VA Enterprise Design Patterns
Information Technology (IT) Service Management

Configuration Management

OFFICE OF TECHNOLOGY STRATEGIES (TS)
OFFICE OF INFORMATION AND TECHNOLOGY (OI&T)

VERSION 2.0
DATE ISSUED: FEBRUARY 2017

APPROVAL COORDINATION

Gary Marshall
Director, Technology Strategies, ASD

Paul A. Tibbits, M.D.
DCIO Architecture, Strategy, and Design

REVISION HISTORY

Version	Date	Approver	Notes
1.0	November 2015	Jaqueline Meadows-Stokes	Updated based on stakeholder review and public forum collaborative feedback. Addressed Section 508 Compliance.
2.0	February 2017	Jaqueline Meadows-Stokes	Updated missing and outdated sections, and updated with feedback from stakeholders during community review.

CONTENTS

QUICK JUMP

Select an icon to skip to a section.

Current Capabilities

Future Capabilities

Use Cases

One-VA Technical Reference Model

The Veteran-Focused Integration Process

Enterprise Design Pattern Scope

---

1 INTRODUCTION

An Information Technology (IT) infrastructure that spans across numerous hosting environments requires a consistent approach to managing its service assets and Configuration Items (CI). A common set of IT Service Management (ITSM) tools and processes is required to ensure flexibility to changing business needs and to adhere to enterprise security policies. The framework addresses the following challenges:

- ITSM CM capabilities are not fully utilized and are dispersed geographically.
- CM processes and IT services assets are not standardized processes.
- An enterprise-level Configuration Management System (CMS) has not been identified.
- Ownership and resources to manage an enterprise CMS have not been identified.

The following sections establish a framework for enterprise-wide Configuration Management (CM) capabilities.

1.1 Business Problem

A unified and consistent CM process is needed within the enterprise in order to ensure the security of Personally Identifiable Information (PII), Personal Health Information (PHI), and controlled information that is stored within the technology infrastructure at the Department of Veterans Affairs (VA). This Enterprise Design Pattern (EDP) will provide capability guidance for a centralized CM process that ensures flexibility to changing business needs and requirements.

This will result in greater security and a more agile methodology for monitoring and managing configuration.

1.2 Business Need

The VA Office of the Inspector General (OIG), the Federal Information Security Management Act (FISMA), and Federal Identity, Credential, and Access Management (FICAM) have identified material weaknesses stemming from a fragmented approach to IT asset management. These assets include all of the CIs that make up IT services. A consistent approach and toolset for managing these CIs ensures that the entire infrastructure satisfies functional and non-functional requirements, including all Service Level Agreements (SLAs). As a result, all infrastructure hosting environments have unified control over potential vulnerabilities; and unexpected configuration changes that inhibit VA's ability to meet customer expectations.

1.3 Business Case

This EDP will provide capability guidance to CM within the enterprise. This provides a common set of ITSM tools and processes for CM for VA systems. This EDP will provide positive business benefits, as outlined in Table 1.

TABLE 1: BUSINESS BENEFITS

Business Benefits	Description
Greater Flexibility for Changing Business Needs	An enterprise level CMS will increase CM flexibility across the enterprise.
Increased Security	A centralized CMS will provide a greater security posture for IT systems within the enterprise.
Standardization of Processes	Enterprise level CM will standardize processes, thereby reducing costs and stewarding VA resources.

1.4 Approach

VA's near-term approach to establishing and deploying an enterprise CM capability includes the following activities:

- Establishing a standard CM methodology (ongoing)
- Evaluating current CM toolset (ongoing)
- Determining parameters for the selection of an enterprise-wide CM toolset (planned)
- Processing the national implementation of standard CM methodology and toolset (planned)

The deployment of an enterprise-wide CM capability will enable a logical view of all CIs across the enterprise. This capability will support the evaluation of IT assets against the One-VA Technical Reference Model (TRM) to ensure that approved products are used in the enterprise.

2 CURRENT CAPABILITIES AND LIMITATIONS

The following figure provides an overview of the current CM process. The limitations that exist could potentially result in the introduction of security vulnerabilities within the enterprise. The subsequent sections provide additional details and recommendations for addressing these issues.

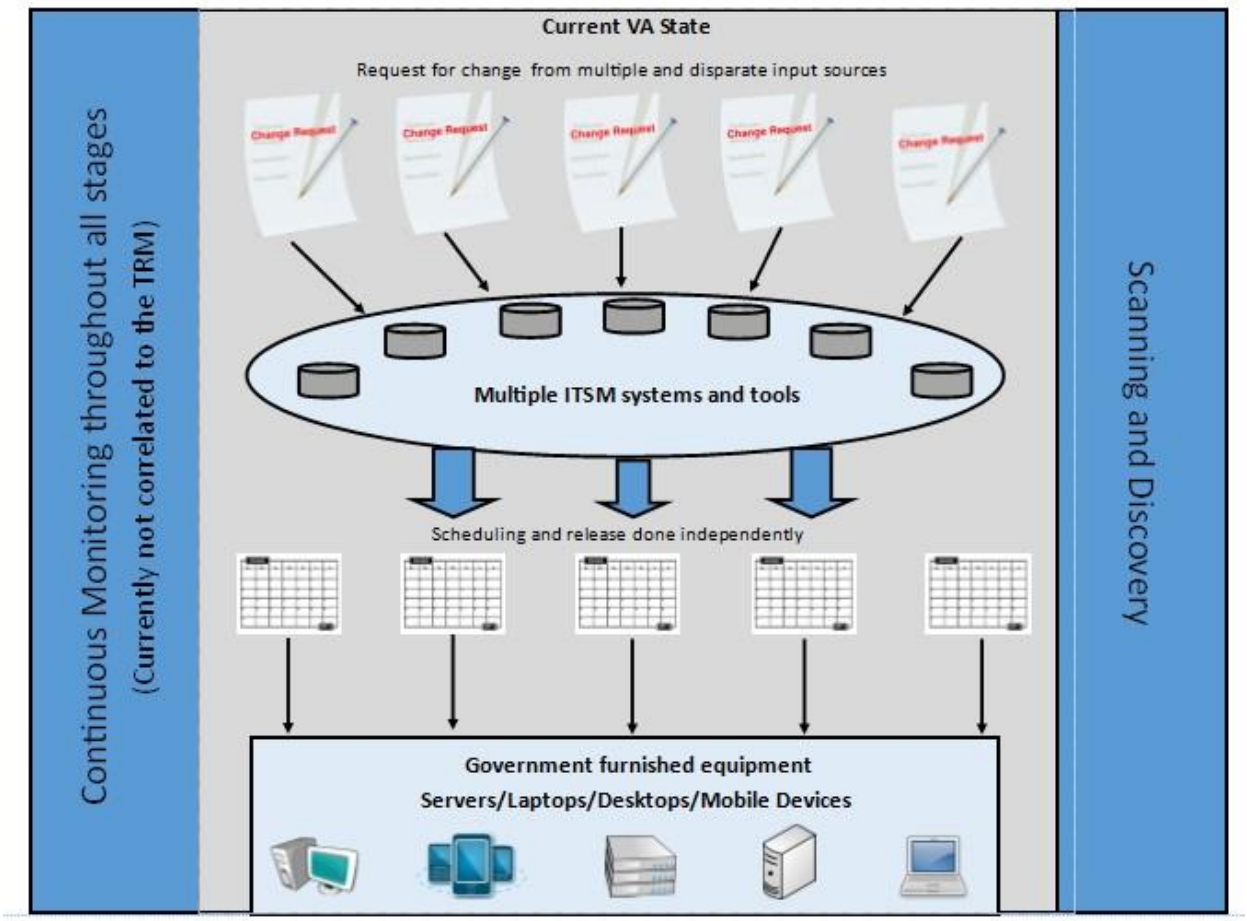

FIGURE 1: CONFIGURATION MANAGEMENT CURRENT STATE

2.1 Inconsistent Baseline Configuration

The lack of a standard CM methodology poses risks to maintaining consistent configuration baselines aligned to VA security policies. A 2015 OIG FISMA audit identified varying levels of compliance with the United States Governance Configuration Baseline (USGCB) standards. This

audit identified numerous endpoint devices that were not configured to a common security configuration standard; these included security vulnerabilities from default network services, excessive permissions, weak administrator passwords, and outdated versions of network operating systems.

2.2 Underutilized Scanning and Discovery Tools

Network management and asset discovery tools from IBM and Microsoft are currently deployed at the program level. These solutions provide limited enterprise capability to measure exposures, fix vulnerabilities automatically, validate security compliance, and generate alerts and reports for vulnerabilities.

International Business Machines (IBM) BigFix scans the entire VA enterprise on a monthly basis. A semi-automated process has been implemented to extract results from BigFix and other VA-owned tools. The results are normalized, reviewed, and assessed for false positives before an actionable list of items for further investigation is returned to field personnel.

Microsoft System Center Configuration Manager (SCCM) 2007 and 2012 are used to "push" patches to assets within the Microsoft platform. BMC Atrium Discovery and Dependency Mapping (ADDM) has been deployed at Enterprise Operations (EO) data centers and is primarily used to identify EO assets. ADDM has the ability to normalize data against a product catalog that is updated twice annually.

2.3 Multiple Configuration Management Databases

Different VA organizations use different CMS products, including disparate CM databases (CMDB) that cover different portions of VA's CIs. VA does not have a complete list of the technical capabilities required from a CMDB system. As a result, the Office of Information & Technology (OI&T) cannot ensure that it employs the optimal tool set to provide all needed capabilities, without duplication or gaps.

3 FUTURE CAPABILITIES

A consistent CM approach throughout VA adheres to the following constraining principles:

- Enterprise-level CM methodology
- Standard secure baseline configurations
- Standard automated scanning and discovery tools
- Federated, enterprise-wide CMS tool

TABLE 2: CONFIGURATION MANAGEMENT BUSINESS BENEFITS

Business Benefits	Description
Enterprise Level Configuration Management Methodology	Utilizing an enterprise-level CM methodology would mean a more agile, secure, and efficient process for CM within the enterprise.
Federated, Enterprise-Wide CMS tool	Managing CM items with a single tool would ensure a single point of control for the process and procedure that is related to CM within the enterprise.

The following subsections provide guidance and additional resources for each principle.

3.1 Enterprise-Level Configuration Management Methodology

The enterprise-wide CM approach aligns to the CM process already published in ProPath and aligned to the National Institute of Standards and Technology (NIST) SP 800-128, as described in Appendix D. The following figure shows the high-level CM process that is based on NIST guidance.

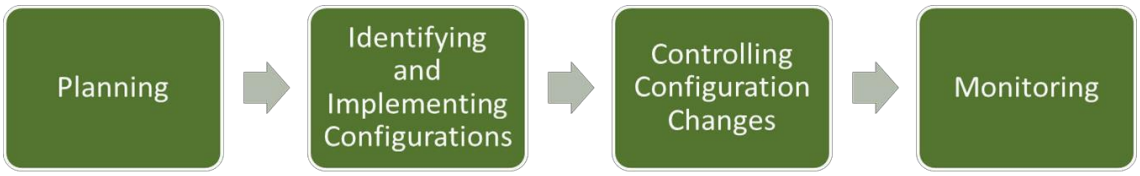

FIGURE 2: ITSM CONFIGURATION MANAGEMENT PHASES PER NIST SP 800-128

Implementation considerations for enterprise CM that are based on the four stages are listed below.

- **Planning:** Planning CM will:
  - Define how the types of assets and CIs are to be selected, grouped, classified, and defined by the appropriate characteristics; to ensure they are manageable and traceable throughout the lifecycle.
  - Define the approach to identification, uniquely naming and labeling all the assets or service components of interest across the service lifecycle; and define the relationships between them.
  - Define the roles and responsibilities of the owner or custodian of the configuration item type at each stage of its lifecycle (e.g., the service owner for a service package or release at each stage of the service lifecycle).
- **Identifying and Implementing Configurations**: An enterprise secure baseline will address configuration settings, software loads, patch levels, documentation, how

information is physically or logically arranged, and how various security controls are implemented. Automation will enable tool interoperability and baseline configuration uniformity across the information system.

- **Controlling Configuration Changes**: Changes to CIs will be approved prior to their implementation, with the exception of an emergency change. Access restrictions will be established, including:
    - Access controls
    - Process automation
    - Abstract layers
    - Change windows
    - Verification and audit activities to limit unauthorized and/or undocumented changes to the information systems
- **Monitoring**: Enterprise monitoring activities will validate the information system assets to adhere to organizational policies, procedures, and the approved secure baseline configuration.

3.2 Standard Secure Baseline Configuration

The Enterprise Systems Engineering (ESE) group is responsible for the development and approval of all configuration baselines. The Baseline and Configuration Management (BCM) section, along with the Security Management and Analytics (SMA) group, acts as both the liaison and a member of the governing body to develop, execute, and review all baselines. The SMA office's BCM section triages and coordinates baseline requests and submits the action item for baseline updates.

Prioritization factors for implementing secure configurations in CIs include:

- System impact level – Implement secure configurations in information systems with a high or moderate security impact level with priority over information systems with a low security impact level
- Risk assessments – Characterize information systems, IT products, or CIs with the most impact on security and organizational risk
- Vulnerability scanning – Characterize information systems, IT products, or CIs that are most vulnerable
- Degree of penetration – Represent the extent to which the same product is deployed within an information technology environment

Test Configuration

Configurations will be fully tested in a production environment to ensure software compatibility with hardware device drivers. Virtual environments will be used for testing secure configurations to determine their functional impact on applications. The test environment will be isolated from the production environment to prevent unforeseen impacts to production or patient services. An isolated testing environment, clearly defined test parameters, specialized support hardware, knowledgeable staff, and appropriate change control processes will be established.

Resolve Issues and Document Deviations

Testing secure configuration implementations may introduce functional problems within the system or applications. These problems are examined individually and resolved or documented as a deviation from, or exception to, the established common secure configurations. When conflicts between applications and secure configurations cannot be resolved, deviations are documented and approved.

Implement Secure Configuration

After adequate testing has been performed and issues have been resolved, VA will be able to deploy new secure configurations.

Record and Approve the Baseline Configuration

The established and tested secure configuration represents the preliminary baseline configuration. This configuration is recorded to support:

- Configuration change control/security impact analysis
- Incident resolution
- Problem-solving
- Monitoring activities

Once recorded, the preliminary baseline configuration will be approved in accordance with organizationally-defined policy. Once approved, the preliminary baseline configuration will become the initial baseline configuration for the information system. When a new baseline configuration is established, the implication is that all of the changes from the last baseline were approved. Older versions of approved baseline configurations will be maintained and made available for review or rollback, as required. The Enterprise Configuration Management Control Board (ECCB) will determine the number or prior versions of the baseline configurations that will be maintained within the CMDB.

3.3 Automated Scanning and Discovery

A fully automated scanning system, using the current implementations of discovery tools, will capture information across the entire enterprise. Endpoint discovery tools will scan the entire enterprise and discover information on all endpoints. Captured information from the endpoint discovery tool will be sent to the data normalization toolset. Automation tools are required to:

- Collect information from a variety of sources (e.g., different type of components, different operating systems, different platforms)
- Use open standards, including XML, that are Secure Content Automation Protocol (SCAP) validated
- Automatically detect and remediate changes from configuration or security baselines
- Include vendor-provided support (e.g., patches, updated vulnerability signatures)
- Allow for data consolidation into Security Information and Event Management (SIEM) tools and dashboard products
- Perform regular audit scans to demonstrate compliance with security policies

3.4 Federated Configuration Management System (CMS)

A federated CMS integrates multiple database systems into a single logical database, as shown in Figure 3. It creates a single federated environment, where data stays in authoritative repositories that can be seamlessly accessed from external sources. Multiple Management Data Repositories (MDRs) are mapped to the CMS to improve communication between multiple repositories.

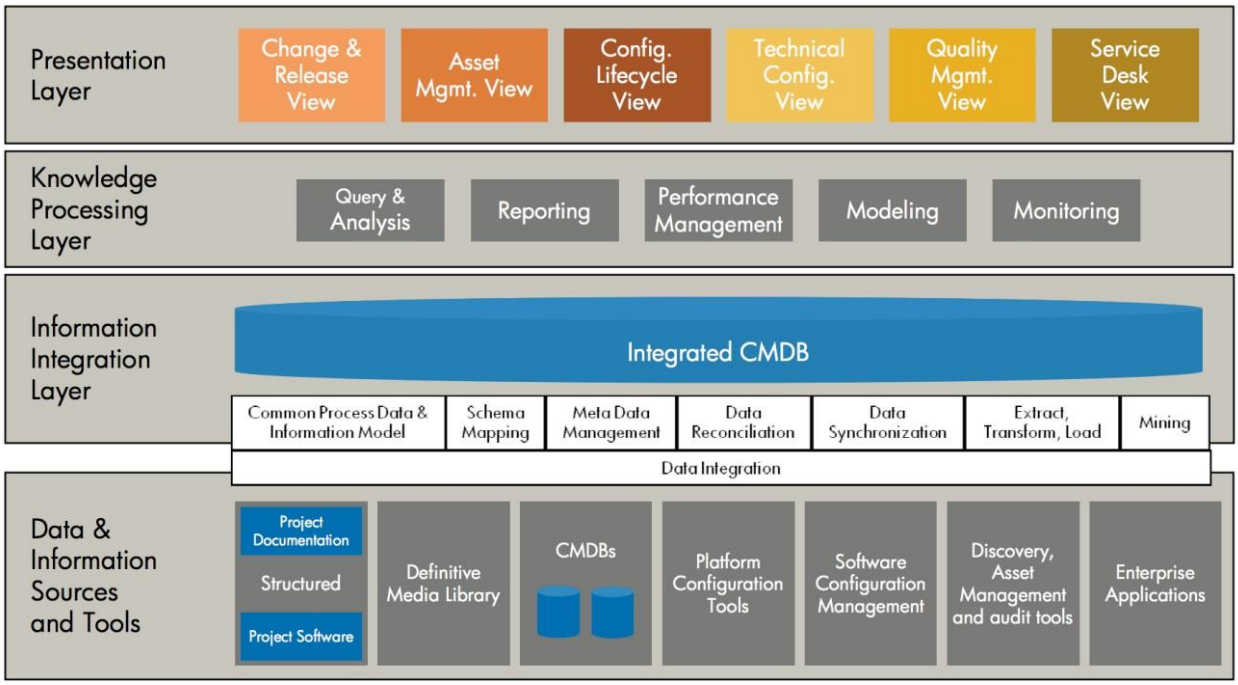

FIGURE 3: "TO BE" ENTERPRISE CMS CONCEPT

The CMS houses reconciled and normalized data from federated CMDBs, supporting a standard product catalog. The CMDB integrates with auto-discovery solutions and provides configuration drift detection and analysis capabilities to ensure that the configuration remains compliant with internal policies and regulations. The CMS includes a configuration test environment within a centrally managed environment for testing IT products, tools, and proposed changes, prior to being released into production. This testing environment evaluates:

- IT products proposed for approval and use within the organization
- Configuration settings for approved IT products
- Patches issued by suppliers prior to deployment through the organization
- Validation of tools that detect unapproved configuration settings
- Verification of testing processes to validate approved configuration settings
- Security impact analyses

CMS drift management capabilities support verification and audit activities. Audits will ensure that the CMS is up-to-date and that the correct and approved CIs are in place. Drift management will perform audits and verification on a regular audit schedule; it will also enable proactive corrective action by using either change or incident requests. These audits will take place within the enterprise and provide a centralized location, where incident management and problem review and resolution can take place. Configuration audits take place:

- Shortly after implementation of a new CMS
- Before and after major changes to the IT infrastructure
- Before a software release or installation
- At random intervals
- At regular intervals
- When all is back to normal after a disaster recovery
- When any unauthorized CIs are detected

In accordance with ITIL service transition objectives, a Federated CMS will ensure that changes and updates to services are mapped to VA's business requirements. End users will receive notifications of any implemented changes or new business requirements. Additionally, retired services are removed in a controlled manner. This will assist in:

- Managing service changes
- Assessing risks
- Releasing planned changes
- Managing expectations to updates

3.5 Alignment to the One-VA Technical Reference Model (TRM)

The enterprise CM toolset is bound by the approved products located in the One-VA TRM. The One-VA TRM will be updated to reflect the tool selection that meets the capability attributes in the previous sections. Future updates to this document will reflect the results of the tool selection effort. The following table references the CM tools that are approved for use at VA.

TABLE 3: REPRESENTATIVE VA ENTERPRISE CM TOOLS

Tool Category	Current Approved Technologies
Configuration Management Database (CMDB)	CA Service Desk Manager, BMC Remedy, Legacy CMDBs
Endpoint Manager	IBM BigFix, Microsoft SCCM, Airwatch MDM
Relationship and Dependency Mapping	BMC ADDM, CA Configuration Automation
Configuration Change Control	CA Configuration Automation
Data Normalization	BMC ADDM, CA IT Asset Manager
Scanning and Discovery	Nessus, IEM, Microsoft SCCM, CA Configuration Automation

3.6 Alignment to Veteran-Focused Integration Process (VIP)

The Veteran-Centric Integration Process (VIP) is a Lean-Agile framework that services the interest of Veterans by efficiently streamlining the activities that occur within the enterprise.

The VIP framework unifies IT delivery oversight and will deliver IT products more securely and predictably. VIP is the follow-on framework from the Project Management Accountability System (PMAS) for the development and management of IT projects; it will propel the Department with even more rigor toward Veteran-focused delivery of IT capabilities.

More information can be found here: https://vaww.oit.va.gov/veteran-focused-integration-process-vip-guide/.

4 USE CASES

4.1 Drift Analysis of Veterans Immunizations Data Systems

4.1.1 Purpose

The Veterans Health Information Systems and Technology Architecture (VistA) Immunization Enhancements (VIMM) project exposes immunization data through an Application Programming Interface (API) that is accessible to internal clinician staff and external partner organizations (e.g., Walgreens). The enterprise CM methodologies and the CMS support control the back-end IT infrastructure CIs that constitute the service. The service provides functionality to consumers through a SLA; significant configuration drift could cause a degradation of service and failure to meet the SLA.

4.1.2 Assumptions

- All aspects of the VistA VIMM monitoring process are housed within VA infrastructure.
- Contracted aspects of the system are able to be controlled and configured by VA assets.

4.1.3 Use Case Description

- Step 1: The CMS maintains information about the CIs and their “correct state” or target baseline in the IT infrastructure, and takes a snapshot of the CI baseline.
- Step 2: Discovery tools identify the status of the actual CI baseline in the IT infrastructure.
- Step 3: The CMS completes a “comparison job” to check against the target baseline.
- Step 4: The CMS determines the amount of drift that CIs made from the target state.
- Step 5: The CMS displays a drift report, and actions are taken to rectify the drift through incident management activities. No action is taken if the drift is insignificant.

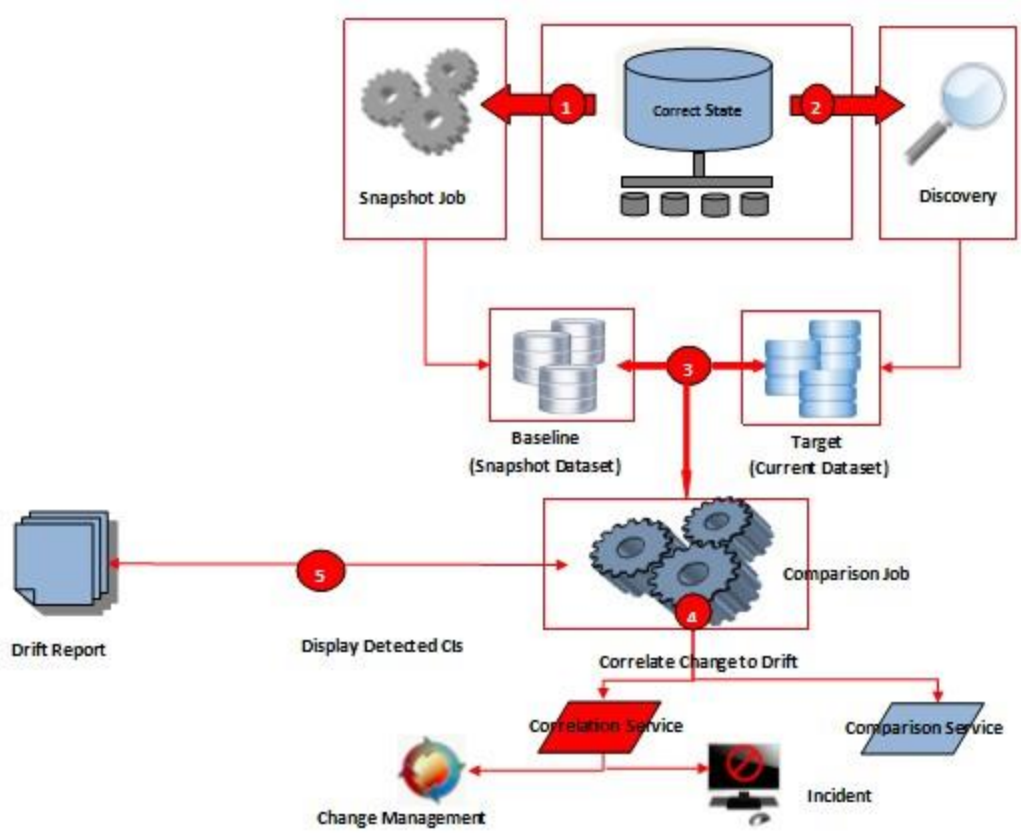

FIGURE 4: DRIFT ANALYSIS USE CASE

4.2 Monitoring Prohibited Software Titles

4.2.1 Purpose

A user downloads a software program that is prohibited in the One-VA TRM for his/her Government Furnished Equipment (GFE) laptop. The software title will go through the scanning process and be checked against the One-VA TRM to determine whether it is authorized or prohibited. If the software title is prohibited, the CM tools will transmit an alert and the user will be notified. The software will automatically be removed if the user does not manually remove it. Data regarding blacklisted software titles will be sent to the CMS. A high-level process flow for this use case is shown in Figure 5.

4.2.2 Assumptions

- The program is owned by VA.
- All systems, assets, and users are either VA-affiliated or able to be controlled and configured by VA assets.

4.2.3 Use Case Description

- Step 1: Endpoint discovery tools scan the entire enterprise and discover information on all endpoints.
- Step 2: The discovery tool produces software titles to be analyzed.
- Step 3: Software titles are checked against product catalog and One-VA TRM.
- Step 4: Software titles are either approved or prohibited based on results from product catalog and One-VA TRM.
- Step 5: Approved software titles are run on the system by a whitelisting tool.
- Step 6: Prohibited software titles go through an incident management process:
    - Email alert regarding prohibited software
    - Initial analysis of prohibited software
    - Initiate incident and create incident ticket
    - Remediation and removal of prohibited software
    - Assess One-VA TRM for alternate solutions
    - Update ticket for resolution status and close
- Step 7: The enterprise CMS maintains data regarding the software titles.

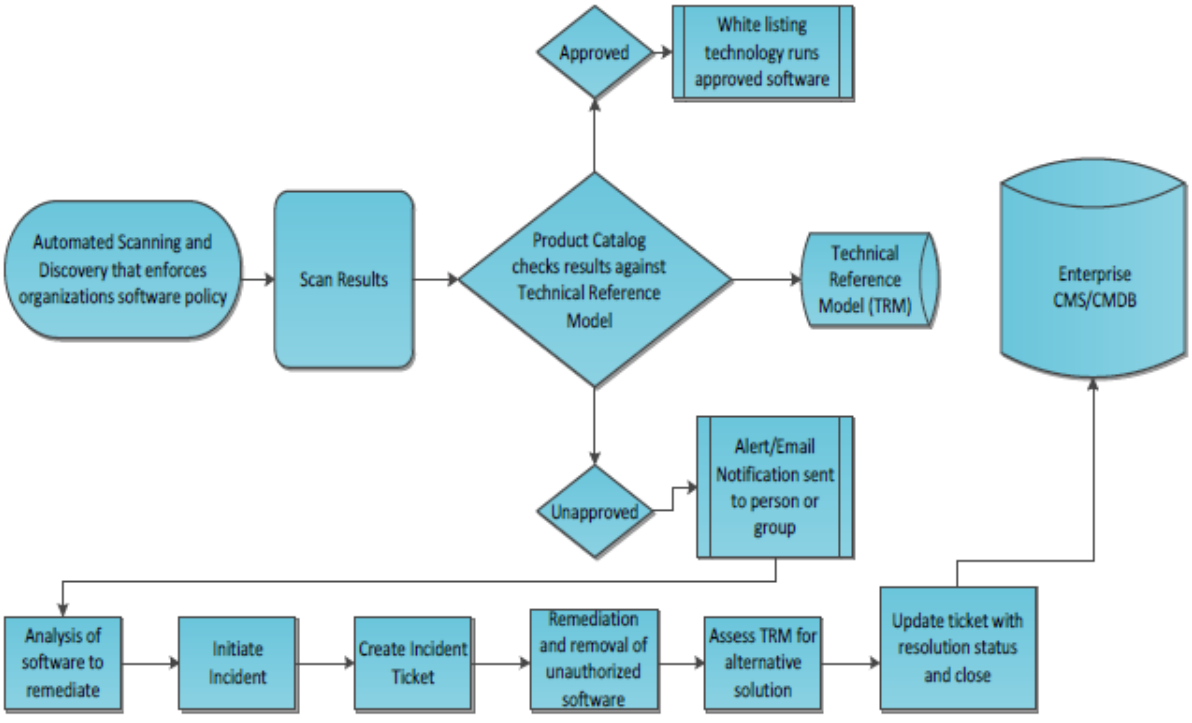

FIGURE 5: MONITORING PROHIBITED SOFTWARE TITLES USE CASE

APPENDIX A. SCOPE

This EDP provides an enterprise-level view of the "As-Is" and "To-Be" mobile capabilities relevant to Veteran-facing mobile applications and the standard processes in use. The document will reference, rather than duplicate, lower-level solution guidance associated with these capabilities.

This EDP provides a vendor-agnostic process framework, based on ITIL best practices and enterprise capabilities that VA will use to implement enterprise-wide IT service CM. This framework includes standardized processes and toolsets to manage VA's IT service configuration items, leading to reduced security vulnerabilities and enhanced customer support across all Lines of Business.

Topics that are out of scope for this EDP, but may be referenced, are:

- Mobile applications used by doctors, clinicians, and care-givers
- Mobile applications used by VA staff
- Interactions between wearable devices that produce patient generated data
- Certification processes for fielding applications
- Mobile security, including single sign-on (SSO)

Document Development and Maintenance

This EDP was developed collaboratively with internal stakeholders from across VA, including participation from VA's OI&T and the Product Development (PD), Office of Information Security (OIS), Architecture, Strategy and Design (ASD), and Service Delivery and Engineering (SDE) pillars. Extensive input and participation was also received from the Veterans Health Administration (VHA), Veterans Benefits Administration (VBA), and the National Cemetery Administration (NCA). In addition, the development effort included engagements with industry experts to review, provide input, and comment on the proposed pattern. This document contains a revision history and revision approval logs to track all changes. Updates will be coordinated with the Government lead for this document, which will also facilitate stakeholder coordination and subsequent re-approval, depending on the significance of the change.

APPENDIX B. DEFINITIONS

This appendix provides definitions for terms used in this document, particularly those related to databases, database management, and data integration.

Key Term	Definition
Approved List	A list of discrete entities, such as hosts or applications, known to be benign and are approved for use within an organization and/or information system.
Authentication (FIPS 200)	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Baseline Configuration	A set of specifications for a system, of Configuration Item (CI) within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes.
Configuration	The possible conditions, parameters, and specifications with which an information system or system component can be described of arranged.
Configuration Baseline	See "Baseline Configuration"
Configuration Change Control	Process for managing updates to the baseline configurations for the configuration items; and evaluation of all change requests and change proposals and their subsequent approval
Configuration Control (CNSSI-4009)	Process for controlling modifications to hardware, firmware, software and documentation to protect the information system against improper modifications before, during, and after system implementation.
Configuration Control Board	Establishment of and charter for a group of qualified people with responsibility for the process of controlling and approving changes throughout the development and operational lifecycle of products and systems; may also be referred to as a change control board;

Key Term	Definition
Configuration Item	Any IT component or other asset that needs to be managed in order to deliver an IT capability. Information about each configuration item is recorded in a configuration record within the configuration management system and is maintained throughout its lifecycle by service asset and configuration management. Configuration items are under the control of change management.
Configuration Item Identification	Any component that needs to be managed in order to deliver an IT Service. Information about each CI is recorded in a configuration record within the configuration management system and is maintained throughout its lifecycle by configuration management. CIs are under the control of change management.
Configuration Management	A collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development and production life cycle.
Configuration Management Plan	A comprehensive description of the roles, responsibilities, policies, and procedures that apply when managing the configuration of products and systems.
Configuration Monitoring	Process for assessing or testing the level of compliance with the established baseline configuration and mechanisms for reporting on the configuration status of items placed under CM.
Enterprise Architecture	The description of an enterprise's entire set of information systems: how they are configured, how they are integrated, how they interface to the external environment at the enterprise's boundary, how they are operated to support the enterprise mission, and how they contribute to the enterprise's overall security posture.

Key Term	Definition
Information Technology (40 U.S.C., Sec. 1401)	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency; for purposes of the proceeding sentence, equipment is used by an executive agency if the equipment the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) Requires the use, to a significant extent, of such equipment, in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources
Patch	An additional piece of code developed to address a problem in an existing piece of software
Remediation	The act of correcting vulnerability or eliminating a threat; three possible types of remediation are installing a patch, adjusting configuration settings, and uninstalling a software application
Risk	A possible event that could cause harm or loss or affect the ability to achieve objectives; a risk is measured by the probability of a threat, the vulnerability of the asset to that threat, and the impact it would have if it occurred.
System	"System" means an interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.
Systemic	An issue or vulnerability found through scanning or discovery that resides in multiple places throughout the enterprise

Key Term	Definition
System Owner	Individual with managerial, operational, technical, and often budgetary responsibility for all aspects of an information technology system
Threat	Any circumstance or event, deliberate of unintentional, with the potential for causing harm to a system.
User	See “Information System User”
VA System Inventory (VASI)	VASI is an authoritative inventory of business-oriented applications and supporting databases that provides a comprehensive repository of basic information about VA systems; represents the relationships between systems and other VA data stores; and captures new systems.
Vulnerability	A Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat device

APPENDIX C. ACRONYMS

The following table provides a list of acronyms that are applicable to and used within this document.

Acronym	Description
ADDM	Atrium Discovery and Dependency Mapping
API	Application Programming Interface
ASD	Architecture, Strategy and Design
CI	Configuration Item
CM	Configuration Management
CMS	Configuration Management System
CMDB	Configuration Management Database
ECCB	Enterprise Configuration Management Control Board
EDP	Enterprise Design Pattern
EO	Enterprise Operations
ESE	Enterprise Systems Engineering
ETA	Enterprise Technical Architecture
FICAM	Federal Identity, Credential, and Access Management
FISMA	Federal Information Security Management Act
GFE	Government Furnished Equipment
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITSM	Information Technology Service Management
MDRs	Management Data Repositories
NCA	National Cemetery Administration
NIST	National Institute of Standards and Technology
OI&T	Office of Information and Technology
OIG	Office of the Inspector General
OIS	Office of Information Security
PD	Product Development
PHI	Personal Health Information
PII	Personally Identifiable Information
PMAS	Project Management Accountability System
SCCM	System Center Configuration Manager
SDE	Service Delivery Engineering
SLA	Service Level Agreement
SMA	Security Management and Analytics Group
SSO	Single Sign-On
TRM	One-VA Technical Reference Model
USGCB	United States Governance Configuration Baseline
VA	Department of Veterans Affairs

Acronym	Description
VBA	Veterans Benefits Administration
VHA	Veterans Health Administration
VASI	Veterans Affairs Systems Inventory
VIP	Veteran-Focused Integration Process
VistA	Veterans Health Information Systems and Technology Architecture

APPENDIX D. REFERENCES, STANDARDS, AND POLICIES

This EDP is aligned to the following VA OI&T references and standards applicable to all new applications being developed in the VA, and are aligned to the VA Enterprise Technical Architecture (ETA):

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
1	VA	VA Directive 6004	Directive establishes VA policy and responsibilities regarding Configuration, Change, and Release Management Programs for implementation across VA.
2	VA	VA 6500 Handbook	Directive information security program. Defining overall security framework for VA.
3	NIST	SP 800-128	Guide for Security-Focused Configuration Management of Information Systems Provides guidelines for organizations responsible for managing and administrating the security of federal information systems and associated environments of operations
4	NIST	SP 800-63-2	Special Publication — Creating a Patch and Vulnerability Management Program Designed to assist organizations in implementing security patch and vulnerability remediation programs.
5	NIST	800-53	Recommended Security Controls for Federal Information Systems and Organizations Outlines the importance of deploying automated mechanisms to detect unauthorized components and configurations within agency networks
6	OMB	Memorandum M-14-04	FY2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management Provides guidance for Federal agencies to follow the report requirements under FISMA.

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
7	OMB	Memorandum M-02-01	Guidance for Preparing and Submitting Security Plans of Actions and Milestones Defines Management and Reporting Requirements for agency Plan of Action and Milestones, including deficiency descriptions, remediation actions, required resources, and responsible parties.
8	White House	FISMA Act of 2002	Reauthorizes key sections of the Government Information Security Reform Act Provides a comprehensive framework for ensuring effective security controls over information resources supporting Federal operations and assets.
9	VA	CRISP	Intended to improve access controls, configurations management, contingency planning, and the security management of a large number of information technology systems.
10	OMB	E-Government Act of 2002	Public Law 107-347 Purpose is to improve the management and promotion of electronic government services and processes by establishing a Federal Chief Information Officer within the Office of Management and Budget, and by establishing a framework of measures that require using Internet-based information technology to improve citizen access to government information and services, and for other purposes.

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
11	VA	Change Plan – Process Template	This Standard Operating Procedure has been created to support and supplement the National Change Management Policy and Standard Document and is not intended to replace the overall management process of the Change Management Program this SOP expands and provides specific information related to the following process being placed under Change Control
12	VA	OI&T Enterprise Change Management Policy	This document establishes an OIT Enterprise Change Management policy ensuring changes to all information technology infrastructure and software configuration items (CIs) are managed and communicated in a disciplined and standardized manner to minimize risk, impact and optimize IT resources
13	VA	OI&T Change Management Process (ProPath)	The purpose of the Change Management (ChM) process is to provide guidance for the management of changes to all Department of Veterans Affairs (VA) Information Technology (IT) environments.
14	VA	SMA Security Baselines	The official versions of the baselines along with process information can be found at: http://vaww.sde.portal.va.gov/svcs/SMA/SitePages/Home.aspx

Disclaimer: This document serves both internal and external customers. Links displayed throughout this document may not be viewable to all users outside the VA domain. This document may also include links to websites outside VA control and jurisdiction. VA is not responsible for the privacy practices or the content of non-VA websites. We encourage you to review the privacy policy or terms and conditions of those sites to fully understand what information is collected and how it is used.