to their systems.

(4) Perform the Configurations, Change and Release processes listed under the "Policy" section.

4. DEFINITIONS.

a. **Authorization:** A formal declaration by a Designated Approving Authority that an 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. (Source(s): NIST SP 800-18 Rev. 1)

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. (Source(s): National Security Information Automated Information Systems)

c. **Change Control:**

(1) Definition from change policy. Change control helps coordinate technical changes to maintain throughput and stability. Examples may include:

(a) Any change to a production environment CI.

(b) Reboots on shared hardware (e.g., servers, storage, customer facing applications, network gear, etc.), or anything affecting the operating state of the shared hardware.

(c) Change requests *not* required for single user devices (e.g., workstations and/or laptops).

(d) Changes to vendor-controlled hardware/software (HW/SW) that impact VA. VA OIT Product owner responsible for entering informational change on planned maintenance or HW/SW lifecycle events (e.g., add server, decommission server, etc.).

(e) Changes from VA partner owned HW/SW affecting VA. Product owner responsible for entering informational change on planned maintenance or HW/SW lifecycle event (e.g., add server, decommission server, etc.).

d. **Configuration Item:** A Configuration Item (CI) is defined as any component that is managed to deliver an IT service. CIs are stored in a CMDB. Information about each CI is recorded and maintained throughout its lifecycle by SCM and IT Asset Management process activities. CIs are composed of attributes which include unique identifiers, as well as technical, ownership and relationship information. Examples of CIs include IT services, hardware, software, location data and may include documentation. (Source: ITIL V4)

e. **Configuration Management Database:** 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. (Source: ITIL V4)

f. **Deployment management:** The technical vehicle that looks at how to move new or changed service.

g. **Incident Caused by Change (ICC):** An incident resulting from a planned or unplanned change to a production CI. For example, if the incident is the result of an addition, modification, or removal of any service, service component, or CI, then it is considered an ICC. Otherwise, it would not be recorded as an ICC. An ICC can be internal or external based on the organization that owns the service or configuration item that was the root cause.

    (1) **Internal ICC**: ICC for which OIT can control remediation and communication efforts. For example, VA owned HW/SW/Configuration or contracted vendor owned HW/SM/Configuration.

    (2) **External ICC**: ICC for which OIT cannot control the remediation and communication efforts. For example, non-contracted vendor or partner.

        (a) Partner – Organization affecting VA OIT operations and not bound by a contract. Sometimes, a Memorandum of Agreement (MOA) may be present, which should define change control requirements.

        (b) Vendor – Party bound by official VA contract, which should have OIT change control specific contract verbiage.

h. **Information System:** Interconnected set of information technology resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications and people. A system can be, for example, a Local Area Network 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. (Source: ITIL V4)

i. **Information System Configuration Baseline:** The information system configuration management baseline is the starting point — an initial configuration entered in the CMDB. (Source: ITIL V4)

j. **Product Owner:** A member of the Agile Team responsible for defining Stories and prioritizing the Product Backlog to streamline the execution of program priorities while maintaining the conceptual and technical integrity of the Features or components for the team. (Source: VASI Glossary of Terms)

k. **Release Management:** Focuses on when and how to make new or updated components available to users.

l. **Service:** A software component participating in a service-oriented architecture that provides functionality or participates in realizing one or more capabilities. (Source: ITIL V4)

m. **Service Line Management:** A combination of trusted management and business planning techniques that can improve the way IT Service is delivered. (Source: ITIL V4)

n. **System Owner:** Person or organization that has responsibility for the development, procurement, integration, modification, operation and maintenance and/or final disposition of an IS. (Source: ITIL V4)

5. REFERENCES.

a. E-Government Act of 2002 published December 17, 2002.

b. Office of Information and Technology Release Management Program (VAIQ 7399362) memo published on November 8, 2013.

c. NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems published August 2011.

d. Federal Information Security Modernization Act of 2014 published December 18, 2014.

e. FIPS 199, Standards for Security Categorization of Federal Information and Information Systems dated February 2004.

f. FIPS 200, Minimum Security Requirements for Federal Information and Information Systems dated March 2006.

g. NIST SP 800-12, Revision 1, Introduction to Computer Security published June 2017.

h. NIST SP 800-30, Revision 1, Guide for Conducting Risk Assessments published September 2012.

i. NIST SP 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy published December 2018.

j. NIST SP 800-40, Revision 4, Guide to Enterprise Patch Management Technologies published April 2022.

k. NIST SP 800-47, Revision 1, Managing the Security of Information Exchanges published July 2021.

l. NIST SP 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations published September 2020.

m. NIST SP 800-59, Guideline for Identifying an Information System as a National Security System published August 2003.

n. NIST SP 800-60 Volume 1, Revision 1, Guide for Mapping Types of Information an Information System to Security Categories published August 2008.

o. NIST SP 800-70, Revision 4, National Checklist Program for IT Products: Guidelines for Checklist Users and Developers published February 2018.

p. NIST Glossary (Major Applications Definition).

q. VA Directive 6500, VA Cybersecurity Program published February 24, 2021.

r. Handbook 6500, Risk Management Framework for VA Information Systems VA Information Security Program published February 24, 2021.

s. Capability Maturity Model Integration (CMMI), Version 1.1 - Continuous Representation posted January 3, 2002.

t. Information Technology Infrastructure Library (ITIL).

u. International Standardization Organization (ISO) 10007, Quality Management – Guidelines for Configuration Management published March 2017, corrected July 2019.

v. IEEE/ISO/IEC 12207, ISO/IEC/IEEE International Standard – Systems and Software Engineering – Software Life Cycle Processes, published September 28, 2017.

w. Committee on National Security Systems Instruction (CNSSI) 4009, CNSS Glossary, published April 6, 2015.

x. Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors published August 27, 2004.

y. VA Systems Inventory (VASI) Glossary and Business Rules – VA | Enterprise Architecture