

---

# **VA Enterprise Design Patterns: IT Service Management**

## **Increment 1: FISMA/FICAM Material Weakness #1 & #6 Resolution**

**Office of Technology Strategies (OTS)  
Architecture, Strategy, and Design (ASD)  
Office of Information and Technology (OIT)**

**Version 1.0**

**Date Issued: 29 July 2014**

---



THIS PAGE INTENTIONALLY LEFT BLANK FOR PRINTING PURPOSES

## **APPROVAL COORDINATION**

Tim McGrail, PMP  
Deputy Director, Acting  
Technology Strategies  
OI&T Architecture, Strategy, and Design (ASD)

Paul A. Tibbits, M.D.  
Deputy Chief Information Officer (DCIO)  
OI&T Architecture, Strategy, and Design (ASD)

## REVISION HISTORY

Version	Date	Organization	Notes
0.1	6/11/2014	ASD TS	Initial Draft
0.6	07/11/2014	ASD TS	Revision with adjudicated comments
1.0	07/16/2014	ASD TS	Revision with adjudicated comments resulting from the ITSM infrastructure lockdown

## REVISION HISTORY APPROVALS

Version	Date	Approver	Role
0.1	6/11/2014	Nicholas Bogden	Government Lead
0.6	07/11/2014	Nicholas Bogden	Government Lead
1.0	07/16/2014	Nicholas Bogden	Government Lead
1.0	07/30/2014	Dr. Paul Tibbits	DCIO, Architecture, Strategy and Design

## TABLE OF CONTENTS

<b>1</b>	<b>INTRODUCTION.....</b>	<b>1</b>
1.1	PURPOSE.....	1
1.2	SCOPE.....	2
1.3	DOCUMENT DEVELOPMENT AND MAINTENANCE.....	3
<b>2</b>	<b>BUSINESS NEED.....</b>	<b>3</b>
<b>3</b>	<b>CURRENT STATE.....</b>	<b>5</b>
3.1	SCANNING AND DISCOVERY TOOLS.....	5
3.1.1	<i>VULNERABILITY SCANNING.....</i>	<i>5</i>
3.1.2	<i>ASSET DISCOVERY (TEM, SCCM, ADDM).....</i>	<i>6</i>
3.2	DATA NORMALIZATION TOOLS.....	6
3.3	COMMERCIAL CATALOGUE SERVICE.....	6
3.4	APPROVED/UNAPPROVED LIST.....	7
3.5	CONFIGURATION MANAGEMENT DATABASE (CMDB) (CA SDM CMDB, BMC ATRIUM, IBM).....	8
3.6	CONFIGURATION CHANGE CONTROL.....	9
3.7	INFORMATION TECHNOLOGY ASSET MANAGEMENT (ITAM).....	9
3.8	LINE OF BUSINESS OWNER CAPABILITY AND DEPENDENCY MAPPING.....	9
3.9	IT EXECUTION (PATCH MANAGEMENT).....	10
<b>4</b>	<b>WAY FORWARD.....</b>	<b>11</b>
<b>5</b>	<b>IT SERVICE MANAGEMENT DESIGN PATTERN TO-BE VISION.....</b>	<b>11</b>
5.1	TECHNICAL ATTRIBUTES FOR DESIGN PATTERN PROCESSES.....	12
5.1.1	<i>Scanning and Discovery Tools.....</i>	<i>12</i>
5.1.2	<i>Data Normalization, Enrichment, and Catalogue Service.....</i>	<i>13</i>
5.1.3	<i>Configuration Management Database (CMDB).....</i>	<i>13</i>
5.1.4	<i>Approved/Unapproved List.....</i>	<i>14</i>
5.1.5	<i>Information Technology Asset Management (ITAM) Database.....</i>	<i>14</i>
5.1.6	<i>Relationship and Dependency Mapping.....</i>	<i>15</i>
5.1.7	<i>Configuration Management.....</i>	<i>16</i>
5.1.8	<i>Patch Management.....</i>	<i>20</i>
5.1.9	<i>Vulnerability Management.....</i>	<i>22</i>
5.1.10	<i>Governance.....</i>	<i>24</i>
5.2	REMOVAL OF UNAUTHORIZED SOFTWARE PROCESS (MW#6).....	25
5.2.1	<i>People.....</i>	<i>25</i>
5.2.2	<i>Process.....</i>	<i>25</i>
5.2.3	<i>Tools.....</i>	<i>32</i>
5.3	VULNERABILITY SCANNING AND REMEDIATION PROCESS (MW#1).....	32
5.3.1	<i>People.....</i>	<i>32</i>
5.3.2	<i>Process.....</i>	<i>32</i>
5.3.3	<i>TOOLS.....</i>	<i>38</i>
<b>6</b>	<b>SECURITY CONSIDERATIONS.....</b>	<b>39</b>
	<b>APPENDIX A: RACI CHART DEFINITION.....</b>	<b>41</b>

<b>APPENDIX B: RESOURCES .....</b>	<b>41</b>
<b>APPENDIX C: DEFINITIONS .....</b>	<b>42</b>
<b>APPENDIX D: ACRONYMS .....</b>	<b>44</b>
<b>APPENDIX E. REFERENCES/APPLICABLE STANDARDS.....</b>	<b>46</b>
Figure 1:Technology Standardization Spectrum and VA's Position .....	4
Figure 2: Configuration Management Lifecycle .....	17
Figure 3: Detailed Process Flow for Removal of Unauthorized Software.....	27
Figure 4: Detailed Process Flow for Vulnerability Scanning and Remediation .....	34

# 1 INTRODUCTION

## 1.1 PURPOSE

According to NIST SP 800-128, Guide for Security Focused Configuration Management of Information Systems, information systems are in constant change in response to new, enhanced, corrected, or updated hardware, software capabilities, patches for correcting software flaws, errors to existing components, new security threats, and changing business functions are required. To ensure the required adjustments to the system do not adversely affect either information security or business continuity and day-to-day operations of that information system, a well-defined configuration management process that integrates information security is imperative.

Recent Office of the Inspector General (OIG), Federal Information Security Management Act (FISMA) and Federal, Identify, Credential and Access Management (FICAM) audits have noted that the VA has a material weakness in the configuration, change, patch, and vulnerability management areas of IT service management (ITSM). In a recent inspection, significant deficiencies were discovered in VA's configuration management controls, which are designed to enable the development and operation of information systems including hardware, software, applications, and documentation. This leaves critical software applications and systems vulnerable and may inhibit restoration of critical services in the event of a system disruption or disaster.

VA needs to implement an enterprise-wide solution for configuration management that will provide the following:

1. *Scanning and Discovery*: An automated system of scanning and discovery tools able to capture information across the entire enterprise
2. *Normalization and Reconciliation*: a tool that can aggregate, normalize and reconcile all the data collected by scanning and discovery tools so that it becomes usable/actionable information
3. *Commercial Software Catalog Subscription*: Effective normalization and reconciliation requires a service that monitors changes in the software industry and provides frequent updates about changes in naming conventions (software companies changing product names or acquiring other software companies), new patches, versions, vulnerabilities, support agreements, etc.
4. *Configuration Management Database*: an enterprise level data base in which to store the aggregated, normalized and reconciled data, which is called a configuration management database (CMDB)
5. *Authorized/Prohibited list*: A technical organization and process to review new software products and requests to install new software titles on VA networks, and maintain an enterprise level list of authorized and prohibited software for the enterprise.

6. *Software Asset Management*: An organization, processes, data, and tools necessary for the effective management, control and protection of software assets throughout all stages of their lifecycle
7. *LOB Software Review*: A line of business organization and process that can review software found in the enterprise, and make determinations about its necessity, criticality, regulatory controls, patient safety and other operational limitations that dictate whether or not the software can be removed, updated or scanned without endangering patient safety, violating federal regulations or harming other critical operations
8. *IT Execution Organization*: A technical organization that can couple information from both the line of business and software monitoring service with CMDB information to remove, patch or upgrade software either in a manual, semi-automated or fully automated manner as appropriate.

## 1.2 SCOPE

This document outlines and recommends an enterprise framework creating an end-to-end configuration management process that directly addresses Federal Information System Controls Audit Manual (FISCAM) Audit Material Weaknesses #1 (Vulnerability Discovery and Remediation) and #6 (Unauthorized Software Discovery and Remediation). These recommendations are as follows:

*Recommendation #1*: Implement a process to ensure all VA organizations are included in the vulnerability management program and implement improved mechanisms to continuously identify and remediate security deficiencies on VA's network infrastructure, database platforms, and Web application servers.

*Recommendation #6*: Develop a comprehensive list of approved and unapproved software and implement a process for monitoring, preventing installation, and removing unauthorized application software on agency devices.

This increment encompasses:

- Identify gaps in the VA's current as-is configuration management tools and processes
- Define a to-be vision for VA to establish a single, authoritative, enterprise-wide ITSM tool suite and associated IT Infrastructure Library (ITIL) processes
- Identify implementation guidelines for VA to develop a consolidated authoritative inventory of all endpoints throughout the enterprise found through discovery and scanning
- Automate approval/unapproval of new or existing software, applications or tools in the VA's Technical Reference Model (TRM)
- Define relationship and dependency mapping throughout the enterprise allowing field operations and line-of-business personnel to make decisions on whether or

not a configuration item can be added, removed, or updated within the enterprise and automating as much of the process as possible

### **1.3 Document Development and Maintenance**

Developed collaboratively with stakeholders from OIT Product Development (PD), Office of Information Security (OIS), Architecture, Strategy and Design (ASD), and Service Delivery and Engineering (SDE), design patterns will guide and synchronize the development of system designs to drive the realization of a common vision for the enterprise. This vision, which is documented in the VA Enterprise Technology Strategic Plan, leverages best-of-breed technologies to maximize the effectiveness, efficiency and security of the VA's IT assists. This creates a feedback loop which cultivates participation and collaboration between both Enterprise Architecture (EA) and solution architecture domains.

This document will be reviewed and updated as needed to account for additional feedback from stakeholders as well as lessons learned from enterprise design pattern implementation. Updates will be coordinated with the Government Lead for this document, who will facilitate stakeholder coordination and subsequent re-approval. Major updates of this document will require formal re-approval per the approval chain listed in the "Approval Coordination" section.

## **2 BUSINESS NEED**

Because the VA OIT supports all IT products (hardware, software, COTS and internally developed systems, across a diverse enterprise of both healthcare and federal benefits, any configuration change management solution requires a robust and careful implementation plan. In order to fully address recommendations #1 & #6, the VA is committed to implementing an integrated ITSM program with specific focus on "Asset and Configuration Management" of people, processes and technologies, such that when changes to VA systems are required, the VA is able to effectively decide which assets require changes, the level of impact of those changes, and make informed, information security, cost appropriate, and life-cycle appropriate changes into a semi-automated process. Examples of the business scenarios which require changes to IT assets and configurations include:

- Software patches and upgrades received from software publishers
- Customer requested changes
- US CERT vulnerability notices
- Self-detected vulnerabilities

VA has the required capabilities for fully-integrated, enterprise-level ITSM, however, those capabilities are currently deployed in a way that leads to overlaps and gaps. VA

OIT needs to focus on the synchronization and integration of existing technologies to ensure no gaps in information security while leveraging a CM plan to streamline costs when upgrades of technologies are needed. VA needs to coordinate efforts in an efficient manner to get the right tools, people, and processes/policy in place to effectively and efficiently utilize existing capabilities.

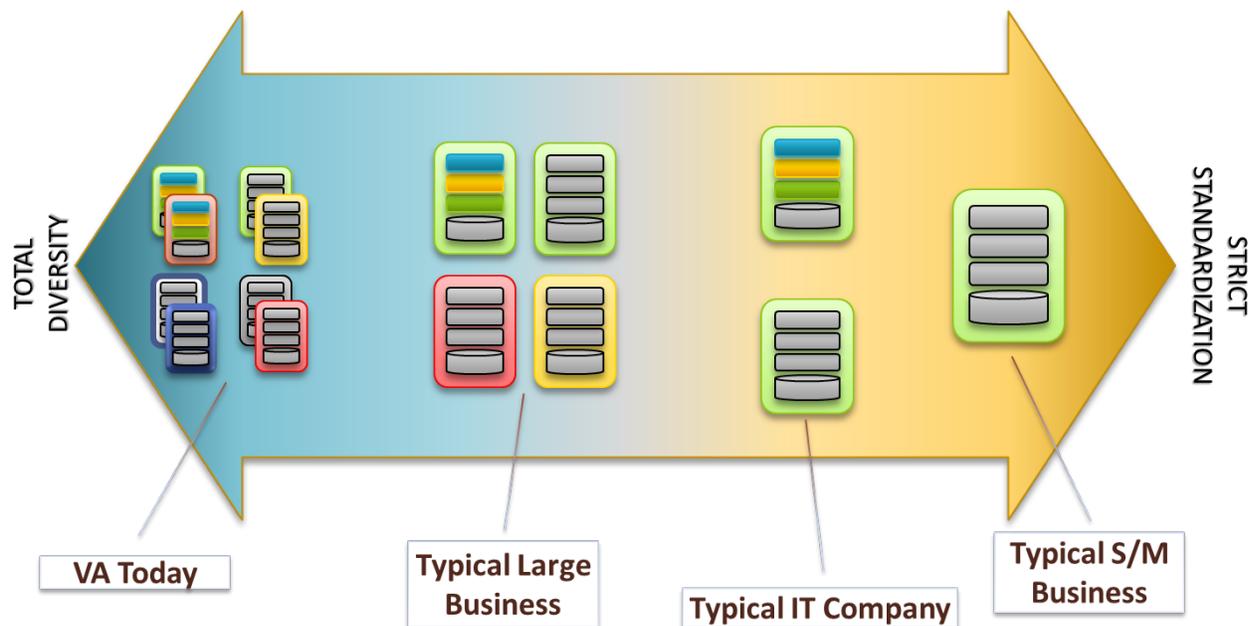


Figure 1: Technology Standardization Spectrum and VA's Position

VA needs to more effectively manage the polarity of technical diversity v. standardization to optimize all three variables on the spectrum: innovation, affordability, and security. Adjusting one, two, or all three variables will change the outcome of the equation. The right place in the “middle” optimizes all three. That optimization point is dynamic and not static.

Currently, VA is operating in a total diverse environment, which is at the far left of the spectrum when compared to typical companies or large businesses, and needs to move closer to the middle.

- Diversity:
  - IT project teams select their own technologies, languages, etc.
    - No enterprise standards, so developers can use diverse number of newer (and older) technologies
    - Many different software licenses
  - Useful for
    - Maximizing innovation and competition

- Decreasing short term development costs and schedules
- Risks
  - Increases long-term cost of sustainment
  - Increased security vulnerabilities
  - Multiple technologies inhibit information sharing
- Standardization:
  - Organization defines specific languages, libraries, plug-ins and web/app/database servers that everyone must use
    - Developers re-use these standardized tools and languages
    - Minimal number of software licenses
  - Useful for
    - Maximizing information sharing
    - Decreasing long term cost of sustainment
    - Enhancing enterprise security
  - Risks
    - Limits competition
    - Increased short term development costs and schedules

### **3 CURRENT STATE**

Currently, there is no automated process in place to effectively automate configuration, patch, and vulnerability management at the VA enterprise level. VA owns a plethora of tools throughout the enterprise that manage a portion of configuration management to some degree. Many of the tools purchased at disparate sites throughout the enterprise are not being fully utilized, or are owned in some capacity at other locations.

Each of these toolsets collects information at varying levels of detail to perform local patch and vulnerability management. VA owns a number of discovery tools, but has never subscribed to a software catalog service to normalize the data discovered by each of the different tools resulting in data that is not usable for its intended purposes (i.e. Approved/Unapproved, Patch, Vulnerability, Configuration, Incident, or IT Asset Management).

#### **3.1 SCANNING AND DISCOVERY TOOLS**

##### **SCANNING**

VA currently deploys NESSUS as its network scanning tool for vulnerability management. NESSUS is able to identify out-of-date software versions and applicable patches or system upgrades, open ports, vulnerable software, and misconfigured services.

In addition to NESSUS, discovery tools currently owned by VA have the capability to perform vulnerability management related tasks. IBM Endpoint Manager and Microsoft SCCM have additional capabilities that are not being fully utilized:

- Proactively identify vulnerabilities
- Provide a fast and easy way to measure exposure
- Automatically fix discovered vulnerabilities
- Identify out-of-date software versions
- Validate compliance with an organizational security policy
- Generate alerts and reports about identified vulnerabilities

### **ASSET DISCOVERY (TEM, SCCM, ADDM)**

VA is currently well into our enterprise-wide implementation of IBM End Point Manager as recommended by Cyber Security experts at the Department of Homeland Security (DHS). We are already using this tool to scan the entire VA enterprise on a monthly basis. In parallel with efforts to automate the processes required to act upon the millions of data points this tool provides, we have implemented a semi-automated process by which the scan results from IBM EPM and other VA owned tools are normalized, reviewed, assessed for “false positives” and then an actionable list of discovered items requiring further investigation is returned to field operations personnel for action.

VA is currently using Microsoft System Center Configuration Manager (SCCM) 2007 to "push" patches, GPOs, etc. out to assets within the Microsoft platform. Through our BPA with Microsoft we have the ability to upgrade to SCCM 2012; however, that capability has not been rolled out to date.

VA deploys BMC Atrium Discovery and Dependency Mapping (ADDM) at enterprise operations (EO) data centers. ADDM was purchased primarily to discovery EO assets. ADDM has the ability to normalize data against a product catalog that is updated twice annually. VA currently utilizes BDNA Technopedia Discover with mixed results. VA is exploring the possibility of rolling BDNA Technopedia Discover licenses to BDNA Technopedia Normalize.

### **3.2 Data Normalization Tools**

VA does not currently deploy any tools to normalize data being generated by its discovery tools across the VA enterprise. VA owns and deploys BMC ADDM at EO data centers, Q-base, a home grown normalization tool at EO sites, and others at various sites. ADDM and Q-base can normalize data generated by discovery tools, but they are not currently being utilized or are able to scale efficiently for the entire enterprise.

### **3.3 Commercial Catalogue Service**

VA currently does not deploy a commercial catalogue service that works in conjunction with data normalization tools throughout the VA enterprise. The BMC ADDM tool does have a catalogue service but it is only updated two times a year and has a limited catalogue that is not sufficient for the entire VA enterprise.

### **3.4 Approved/Unapproved List**

VA currently deploys the OneVA Technical Reference Model (TRM), a VA developed software tool and set of processes that supports the request intake and decision-making processes whereby technologies and standards are approved/unapproved as well as maintains record of what has been approved/unapproved. The automated review process can be initiated through two different avenues, (1) a user, project team member, or SME/ OIT staff member anywhere in the VA can submit a request, (2) current approved technologies are reviewed (refreshed) on a yearly basis while out of date technologies are archived.

Each approved entry on the TRM list provides specific installation and use guidance, to include potential technological constraints, of the wide range of technologies that a development project may select from our non-Government business partners, to meet technological project requirements.

The TRM list is not intended to direct procurements, but offers a wide range of information on products available from both government and non-government business partners. This enables the project manager or regional/local OIT offices to better manage the technology installed and implemented within their environment or product. To assist to our VA community, we also include any known existing VA licensing information.

The OneVA TRM entry includes a Technology/Standard List, Forecasts, Licensing, Technology Relationships, and VA Categorization Framework. Two types of entries are listed in the TRM: standards and software technologies. The Technology/Standard List identifies technologies and technical standards that have been assessed and have been determined to be either compliant or non-compliant with VA's technical approach to IT solutions. Technologies or technical standards that are NOT listed on the Technology/Standard List are considered unapproved for use. Technologies and technical standards that do not appear on the TRM have not been assessed; an assessment or a waiver must be requested to obtain approval to use the technology.

1. Standard: A standard refers to one or more related specifications that have been sanctioned or recognized externally by standards development organizations and have been widely used and accepted by industry, have been mandated by government policy, or have been internally sanctioned or mandated for use by VA. Standards may be expressed in a variety of ways, such as with hardware and software specifications, code sets, and terminologies. They may identify policies, guidelines, characteristics, constraints, and/or conformance criteria. Standards listed in the TRM are enforced and are enforceable based on external or VA-defined conformance criteria.

2. **Software Technology:** Software technology is software that is acquired to support IT business. Software technologies include commercial products, open source/freeware libraries, frameworks, and helper classes.

While policy has been put in place forcing VA personnel and contractors to use the TRM to determine if standards and software technology have been approved for use within the VA, there is no policy in place that gives authority to the TRM for managing compliance. This allows for the download and installation of software, throughout the enterprise, that has not been approved by the TRM increasing the vulnerability problem VA currently has. However, the problem is that there is no control mechanism or active enforcement organization preventing the acquisition, download, installation, and use of software not approved by the TRM.

While significant strides have been made over the past several years to streamline the lengthy approval process within the TRM, there is currently no automation within the TRM approval process.

### **3.5 Configuration Management Database (CMDB) (CA SDM CMDB, BMC Atrium, IBM)**

Currently, several different organizations maintain and use their own CMDBs (using different vendors' CMDB products, not merely different instances of the same product) for their own purposes. VA does not have a single, complete, agreed-upon list of the technical capabilities it requires from a CM system. Therefore, VA OI&T cannot ensure that it possesses the optimal tool set required to provide all needed capabilities without duplication or gaps.

Various local Chief Information Officers (CIOs) throughout the enterprise have purchased BMC Remedy to support their sites. BMC Remedy is currently being phased out of the enterprise due to the recent acquisition of CA Service Desk Manager to support the National Service Desk (NSD).

VA has purchased and is currently implementing CA Service Desk Manager intended to be used as our enterprise level Configuration Management Database (CMDB) to replace a myriad of local and regional CMDBs. This effort will create a single, enterprise level CMDB able to support numerous IT Service Management (ITSM) processes including the process in place to review/monitor unauthorized software. VA is populating this CMDB with data from not only IBM Endpoint Manager, but also legacy CMDBs and other scanning and discovery tools capable of finding software, technologies, and other information the IBM tool may not. (Currently, CA Service Desk Manager is being utilized by SDE Enterprise Operations (EO) teams, but has never been fully implemented beyond the data centers they operate).

While the VA does own tools (e.g. BMC ADDM) with the capability to map relationships and dependencies, it has not fully developed or implemented those technologies throughout the enterprise. This is critical to configuration/change management as it allows field operations to understand which underlying business processes will be affected by updating, adding, or removing specific configuration items.

### **3.6 Configuration Change Control**

VA currently utilizes 3 different toolsets for configuration management. CA Configuration Automation is being deployed at the data centers and is being utilized on EO servers. Both IBM Endpoint Manager and Microsoft SCCM have been deployed and are being utilized for configuration management on endpoints. Microsoft SCCM primarily focuses on configuration management for products within the Microsoft suite, while IBM Endpoint Manager is being utilized for configuration management for the remaining endpoints throughout the enterprise.

### **3.7 Information Technology Asset Management (ITAM)**

VA is currently utilizing the CA tool suite as its IT Asset Management Database. Currently, VA is using the CA tool suite to track the complete lifecycle of an asset from purchase order (PO) and costs associated with hardware and software assets to original equipment manufacturer (OEM) warranties, and OEM maintenance costs and schedules utilizing the software asset management (SAM) add-in to the toolset to track software products. Where applicable, we are tracking reinstatement fees where VA has let software licensing expire.

While CA SAM is able to be accessed outside of EO data centers, the detailed license entitlements information from contracts, agreements, and purchase orders is fragmented among many organizations throughout the enterprise. VA cannot quickly or easily populate the CA SAM database due to the difficulty in gathering the detailed information it requires.

CA ITAM does have the capability to normalize data found through discovery against a stock keeping unit (SKU) catalog. The ITAM Team and its core competency to manage and track OEM warranties and maintenance coverage does so throughout multiple VA Sites outside the AITC but does not perform this function for 100% of the enterprise. The CA ITAM tool becomes enterprise capable if and when discovery tools feed the ITAM repository information about deployed assets.

### **3.8 Line of business owner Capability and Dependency Mapping**

The VA Systems Inventory (VASI) is a custom-built VA system that maps business functionality (“systems”) to underlying software applications. VASI is a database with a web front end that does not have relationship discovery capabilities, or custom code to

do so. Relationships between systems and their infrastructure components must be manually input into the system.

Through use of VASI, and by understanding the relationship between systems, applications, platforms, and infrastructure to the underlying business functions they support, VA will effectively be able to eliminate duplicative systems inventories maintained by various stakeholders throughout the enterprise, thus allowing VA to better align current IT capabilities with strategic goals and current business processes.

Developing an authoritative inventory of business-oriented applications and supporting databases, enables VA to better manage IT investments through more enterprise-wide portfolio management capabilities through a holistic representation of the relationship between system and VA data store. While VASI will ultimately provide relationship and dependency mapping between system and underlying business process, it is still in the early stages of being rolled out. It is not at full capacity, nor is it being utilized throughout the VA. Additionally, it does require data to be input manually.

### **3.9 IT Execution (Patch Management)**

Currently VA deploys Microsoft System Center Configuration Manager (SCCM) and IBM Endpoint Manager to push patches throughout the enterprise. SCCM is being utilized to push patches out to Microsoft products, while Endpoint Manager pushes patches out to non-Microsoft products. VA also currently uses Absolute in the deployment of patches to Apple Mac systems across the enterprise.

Having two products performing the same function poses a few problems as it pertains to patch management. While, both SCCM and Endpoint Manager are able to scan and discover data on configuration items throughout the enterprise, they do so at varying levels of detail and with varying degrees of complexity. This alone poses a major problem; it allows for software patches to be pushed out to redundant configuration items, or for configuration items to “slip through the cracks” due to the usability of the data provided by discovery.

Another issue VA currently has is the process of how patches and updates are sent to a system. Today, when updates are sent to a device the configuration settings are modified to ESE Standards (e.g., auto update or other functionality that is not allowed in the VA), when updates are sent with a system that does not have checks and balances and installs the software without uninstalling or puts the software in a default setting this can compromise the systems security and introduce other risk factors. At a later date when updates need to be made one tool may not be able to make the changes because the package can't install/update as it is not installed in a standard folder or using defined naming standards that the ESE baseline owner has configured. Allowing owners of

other tools to change configuration settings that have not been vetted and approved by the baseline owner only adds additional level of disconnect in the organization.

#### **4 WAY FORWARD**

To mitigate risks in the near term, VA has performed manual analyses using scan results from IBM Endpoint Manager. We have normalized and reconciled scan data from sample facilities against the TRM to create an actionable list of discovered items requiring further investigation. That list has been provided to field operations personnel with guidance to review each item with previously identified line-of-business (LOB) customers and take appropriate action based on further, detailed analyses. These actions include a combination of patching, system removal and/or development of a risk based decision memorandum as appropriate to the particular situation.

To meet this challenge in a more effective and sustainable manner, VA OI&T has established a cross functional group that is developing a concept of operations and estimating the resources required to establish a technical organization that can couple information from both the line of business and software monitoring services with CMDB information to make determinations about software necessity, criticality, regulatory controls, patient safety and other operational limitations that dictate whether or not the software can be removed, updated or scanned without endangering patient safety, violating federal regulations or harming other critical operations.

#### **5 IT SERVICE MANAGEMENT DESIGN PATTERN TO-BE VISION**

Implementing a formal, automated process for the identification and removal of unauthorized software requires people, processes and technology. In order to achieve this vision, VA must continue to maintain a robust Technical Reference Model (TRM) that provides consolidated and coordinated guidance concerning software, technologies and standards that are authorized in the VA environment, in the form of a comprehensive “Approved/Unapproved” list with additional information such as forecasting information, lifecycle support dates and implementation constraints for each technology in the TRM.

Together with the TRM, VA must establish processes to review software found in the enterprise through discovery, normalize that data, and perform analysis against the TRM allowing line-of-business organizations to make determinations about its necessity, criticality, regulatory controls, patient safety and other operational limitations that dictate whether or not the software can be removed, updated or scanned without endangering patient safety, violating federal regulations or harming other critical operations.

VA must fully resource and empower a technical organization that can couple information from both the line-of-business and software monitoring service with CMDB information to remove, patch or upgrade software either in a manual, semi-automated or fully automated manner as appropriate.

## **5.1 Technical Attributes for Design Pattern Processes**

### **SCANNING AND DISCOVERY TOOLS**

VA must establish and implement a fully-automated system of scanning, using currently owned discovery tools, to capture information across the entire enterprise.

VA OI&T must fully implement an endpoint discovery tool with the capability to scan the enterprise and discover information on all endpoints across the enterprise. Information captured by the endpoint discovery tool will then flow to the data normalization toolset.

VA OI&T must fully implement a server discovery tool with the capability to scan the enterprise and discover all server information across the enterprise. Information captured by the server discovery tool will flow to the data normalization toolset.

Automated tools should be able to scan different information system components (e.g., Web server, database server, network devices, etc.) running different operating systems, identify the current configuration settings, and indicate where they are noncompliant with policy. Automation tools must:

- Have the ability to pull information from a variety of sources (different type of components, different operating systems, different platforms, etc.);
- Make use of standardized specifications such as XML and SCAP;
- Integrate with other products such as help desk, inventory management, and incident response solutions;
- Integrate with the Change and Configuration Management solutions allowing VA to know what incidents are being logged against a product or system, what changes have been authorized, and what the authorized configuration is of the systems and/or software.
- Include vendor-provided support (patches, updated vulnerability signatures, etc.);
- Maintain compliance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines and link vulnerabilities to SP 800-53 controls;
- Provide standardized reporting capability (e.g. SCAP, XML) including the ability to tailor output and drill down; and
- Allow for data consolidation into Security Information and Event Management (SIEM) tools and dashboard products.

## **Data Normalization, Enrichment, and Catalogue Service**

Effective normalization, reconciliation, and enrichment requires a service that monitors changes in the software industry and provides frequent updates about changes in naming conventions (software companies changing product names or acquiring other software companies), new patches, versions, vulnerabilities, support agreements, etc.

VA does not currently deploy any tools that normalize data being generated by its discovery tools. VA currently owns BMC ADDM which has the capability to do the data normalization required to fully automate the configuration management process, however ADDM is only updated twice-yearly; not frequent enough for VA's information requirements regarding vulnerabilities, patches, and updates.

VA must fully deploy a Data normalization and enrichment tool with the capability to aggregate, normalize, reconcile, and enrich all the data collected by scanning and discovery tools across the entire VA enterprise. Once normalized the data will be compared, as part of an automated process, against the information listed within the TRM; approved information will then flow into the CMDB where it will become usable/actionable information.

## **Configuration Management Database (CMDB)**

VA OI&T must designate and populate a single, authoritative, enterprise-wide Configuration Management Database (CMDB) at the enterprise level that stores the aggregated, normalized and reconciled data found through discovery then normalized.

The enterprise CMDB must have the capability to:

- Provide a single source of truth about IT asset attributes with detailed data remaining in the respective data stores (e.g. Software Asset Management Database)
- Allow for the visualization of IT relationships and interdependencies, covering parent-child (dependencies) as well as peer-to-peer relationships
- Be rooted in ITIL but able to rapidly exceed conventional ITIL boundaries
- Not be a replacement of operational tools
- Allow for filtering ("what CIs/relationships am I interested in") as well as configuration of what is under manual change control and automated change control
- Provide a graphical representation of CIs and their relationships for the purpose of change planning, impact analysis and root cause analysis
- Administer security across federated data sources
- Require CIs under change control to have approved change orders
- Allow CIs aspects (attributes) not under change control to be automatically updated through discovery and reconciliation (avoid the "death of a thousand manual updates")

- Ensure unauthorized changes are detected and configuration managers are alerted to resolve differences

In addition to the capabilities listed above, the CMDB must capture data elements on configuration items to aid in the facilitation of the Configuration, Patch, and Vulnerability Management Program. Additional data elements include:

- Status of the configuration item (e.g., operational, spare, disposed, etc.);
- Relationships to other configuration items in the inventory;
- Relationships to/dependencies on other information systems;
- Other information systems supported by this component;
- Identification of any Service-Level Agreements (SLA) that apply to the component;
- Applicable common secure configurations;
- Security controls supported by this component; and Identification of any incident logs that apply to the component.

#### **Approved/Unapproved List**

VA must establish, or maintain a technical organization and process to review new software products and requests to install new software titles on VA networks, and maintain an enterprise level list of authorized and prohibited software (i.e. approved/unapproved list) for the enterprise.

VA will implement a fully-automated process to determine if CIs found through discovery have been approved in the TRM. Where there is a COTS tool VA currently owns, with the capability to act as the authoritative source in concert with the TRM, VA will use that software. The tool must ensure that when software that is not on the TRM approved software list is auto uninstalled immediately and a security incident logged to track the installation, and if required get the software authorized.

A controlled and logical expansion of the TRM, coupled with a methodical approach to minimize the total number of different applications used throughout the VA, will bring the installed base and the TRM into alignment. As we move to our fully automated solution, alignment will be maintained by virtue of the system being implemented to standardize and integrate Endpoint Scanning Tools, CMDB, and the VA TRM.

#### **Information Technology Asset Management (ITAM) Database**

VA currently owns tools with the capability to fully automate IT Asset Management (ITAM) but it has not fully implemented those toolsets. IT Asset Management (ITAM) is the management and reconciliation of the physical, financial and contractual life-cycle attributes of IT assets (hardware and software) to enable the delivery of cost-efficient,

timely business knowledge to better manage and control the business and operational aspects of IT.

VA must fully implement existing asset management tools with the capability to:

- Monitor license compliance
- Normalize purchase and discovery data
- Be a 100% web based solution
- Track assets from cradle to grave
- Allow VA to fully gain control over asset usage

A CI inventory adds real value to a Configuration, Patch, and Vulnerability Management program when each item in the inventory is associated with information that can be leveraged for determination of approved configuration baselines, configuration change control/security impact analysis, and monitoring/reporting. VA must include information on data elements for each configuration item in the inventory to include:

- Unique Identifier and/or Serial Number;
- Information System of which the component is a part;
- Type of IS component (e.g., server, desktop, application);
- Manufacturer/Model information;
- Operating System Type and Version/Service Pack Level (preferably using the appropriate Common Platform Enumeration Name);
- Presence of virtual machines;
- Application Software Version/License information (preferably using the appropriate Common Platform Enumeration Name);
- Physical location (e.g., building/room number);
- Logical location (e.g., IP address);
- Media Access Control (MAC) address;
- Owner;
- Operational status;
- Primary and secondary administrators; and
- Primary user (if applicable)

## **Relationship and Dependency Mapping**

The VA Systems Inventory (VASI) team will develop and establish initial dependency and relationship mapping allowing field operations teams to review software found in the enterprise, and make determinations about its necessity, criticality, regulatory controls, patient safety and other operational limitations that dictate whether or not the software can be removed, updated or scanned without endangering patient safety, violating federal regulations or harming other critical operations.

The Service Desk Manager (CA SDM) tool currently has the capability to do analysis of what systems are affected when software is added, updated or removed from the enterprise, but will require initial dependency mapping be done.

VA must fully deploy an automated tool to populate the VASI with information about the relationships between systems, their component services, and platforms and infrastructure. VASI information must be housed in the enterprise CMDB as one system of record. This will allow the enterprise to track changes made to relationships and information stored in the VASI system via change management process.

## **Configuration Management**

Given the continually evolving nature of an information system and the mission it supports, the challenge for organizations is not only to establish an initial baseline configuration that represents a secure state (which is also cost-effective, functional, and supportive of mission and business processes), but also to maintain a secure configuration in the face of the significant waves of change that ripple through organizations.

In many cases, organizational policies, in accordance with federal laws, standards, directives, and orders, establish generally accepted common secure configurations (e.g., National Checklist Program, DISA STIGs, CIS benchmarks). Configurations identified in the National Checklist Program as well as SCAP-expressed checklists are sources for establishing common secure configurations. Commercial product developers are also a potential source for common secure configurations. Deviations from common secure configurations are justified and recorded.

Using the secure configuration previously established as a starting point, VA will follow a structured approach when implementing secure configurations:

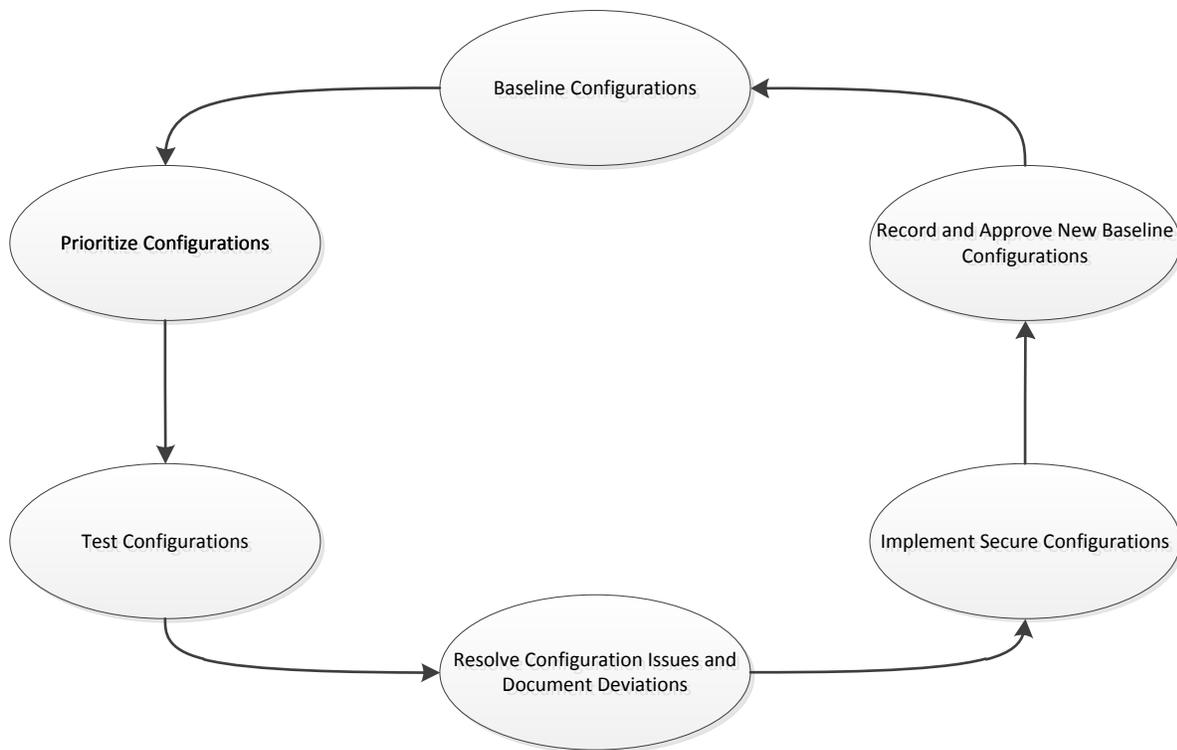


Figure 2: Configuration Management Lifecycle

### ***Baseline Configurations***

The approved baseline configuration for an information system and associated components represents the most secure state consistent with operational requirements and constraints. For a typical information system, the secure baseline may address configuration settings, software loads, patch levels, how the information system is physically or logically arranged, how various security controls are implemented, and documentation. Where possible, automation is used to enable interoperability of tools and uniformity of baseline configurations across the information system.

The baseline configuration of an information system includes the sum total of the secure configurations of its constituent CIs and represents the system-specific configuration against which all changes are controlled.

ESE will be the primary owner of the baseline configurations and with collaboration with FO, EO, NSD, OIS and PD all changes to the baselines will be managed by them.

### ***Prioritize Configurations***

In the ideal environment, all IT products within VA would be configured to the most secure state that still provides the functionality required by the organization. However,

due to limited resources and other constraints, VA must prioritize which information systems, IT products, or CIs to target first for secure configuration.

In determining the priorities for implementing secure configurations in information systems, IT products, or CIs, VA must consider the following criteria:

- *System impact level* – Implementing secure configurations in information systems with a high or moderate security impact level may have priority over information systems with a low security impact level.
- *Risk assessments* – Risk assessments can be used to target information systems, IT products, or CIs having the most impact on security and organizational risk.
- *Vulnerability scanning* – Vulnerability scans can be used to target information systems, IT products, or CIs that are most vulnerable. For example, the Common Vulnerability Scoring System (CVSS) is a specification within SCAP that provides an open framework for communicating the characteristics of software flaw vulnerabilities and in calculating their relative severity. CVSS scores can be used to help prioritize configuration and patching activities.
- *Degree of penetration* – The degree of penetration represents the extent to which the same product is deployed within an information technology environment. For example, if an organization uses a specific operating system on 95 percent of its workstations, it may obtain the most immediate value by planning and deploying secure configurations for that operating system. Other IT products or CIs can be targeted afterwards.

### ***Test Configurations***

VA will fully test secure configurations prior to implementation in the production environment as there are a number of issues that may arise when implementing configurations including software compatibility and hardware device driver issues. For example, there may be legacy applications with special operating requirements that do not function correctly after a common secure configuration has been applied. Additionally, configuration errors could occur if OS and multiple application configurations are applied to the same component. For example, a setting for an application configuration parameter may conflict with a similar setting for an OS configuration parameter.

Where possible, VA will use virtual environments for testing secure configurations as the examination of the functional impact on applications without having to configure actual machines. The test environment cannot be connected to the production environment due to the risk of unforeseen impact to production or patient services. This requires an isolated testing environment, clearly defined test parameters, specialized support hardware, knowledgeable staff and appropriate change control processes. The testing will be conducted as security patches are released by the vendor(s) and will be

managed through a change control and release process and tiered testing process. The process will begin with a high level testing of common core applications or baseline on a given IT system. Once core applications have been tested at the baseline layer, the testing will continue to the regional and VISN testing level under similar conditions that provide for isolation of unique applications that may be impacted by the patches released by the vendor(s). Again, virtual devices are recommended due to the versatility or configuration management offered.

All testing layers will be interconnected and housed within the VA configuration testing environment. The VA configuration test environment will reside within an isolated section of the VA network and will permit limited access to test engineers. This will allow for virtual images to be managed at the baseline layer while providing various regional and VISN level testing access across the testing infrastructure. Through standardized testing the VA testing environment will allow for better test control, more accurate configuration management, and more thorough modeling of the VA IT infrastructure. Problems or issues discovered at any layer of testing will require the testing process at the impacted Tier layer to reset in order to reduce overall risk to VA production and patient systems.

### ***Resolve Issues and Document Deviations***

Testing secure configuration implementations may introduce functional problems within the system or applications. For example, the new secure configuration may close a port or stop a service that is needed for OS or application functionality. These problems are examined individually and either 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 as appropriate.

### ***Deploy Secure Configurations***

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

### ***Record and Approve the Baseline Configuration***

The established and tested secure configuration, including any necessary deviations, represents the preliminary baseline configuration and is recorded in order to support configuration change control/security impact analysis, incident resolution, problem-solving, and monitoring activities. Once recorded, the preliminary baseline configuration is approved in accordance with organizationally defined policy. Once approved, the preliminary baseline configuration becomes the initial baseline configuration for the information system and its constituent CIs.

When a new baseline configuration is established, the implication is that all of the changes from the last baseline have been approved. Older versions of approved baseline configurations are maintained and made available for review or rollback as needed.

The Enterprise Configuration Management Control Board (ECCB) will determine the number or prior versions of the baseline configurations will be maintained within the CMDB.

### ***Pre-Approved Changes***

In the interest of resource management, VA will designate the types of changes that are preapproved (i.e., changes that are not sent for approval) and changes that are typically *not* included under configuration control. Vendor-provided security patches, updated antivirus signatures, and replacement of defective peripherals or internal hardware are examples of changes that may be preapproved. Database content updates, creating/removing/updating accounts, and creation or deletion of user files are examples of changes that are typically exempt from configuration change control.

Pre-approved changes must still follow VA Directive 6400 and must be recorded and managed as a change to our environment.

### ***Unscheduled Changes***

When unscheduled changes must be made and time does not allow for following the established configuration change control process, unscheduled changes are still managed and controlled.

Unscheduled changes are considered Emergency Changes. Where unscheduled changes must occur the enterprise will continue to follow the guidance outlined in the National Patch and Change Management Process document for Emergency Changes.



National Patch  
Management and Change

## **Patch Management**

Widespread manual patching of computers is becoming ineffective as the number of patches that need to be installed grows and as attackers continue to develop exploit code more rapidly. While patching and vulnerability monitoring can often appear an

overwhelming task, consistent mitigation of organizational vulnerabilities can be achieved through a tested and integrated patching process that makes efficient use of automated patching technology. Enterprise patch management tools will allow VA to automatically push patches out to many computers quickly.

Manual methods may need to be used for operating systems and applications not supported by automated patching tools, as well as some computers with unusual configurations; examples include embedded systems, industrial control systems, medical devices, and experimental systems. For such computers, there will be a written and implemented procedure for the manual patching process.

VA will continue to deploy both Agent Based, and Non-Agent Based patching solutions throughout the enterprise.

### ***Agent-Based Patching Solutions***

Agent-based patching solutions use a centralized computer (or cluster of computers) that manage the patching process for all participating computers. However, with this model a software program (agent) is installed on each participating computer. The overall agent patching process will work as follows:

1. The agent communicates with the central computer to learn about new patches. Depending on the implementation, the agent may poll the central computer periodically or may be contacted directly by the central computer (which is more efficient).
2. The agent has administrator or root access to the computer, and it uses that privilege to determine which patches are missing. This status is usually transmitted to the central computer so that the overall patching administrator can view the status of all participating computers. This also enables the central administrator to produce patching reports regarding the patch security level for each system.
3. The agent receives instructions from the central computer on which patches to install and how to install them. In cases where a reboot is required, the central computer may instruct the agent to patch and automatically reboot the computer. Alternately, the central computer may instruct the agent to patch and then notify the user that the computer needs rebooting (with the option of an automated reboot within a specified timeframe).

Through continued use of an agent-based solution VA will eliminate the excessive network bandwidth usage that occurs with the non-agent-based solution.

## ***Non-Agent Patching Solutions***

Non-agent patching solutions are similar to network-based vulnerability scanners. There is usually a single computer that scans computers through the network. However, unlike many vulnerability scanners, the non-agent patching solution is usually given administrator access to the computers participating in the automated patching program. This gives the patching program access to much more information than is available through simple network scanning. It also gives the patching program the ability to install patches on participating computers. Given the similarity between non-agent patching solutions and vulnerability scanners, it is not surprising that some commercial non-agent patching solutions also detect vulnerabilities, and can do so with greater accuracy than a vulnerability scanning program that does not have administrator access to the computer.

Through continued use of non-agent patching solutions VA will ensure that it is reaching all endpoints throughout the enterprise that do not have agents installed locally on each machine ensuring complete coverage throughout the enterprise.

In addition to using both Agent Based and Non-Agent Based patching tools VA will group and assign priority levels to configuration items to facilitate remediation efforts. Resource grouping and prioritization will expedite the assessment of risk to systems, and will be used to help identify which systems may require the special attention of the OIS Office of Cyber Security. The primary grouping should be by system name and the system's Federal Information Processing Standard (FIPS) 199 impact designation. It may also be useful to group resources by network location. This is particularly important for those resources that are directly exposed to the Internet and those that reside behind internal high-security areas. If this grouping and prioritization is not performed, VA will embark upon unnecessarily costly remediation strategies. Prioritization will allow VA to focus immediate patching efforts on the vulnerable configuration items that are most at risk (e.g., possibly those directly exposed to the Internet).

## **██████ Vulnerability Management**

Vulnerability management is a security practice designed to proactively prevent the exploitation of IT vulnerabilities that exist within an organization. The expected result is to reduce the time and money spent dealing with vulnerabilities and exploitation of those vulnerabilities. Proactively managing vulnerabilities of systems will reduce or eliminate the potential for exploitation and involve considerably less time and effort than responding after an exploitation has occurred.

VA will continue to use the vulnerability scanning tools it is currently using to identify open ports, vulnerable software, and misconfigured services. Vulnerability scanners can help identify out-of-date software versions and applicable patches or system

upgrades. In addition, certain vulnerability scanners are able to automatically make corrections and fix certain discovered vulnerabilities. Scanning tools must continue to provide the following capabilities:

- Identify active hosts on networks
- Identify active and vulnerable services (ports) on hosts
- Identify vulnerabilities associated with discovered operating systems and applications
- Test compliance with host application usage/security policies.

Where scanning and discovery tools have the capability to perform vulnerability scanning tasks, those tools will be utilized to:

- Proactively identify vulnerabilities
- Provide a fast and easy way to measure exposure
- Automatically fix discovered vulnerabilities
- Identify out-of-date software versions
- Validate compliance with an organizational security policy
- Generate alerts and reports about identified vulnerabilities.

In addition to vulnerability scanning tools, VA will take advantage of the publicly available vulnerability and patching resources provided by the U.S. government. These products should be directly used as a source of official and validated U.S. government information on vulnerabilities. VA will also employ use of COTS products that provide interoperability with the U.S. government vulnerability and patching resources and standards. OIS Office of Cyber Security will also subscribe to the US-CERT cyber security alerts to learn about the vulnerabilities that are considered most critical by the U.S. government, even if OIS Office of Cyber Security subscribes to generic vulnerability services. This will help ensure that the highest priority vulnerabilities receive appropriate attention.

In addition to the U.S. Government resources provided (Appendix B) information on vulnerabilities, VA will regularly monitor publically available vulnerability information. Sources that provide vulnerability information are:

- Vendor Web sites and mailing lists
- Third-party Web sites
- Third-party mailing lists and newsgroups
- Vulnerability scanners
- Vulnerability databases
- Enterprise patch management tools
- Other notification tools

## **Governance**

The true impact of vulnerability can only be determined by looking at each vulnerability in the context of VA's unique security infrastructure and architecture. In addition, the impact of a vulnerability on a system depends on the network location of the system (i.e., when the system is accessible from the Internet, vulnerabilities are usually more serious). To remediate impact, VA must define and document policies for the Configuration, Patch, and Vulnerability Management program. ASD IT Governance and Policy will develop, disseminate, and periodically review and update the Configuration, Patch, and Vulnerability Management policies for the organization. The policies are included as a part of the overall organization-wide security policy. The policy will include:

- Purpose – the objective(s) in establishing organization-wide Configuration, Patch, and Vulnerability Management policy;
- Scope – the extent of the enterprise architecture to which the policy applies;
- Roles – the roles that are significant within the context of the policy;
- Responsibilities – the responsibilities of each identified role;
- Activities – the functions that are performed to meet policy objectives;
- Common secure configurations – federal and/or organization-wide standardized benchmarks for configuration settings along with how to address deviations; and
- Records – the records of configuration management activities to be maintained; the information to be included in each type of record; who is responsible for writing/keeping the records; and procedures for protecting, accessing, auditing, and ultimately deleting such records.
- Training requirements;
- Use of templates;
- Use of automated tools;
- Prohibited configuration settings; and
- Requirements for inventory of information systems and components.

The Configuration, Patch, and Vulnerability Management policy emphasizes management commitment, clarifies the required level of coordination among organizational entities, and defines the configuration monitoring approach.

### **5.2 ITSM Tasks, Process and RACI**

The following sections elaborate on the roles and responsibilities associated with the processes for addressing Material Weakness Recommendations 1 and 6 to address each of the attributes above. Information regarding each process has been consolidated into the following Microsoft Excel file. This file contains the RACI Matrix for each process, as explained in Appendix A of this document.



### 5.3 Removal of Unauthorized Software Process (MW#6)

#### People

Executing this process as described above will result in each site being scanned every six months, with all known vulnerabilities being remediated and unauthorized software being removed in the six months between scans. Accordingly, each successive scan should generate fewer issues and require less resources to execute, allowing scan frequencies to be increased over time.

Executing this process beginning August 1, 2014 requires necessary staff be dedicated to this effort no later than July 23, 2014, and, determination of the normalization and reconciliation tool be completed no later than August 23, 2014. However, if resources are allocated as required and this process is started no later than August 1, OIG recommendations #1 and #6 will be substantially resolved by September 30, 2014.

The defined, and agreed upon, roles and responsibilities for each task involved in the Vulnerability Scanning and Remediation process can be found in the RACI Matrix located in Columns J-R of the “MW#6 Process” tab of the embedded file located at the end of Section 1.

#### Process

The process described herein is a sixty (60) day *Planning, Scanning & Remediation Process* which will initially be repeated for approximately 17% of the VA IT enterprise each month such that every device in the entire VA is scanned for vulnerabilities and unauthorized software at least twice per year. This document describes specific activities within each phase of the plan and aligns Offices of Responsibility to each activity.

This process is divided into three areas. The *Scanning Phase*, describes specific steps that must take place prior to vulnerability scanning. The *Triage Phase* describes the detailed steps that must happen at the enterprise level. The *Remediation Cycle* provides the detailed steps that must occur after scanning has taken place. Coordination must occur, through synchronization meetings across OI&T and with customer organizations and a dedicated SharePoint site, to ensure OI&T and customer staffs are prepared when scanning begins, and remain informed and engaged until all vulnerabilities are remediated and unauthorized software is removed or approved for use.

Figure 3 provides a visual overview of the process for removal of unauthorized software that consolidates several process steps to show a high-level summary of key activities. The *Scanning Phase* maintains its own area, but for the purposes of simplification, the *Triage Phase* and *Remediation Cycle* have been consolidated into one area to summarize the joint efforts required to develop and execute remediation plans.

This first iteration of this 60 day process MUST start August 1, 2014 in order for the VA to close 2013 FISMA Audit Findings #1 or #6 by September 30, 2014. Successful execution of this process starting August 1<sup>st</sup> absolutely requires all necessary resources are allocated No Later Than July 23, 2014 (with some required sooner) in accordance with the Recommendation #1 and #6 Project Plan and the VA Enterprise Configuration Management Design Pattern.

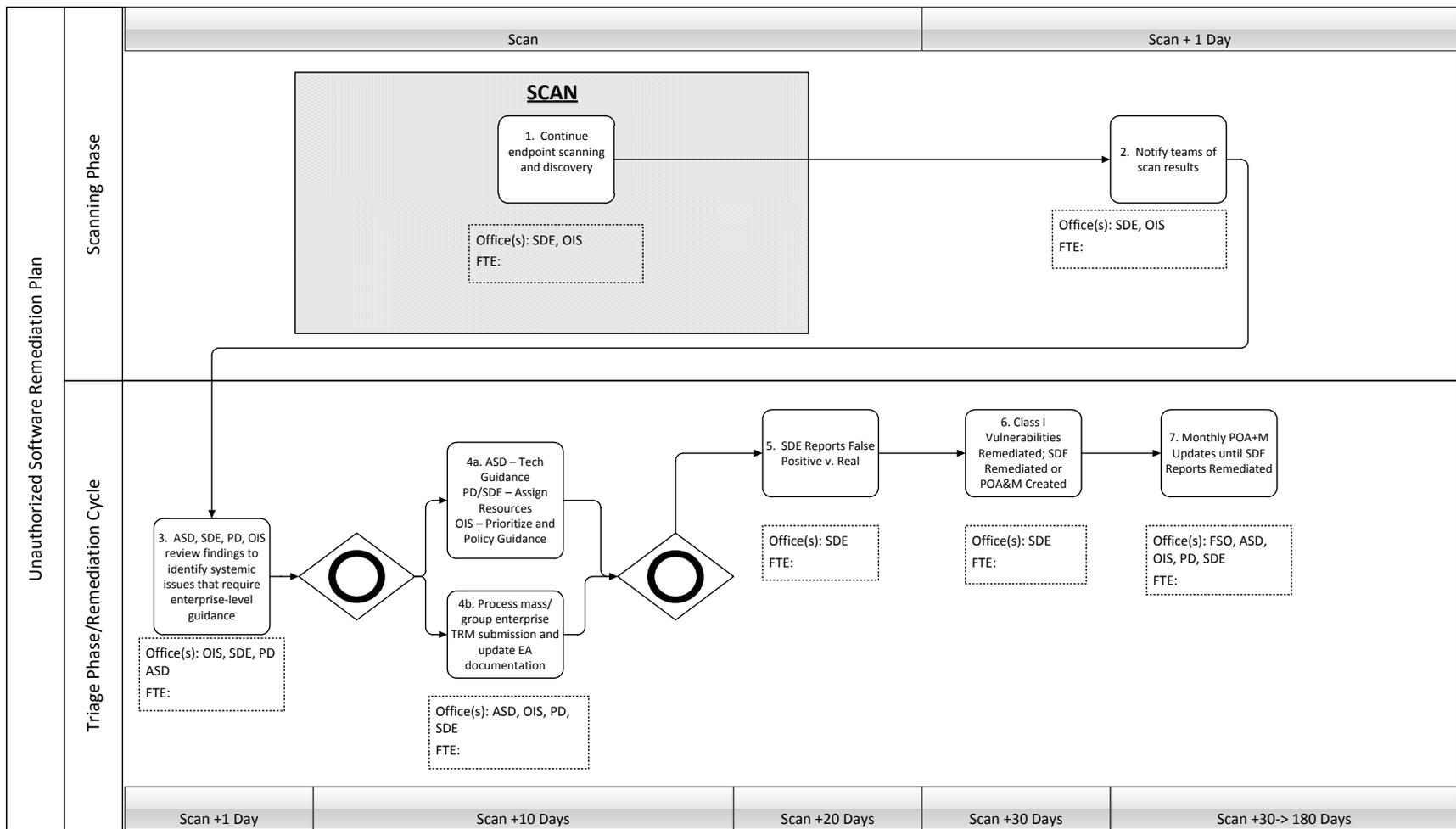


Figure 3: Detailed Process Flow for Removal of Unauthorized Software

## ***Scanning Phase***

### **1. Continue endpoint scanning**

VA will continue with endpoint discovery scans of everything on the VA Network. All sites will continue to be scanned for endpoints that are compliant with the authorized list provided by the Technical Reference Model (TRM). Each month, ASD will publish a draft schedule that will evaluate approximately 17% of the enterprise networks for use in generating reports and for facilitating the remediation efforts.

### **2. Notify Teams of Scan Results**

Notification to engineering and analysis teams that updated scan data is posted. Engineering and analysis teams will receive notification from responsible scan teams.

## ***Triage Phase***

ASD, SDE/PD and OIS will review findings to identify systemic issues that require enterprise level technical or policy guidance to avoid having local sites repeat each other's labor or remediate the same problem differently at various sites.

### **3. Business priority categorization of systems**

Based on business priority function & criticality, ASD will categorize a list of all VA systems based on:

- Person Safety
- Veteran Payments
- Other Operations
- Others

VA must ensure that everything in the VA "Master Reportable FISMA Inventory" is included in the Enterprise Architecture.

### **4. Map IT assets to IT systems**

SDE will use the information found through discovery and the VA list of systems and develop a dependency mapping of IT assets mapped to designated IT systems in the VA enterprise.

### **5. Business priority categorization of assets aligned to systems**

SDE will utilize the lists developed through Business Priority Categorization of Systems and Map IT Assets to IT Systems and develop a comprehensive list of all IT assets in the VA IT Enterprise (regardless of "owner" or "operator") and categorize them by business function and criticality.

### **6. Normalize/reconcile scan inventory and architecture data to generate required reports**

ASD will take the raw data generated through scanning and normalize/reconcile that data to generate required reports. Reports will be categorized by TRM status and based on Business Priority Category:

- Person Safety
- Veteran Payments
- Other Operations
- Others

7. Disseminate initial reports throughout the enterprise

The normalized and reconciled reports will be disseminated throughout the enterprise.

8. IA Risk Assessment of scan results

OIS will categorize and prioritize the list of discovered software based on pre-determined IA Risk Category.

9. Assess Alternative COAs

ASD will analyze the list of normalized software; the mapping of IT assets to IT systems; and IA Risk Assessment and develop:

- List of installed software titles that will be sent to the regions for action
- List of installed software titles that will be handled at the enterprise level. The enterprise list will be divided into 3 sub-categories:
  1. Submit to TRM (Keep)
  2. Replace/Substitute
  3. Remove (with priority/urgency for removal based on multiple criteria)

10. Assign issues that cannot be resolved at the enterprise level

Issues that are determined non-systemic, and thus will not be handled at the enterprise level, will be assigned to the responsible parties to begin the *Remediation Phase*.

11. Build software removal package for enterprise wide software to be removed

Where an issue, deemed systemic, that will handled at the enterprise level, requires removal, SDE will develop a removal package for software to be removed throughout the enterprise. Immediately following the build of the removal package, the *Remediation Cycle* will begin.

12. Build installation prevention packages for enterprise wide software to be removed

Where an issue, deemed systemic, that will handled at the enterprise level, requires installation prevention, SDE will develop an installation prevention package preventing

the software from being installed throughout the enterprise. Immediately following the build of the installation prevention package, the *Remediation Phase* will begin.

13. Build software upgrade package for enterprise wide upgrades

Where an issue, deemed systemic, that will be handled at the enterprise level, requires an upgrade, SDE will develop an upgrade package for software to be upgraded throughout the enterprise. Immediately following the build of the upgrade package, the *Remediation Cycle* will begin.

14. Build software replacement package for enterprise wide software replacements

Where an issue, deemed systemic, that will be handled at the enterprise level, requires replacement prevention, SDE will develop a replacement package for software to be replaced throughout the enterprise. Immediately following the build of the replacement package, the *Remediation Phase* will begin.

15. Process mass/group enterprise wide TRM submission

Where an issue, deemed systemic, that will be handled at the enterprise level, requires an enterprise-wide TRM submission, ASD will develop the enterprise-wide TRM submission package for software to be added to the TRM.

16. Assess enterprise wide TRM requests

Where an issue, deemed systemic, that will be handled at the enterprise level, requires an enterprise-wide TRM submission, ASD will assess the enterprise-wide TRM submission package for software to be added to the TRM.

ASD will provide feedback to SDE for all issues “Approved without constraints” to be incorporated into business priority categorization of assets aligned to systems.

17. Software consolidation analysis and guidance (RRTF)

Based on analysis of all systemic issues handled at the enterprise level, ASD will develop a list of potential ELA candidates for future Ruthless Reduction Task Force (RRTF) initiatives.

18. Software ELA analysis

Based on analysis of all systemic issues handled at the enterprise level, SDE will develop a list of software that may require changes to ELAs, modification to existing ELAs or future ELA awards.

19. ONE VA EA Feedback

Based on analysis of all systemic issues handled at the enterprise level, ASD will provide feedback to the OneVA EA identifying areas to reconcile the TRM, ITARS and other acquisition specific documentation.

***Remediation Cycle***

20. Validation and assignment - Review scan results and identify and report false positives v. actual issues

After received the list of normalized scan results not deemed systemic field offices and EO will work to identify scan and report findings that are “false positives” versus actual issues.

Where false positives have been identified coordination will occur between field offices and EO, and scanning and discovery operators to use that feedback to update tool settings/configurations to reduce future false positives wherever applicable.

21. Submit change order

After validating findings of scan, SDE will determine analyze mapping of IT asset to IT system to determine remediation strategy. SDE will validate all remove/installation prevention/upgrade and replace packages and confirm remediation steps by submitting a Change Order with validated findings.

Standardized change processes and tools (including Implementation Plan, Test Plan and Results, and Back-Out Plan) must be utilized.

22. Detail Remediation Method & POAM

After submitting a Change Order with validated findings SDE must develop a detailed plan of actions and milestones (POA&M) that lists all actions required to perform remediation.

All Remediation Reports and POA&Ms will be completed and submitted using a pre-developed, standard template in the Configuration Management SharePoint site within 30 days of the scan.

23. Execute remediation plan

Within 30 days after scanning has taken place, responsible organizations will execute and fully remediate all known issues based on steps outlined in the POA&M. (Note: All Class I issues MUST be remediated within 30 days after scanning has taken place. Responsible organizations may only provide <150 day POA&Ms for remediation of non-Class I issues.)

24. Identify and document any non-remediated risks

Where non-Class I issues have not been remediated a detailed <150 day POA&M must be developed and submitted to uploaded to the Configuration Management SharePoint site.

25. Participate in monthly risk documentation update (RDU) meetings

If field offices and EO have a POA&M in place to fix issues not remediated within the first 30 days, they will submit monthly status reports via the Configuration Management

SharePoint site and attend monthly status meetings until the issue is fully remediated and they submit a Remediation report for it in the portal.

#### 26. Continue executing long term-remediation plans

Field offices and EO must continue to execute POA&Ms for non-Class I issues until remediated.

#### Tools

Where VA OI&T owns tools with the capabilities to carry out the specific tasks outlined in this design pattern process it must use those tools. If the tools required carrying out a specific task are not currently owned within the VA IT enterprise, VA must purchase those tools in accordance with Federal Acquisition Regulations (FAR). Please refer to Column H in the embedded file located at the end of end of Section 5.1 for tools information associated with each process step.

### 5.4 Vulnerability Scanning and Remediation Process (MW#1)

#### People

Executing this process as described above will result in each site being scanned every month for all known vulnerabilities, and on an ad hoc basis for newly-identified vulnerabilities, with a POA&M being developed outlining remediation activities. Accordingly, each successive scan should generate fewer issues and require less resources to execute, allowing scan frequencies to be increased over time.

Executing this process beginning August 1, 2014 requires necessary staff be dedicated to this effort no later than July 23, 2014, and, purchase of the normalization and rationalization tool be completed no later than August 23, 2014. However, if resources are allocated as required and this process is started no later than August 1, OIG recommendation #1 will be substantially resolved by September 30, 2014.

The defined, and agreed upon, roles and responsibilities for each task involved in the Vulnerability Scanning and Remediation process can be found in the RACI Matrix located in Columns J-R of the "MW#1 Process" tab of the embedded file located at the end of Section 1.

#### Process

The process described herein is a thirty (30) day *Planning, Scanning & Remediation Process* which will be repeated for the entirety of the VA IT enterprise each month such that the every device in the entire VA is scanned for vulnerabilities. This document describes specific activities within each phase of the plan and aligns Offices of Responsibility to each activity.

This process is divided into three phases. The *Scanning Phase*, describes specific steps that must take place prior to vulnerability scanning. The *Triage Phase* describes

the detailed steps that must happen at the enterprise level. The *Remediation Cycle* provides the detailed steps that must occur after scanning has taken place. Coordination must occur, through synchronization meetings across OI&T and with customer organizations and a dedicated collaboration site, to ensure OI&T and customer staffs are prepared when scanning begins, and remain informed and engaged until all vulnerabilities are remediated.

Figure 4 provides a visual overview of the process for vulnerability scanning that consolidates several process steps to show a high-level summary of key activities. The *Scanning Phase* maintains its own area, but for the purposes of simplification, the *Triage Phase* and *Remediation Cycle* have been consolidated into one area to summarize the joint efforts required to develop and execute remediation plans.

This first iteration of this 30 day process MUST start August 1, 2014 in order for the VA to close 2013 FISMA Audit Finding #1 by September 30, 2014. Successful execution of this process starting August 1<sup>st</sup> absolutely requires all necessary resources are allocated No Later Than July 23, 2014 (with some required sooner) in accordance with the Recommendation #1 and #6 Project Plan and the VA Enterprise Configuration Management Design Pattern.

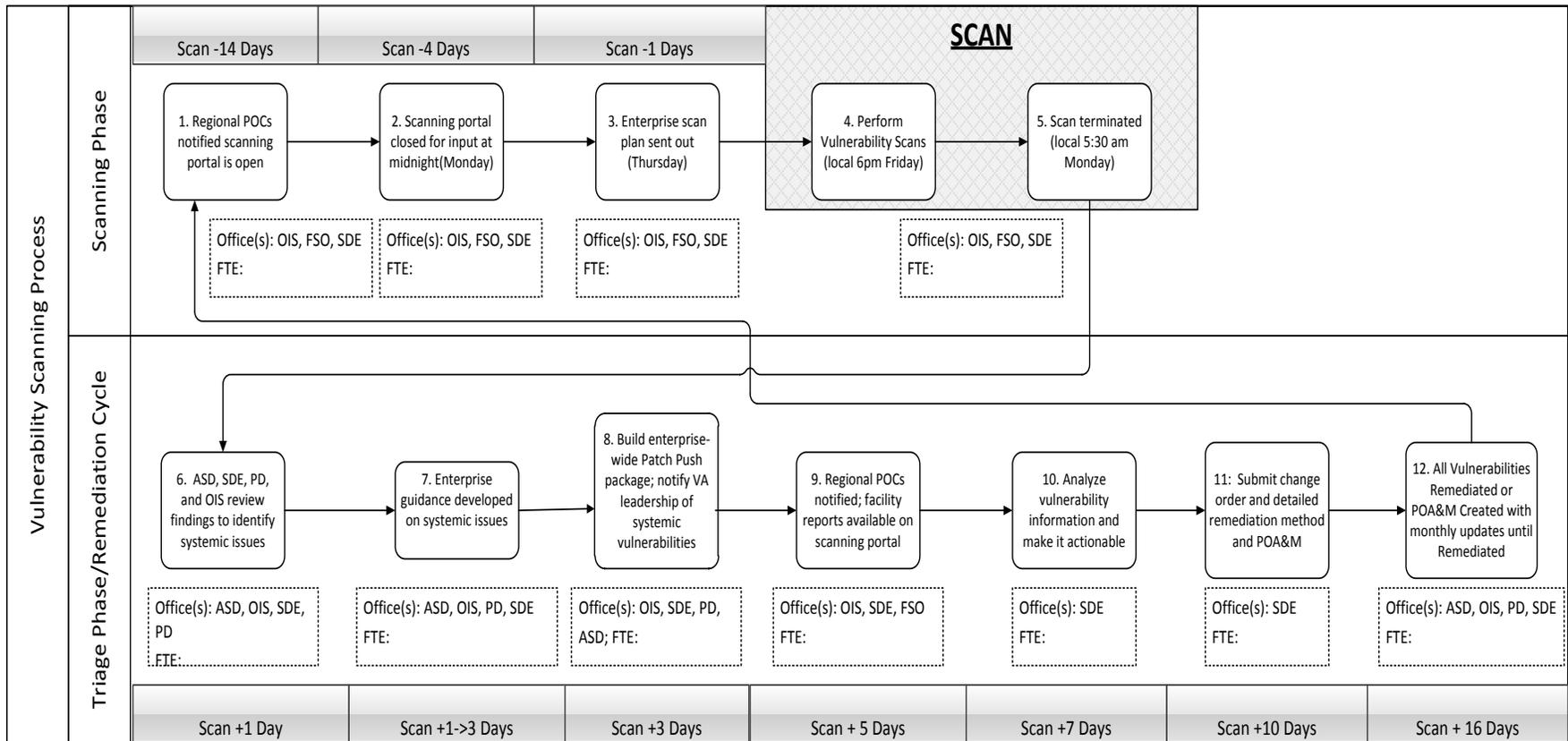


Figure 4: Detailed Process Flow for Vulnerability Scanning and Remediation

## **Scanning Phase**

1. Regional, system and all other scanning POCs notified that scanning portal is open

OIS will notify all points of contact (POC) that the scanning portal is open for input two weeks prior to the start of the monthly enterprise scan.

2. Regional, system and all other scanning POCs populate the portal with IP scan ranges

All notified POCs will populate the scanning portal with IP scan ranges. The scanning portal will be closed for input at midnight (Monday) four days prior to the scan. All regional POCs will be notified.

3. Scanning portal closed for input

Notification will be sent out to all previously notified POCs that the scanning portal will be closed for input at midnight (Monday) four days prior to the scan. All regional POCs will be notified.

4. Validate Accuracy of IP scan ranges for VA sites, to include any exceptions

OIS/SDE will validate with previously notified POCs the accuracy of IP scan ranges for all VA sites being scanned.

5. Enterprise scan plan alert and details are sent out to all POCs

OIS will send out a notification to all previously identified POCs of finalized scan details.

6. Perform vulnerability scans

OIS/SDE will perform vulnerability scanning on all sites outlined in the scan plan. Scanning will begin at 6:00pm (local time) on Friday and terminate at 5:30am (local time) the following Monday.

7. Post sites results to portal; enterprise report also available for distribution

OIS/SDE will post all scan results to the scanning portal, and will also develop enterprise reports. Enterprise reports will be created in three formats: Roll-up report, detailed Excel spreadsheets, and CSV format.

The Roll-up Report will be provided to the Enterprise Change Control Board following each monthly scan.

## **Triage Phase**

ASD, SDE/PD and OIS will review findings to identify systemic issues that require enterprise level technical or policy guidance to avoid having local sites repeat each other's labor or remediate the same problem differently at various sites.

8. Business priority categorization of systems

Based on business priority function & criticality, ASD will categorize a list of all VA systems based on:

- Person Safety
- Veteran Payments
- Other Operations
- Others

VA must ensure that everything in the VA “Master Reportable FISMA Inventory” is included in the Enterprise Architecture.

9. Map IT assets to IT systems

SDE will use the information found through discovery and the VA list of systems and develop a dependency mapping of IT assets mapped to designated IT systems in the VA enterprise.

10. Business priority categorization of assets aligned to systems

SDE will utilize the lists developed through Business Priority Categorization of Systems and Map IT Assets to IT Systems and develop a comprehensive list of all IT assets in the VA IT Enterprise (regardless of “owner” or “operator”) and categorize them by business function and criticality.

11. Merge and normalize/reconcile scan data to enable generation of usable reports

ASD will take the raw data generated through scanning and normalize/reconcile that data to generate required reports. Reports will be categorized by risk status and based on Business Priority Category for all vulnerabilities that are not within the VA baseline.

12. IA Risk Assessment of scan results

OIS will categorize and prioritize the list of all vulnerabilities based on pre-determined IA Risk Category.

13. Group vulnerability findings

ASD will use the IA risk assessment results and group vulnerability findings into 3 categories:

1. Systemic in Baseline
2. Systemic Not in Baseline
3. Not Systemic

14. Distribute non-systemic reports to appropriate parties

ASD will distribute a list of non-systemic vulnerabilities for system owner/operators to develop POA&Ms and other remediation efforts.

15. Inform enterprise of vulnerabilities deemed systemic

ASD will distribute a list of systemic vulnerabilities for enterprise vulnerability management group to develop POA&Ms and being other remediation planning efforts.

16. Build an enterprise-wide Patch Push Package

Where an issue, deemed systemic, that will be handled at the enterprise level, requires an enterprise-wide Patch Push Package to be developed, SDE will develop the enterprise-wide Patch Push Package for vulnerabilities to be patched.

17. Build software upgrade package for enterprise-wide upgrades

Where an issue, deemed systemic, that will be handled at the enterprise level, requires an enterprise-wide Upgrade Package to be developed, SDE will develop the enterprise-wide Upgrade Package for vulnerabilities to be upgraded.

18. Build hardware/software replacement package for enterprise-wide vulnerability replacements

Where an issue, deemed systemic, that will be handled at the enterprise level, requires an enterprise-wide hardware/software Replacement Package to be developed, SDE will develop the enterprise-wide Replacement Package for vulnerabilities to be replaced.

19. Notify VA leadership of systemic vulnerabilities that cannot be fixed without reallocation & prioritization of resources, or policy change

Where an issue, deemed systemic, that will be handled at the enterprise level, is unable to be patched at the enterprise level within significance, reallocation and prioritization of resources, or change in policy OIS will notify Senior VA Leadership.

**Remediation Cycle**

20. Analyze vulnerability information and make it actionable

SDE will analyze the normalized and reconciled list of scan data and assign priority based on risk level. Vulnerabilities considered Emergency MUST be assigned the highest priority. Vulnerabilities will be assigned risk level based on criteria listed below as outlined in the SDE Change Management Plan for National Patch Management.

- *Standard* – based on documented process for the type of change the change would skip as many of the unrelated steps as necessary for streamlining the change.
- *Normal* – No standardized method has been documented for this the process must follow the full National Change Management Process.
- *Emergency* – based on the need for the remediation if the change is designed as an emergency change, the change will be implemented immediately the change will follow normal process but after the fact to ensure communication to the affected areas of the organization.

21. Submit change order

After validating findings of scan, SDE will analyze mapping of IT asset to IT system to determine remediation strategy. SDE will validate all patch/push, upgrade and replace

packages and confirm remediation steps by submitting a Change Order with validated findings.

Standardized change processes and tools (including Implementation Plan, Test Plan and Results, and Back-Out Plan) must be utilized.

#### 22. Detail Remediation Method & POAM

After submitting a Change Order with validated findings SDE must develop a detailed plan of actions and milestones (POA&M) that lists all actions required to perform remediation.

All Remediation Reports and POA&Ms will be completed and submitted using a pre-developed, standard template in the Configuration Management SharePoint site.

#### 23. Execute remediation plan

Within 30 days after scanning has taken place, responsible organizations will have executed and fully remediated all known issues based on steps outlined in the POA&M. (Note: All Class I issues MUST be remediated within 30 days after scanning has taken place.)

#### 24. Identify and document any non-remediated risks

Where non-Class I issues have not been remediated a detailed POA&M must be developed and submitted to uploaded to the Configuration Management SharePoint site.

#### 25. Participate in monthly risk documentation update (RDU) meetings

If field offices and EO have a POA&M in place to fix issues not remediated within the first 30 days, they will submit monthly status reports via the Configuration Management SharePoint site and attend monthly status meetings until the issue is fully remediated and they submit a Remediation report for it in the portal.

#### 26. Continue executing long term-remediation plans

Field offices and EO must continue to execute POA&Ms for non-Class I issues until remediated.

### **TOOLS**

Where VA OI&T owns tools with the capabilities to carry out the specific tasks outlined in this design pattern process it must use those tools. If the tools required carrying out a specific task are not currently owned within the VA IT enterprise VA must purchase those tools in accordance with Federal Acquisition Regulations (FAR). Please refer to Column H in the embedded file located at the end of end of Section 5.1 for tools information associated with each process step.

## 6 SECURITY CONSIDERATIONS

OIS Office of Cyber Security is responsible for monitoring security sources for vulnerability announcements, patch and non-patch remediations, and threats that correspond to the software within the organizational software inventory. A variety of sources should be monitored to ensure that VA is aware of all newly discovered vulnerabilities. OIS Office of Cyber Security is responsible for monitoring for vulnerabilities, remediations, and threats:

- *Vulnerabilities.* Vulnerabilities are software flaws or misconfigurations that cause a weakness in the security of a system. Vulnerabilities can be exploited by a malicious entity to violate policies—for example, to gain greater access or permission than is authorized on a computer.
- *Remediations.* There are three primary methods of remediation: installation of a software patch, adjustment of a configuration setting, and removal of affected software.
- *Threats.* Threats are capabilities or methods of attack developed by malicious entities to exploit vulnerabilities and potentially cause harm to a computer system or network. Threats usually take the form of exploit scripts, worms, viruses, rootkits, and Trojan horses. System administrators should monitor for vulnerabilities, remediations, and threats for systems under their control running software not contained in the organizational inventory.

There are several types of resources available for monitoring the status of vulnerabilities, remediations, and threats. Each type of resource has its own strengths and weaknesses. VA must use more than one type of resource to ensure accurate and timely knowledge. The most common types of resources are as follows:

- Vendor Web sites and mailing lists to obtain all available patches from vendors not supported by the enterprise patch management tool. Vendor Web sites provide:
  - Patches that are released by the application vendors who developed and are most familiar with the product.
  - Patches downloaded from vendor Web sites are most likely free of malicious code.
  - An array of information about vulnerabilities associated with their applications, including methods of mitigation and instructions for installing and using patches.
  - Unique expertise concerning their products.
- Third-party Web sites to obtain all available patches from vendors not supported by the enterprise patch management tool. Third-party websites provide:
  - Timely release of information on new vulnerabilities
  - Depending on the site:
    - Coverage of more than one vendor or product, allowing the system administrator to visit fewer Web sites to gather information (i.e., “one-stop shopping”)

- Specialization in a particular product or platform (saving the system administrator time because they do not have to navigate through unrelated data)
  - For sites that allow site users to post:
    - Similar benefits as the third-party mailing lists and newsgroups
    - A filtering or rating mechanism that allows user to read only “high value” postings
  - Potentially more acceptable alternatives to the official mitigation techniques provided by the vendor
  - Information that the vendor chooses not to provide.
- Third-party mailing lists and newsgroups that highlight the most critical vulnerabilities (e.g., the USCERT Cyber Security Alerts). Such lists will help organizations focus on the most important vulnerabilities that may get overlooked among the myriad of vulnerabilities published by more general vulnerability resources.
- Vulnerability scanners
- Vulnerability databases to obtain immediate information on all known vulnerabilities and suggested remediations (e.g., the National Vulnerability Database)
- Enterprise patch management tools
- Other notification tools

After initial assessment of a new vulnerability, remediation, or threat, OIS Office of Cyber Security will continue to monitor for updates and new information. By performing ongoing monitoring for new information, OIS Office of Cyber Security will be aware of the new patches and will determine if it provides a better solution than a software reconfiguration. Ongoing monitoring is also important because additional analysis of vulnerabilities might determine that they are more or less severe than previously thought.

## **APPENDIX A: RACI CHART DEFINITION**

In project management, it is very important for all the stakeholders to understand the responsibilities and accountabilities of each person. While smaller teams can have more informal rules to keep track of responsibilities, in bigger teams with cross-department and inter-organizational collaboration, it is very important to create a more formal process to track responsibilities. This helps reduce confusion and leads projects to faster completion.

One of the important tools for tracking roles & responsibilities is the Responsibility Assignment Matrix (RACI matrix). RACI stands for:

- Responsible – Who is responsible for the execution of the task?
- Accountable – Who is accountable for the tasks and signs off the work?
- Consulted – Who are the subject matter experts who are to be consulted?
- Informed – Who are the people who need to be updated of the progress?

## **APPENDIX B: RESOURCES**

This Design Pattern includes information and references that were gathered and reviewed from the sites listed below. Additionally, these sites will be used as resource items to implement the processes outlined within this document.

<http://oval.mitre.org/>

<http://nvd.nist.gov/>

<http://cve.mitre.org/compatible/>

<http://www.us-cert.gov/cas/alerts/>

[http://vaww.ea.oit.va.gov/Architecture\\_Engineering\\_Review\\_Board.asp](http://vaww.ea.oit.va.gov/Architecture_Engineering_Review_Board.asp)

<http://trm.oit.va.gov/TRMHomePage.asp>

<http://vaww.ea.oit.va.gov/wp-content/uploads/2014/04/OneVA-Enterprise-Technology-Strategic-Plan-Feb-28-2014-508-corrections-March-25v3.docx>

<https://vaww.portal2.va.gov/sites/infosecurity/index.aspx>

<http://www.iti1-officialsite.com/>

[http://www1.va.gov/vapubs/viewPublication.asp?Pub\\_ID=458&FTtype=2](http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=458&FTtype=2)

## APPENDIX C: DEFINITIONS

Name	Definition
Approved List	A list of discrete entities, such as hosts or applications that are known to be benign and are approved for use within an organization and/or information system.
Authentication (FIPS 200)	Verifying the identify 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 procedres. 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
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;
Configuration Item	<p>An identifiable part of a system (e.g., hardware, software, firmware, documentation, or a combination thereof) that is a discrete target of configuration control processes.</p> <p>A Baseline Configuration is a set of specifications for a system, or 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</p>

		configuration is used as a basis for future builds, releases, and/or changes.
Configuration Identification	Item	Methodology for selecting and naming configuration items that need to be placed under CM;
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.
False Positive		A result that indicates that a given condition is present when it is not
Information System User (CNSSI-4009)		Individual or (system) process acting on behalf of an individual, authorized to access an information system.
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	The probability that a particular threat will exploit a particular vulnerability.
System	A set of IT assets, processes, applications, and related resources that are under the same direct management and budgetary control; have the same function or mission objective; have essentially the same security needs; and reside in the same general operation environment. When not used in this formal sense, the term is synonymous with the term "host". The context surrounding this word should make the definition clear or else should specify which definition is being used.
Systemic	An issue or vulnerability found through scanning or discovery that resides in multiple places throughout the enterprise.
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 or unintentional, with the potential for causing harm to a system.
User	See Information System User
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 D: ACRONYMS

Acronym	Description
ADDM	Atrium Discovery and Dependency Mapping

ASD	Architecture, Strategy and Design
CA	Computer Associates
CA SDM	Computer Associates Service Desk Manager
CCB	Configuration Control Board
CERT	Computer Emergency Readiness Team
CI	Configuration Item
CIO	Chief Information Officer
CM	Configuration Management
CMDB	Configuration Management Database
COTS	Commercial Off-the-shelf
CPE	Common Platform Enumeration
CVE	Common Vulnerabilities and Exposures
DHS	Department of Homeland Security
DOD	Department of Defense
EO	Enterprise Operations
FEA	Federal Enterprise Architecture
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GOTS	Government Off-the-shelf
IBM EPM	IBM Endpoint Manager
IS	Information System
IT	Information Technology
ITAM	Information Technology Asset Management
ITIL	Information Technology Infrastructure Library

LOB	Line-of-Business
MAC	Media Access Control
NIST	National Institute of Standards and Technology
NSD	National Service Desk
OI&T	Office of Information and Technology
OIG	Office of the Inspector General
OIS	Office of Information Security
OMG	Office of Management and Budget
OVAL	Open Vulnerability Assessment Language
PD	Product Development
SCAP	Security Content Automation Protocol
SCCM	System Center Configuration Manager
SDE	Service Delivery Engineering
SIEM	Security Information and Event Management
SLA	Service Level Agreement
TRM	Technical Reference Model
US-CERT	United States Computer Emergency Readiness Team
USGCB	United States Government Configuration Baseline
VA	Department of Veterans Affairs
VASI	Veterans Affairs Systems Inventory
XML	Extensible Markup Language

## **APPENDIX E. REFERENCES/APPLICABLE STANDARDS**

This Design Pattern includes information and references that were gathered and reviewed from:

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
1	VA	VA Directive 6004	<ul style="list-style-type: none"> <li>• Directive establishes VA policy and responsibilities regarding Configuration, Change, and Release Management Programs for implementation across VA.</li> </ul>
2	VA	VA 6500 Handbook	<ul style="list-style-type: none"> <li>• Directive information security program.</li> <li>• Defining overall security framework for VA.</li> </ul>
3	NIST	800-128	<ul style="list-style-type: none"> <li>• Guide for Security-Focused Configuration Management of Information Systems</li> <li>• Provides guidelines for organizations responsible for managing and administering the security of federal information systems and associated environments of operations</li> </ul>
4	NIST	SP 800-63-2	<ul style="list-style-type: none"> <li>• Special Publication — Creating a Patch and Vulnerability Management Program</li> <li>• Designed to assist organizations in implementing security patch and vulnerability remediation programs.</li> </ul>
5	NIST	800-53	<ul style="list-style-type: none"> <li>• Recommended Security Controls for Federal Information Systems and Organizations</li> <li>• Outlines the importance of deploying automated mechanisms to detect unauthorized components and configurations within agency networks</li> </ul>
6	OMB	Memorandum M-14-04	<ul style="list-style-type: none"> <li>• FY2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management</li> <li>• Provides guidance for Federal agencies to follow the report requirements under FISMA.</li> </ul>
7	OMB	Memorandum M-02-01	<ul style="list-style-type: none"> <li>• Guidance for Preparing and Submitting Security Plans of Actions and Milestones</li> <li>• Defines Management and Reporting Requirements for agency POA&amp;Ms, including deficiency descriptions, remediation actions, required resources, and responsible parties.</li> </ul>
8	White House	FISMA Act of 2002	<ul style="list-style-type: none"> <li>• Reauthorizes key sections of the Government Information Security Reform Act</li> <li>• Provides a comprehensive framework for ensuring effective security controls over information resources supporting Federal operations and assets.</li> </ul>
9	VA	CRISP	<ul style="list-style-type: none"> <li>• Intended to improve access controls, configurations management, contingency planning, and the security management of a large number of information technology systems.</li> </ul>
10	Congress	E-Government Act of 2002	<ul style="list-style-type: none"> <li>• Public Law 107-347</li> <li>• 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.</li> </ul>