**Veterans On-line Health Application**

(VOA)

SSP Appendix A

NIST SP 800-53 Rev4 Security Controls

High Baseline

00/00/2016

**Table of Contents**

[1 Technical Controls 5](#_Toc442090760)

[1.1 Access Control (AC) 5](#_Toc442090761)

[AC-2.E5 Account Management E5: Inactivity Logout 5](#_Toc442090762)

[AC-2.E11 Account Management E11: Usage Conditions 5](#_Toc442090763)

[AC-2.E12 Account Management E12: Account Monitoring/ Atypical Usage 5](#_Toc442090764)

[AC-2.E13 Account Management E13: Disable Accounts for High-Risk Individuals 6](#_Toc442090765)

[AC-6.E3 Least Privilege E3: Network Access to Privileged Commands 6](#_Toc442090766)

[AC-6.E5 Least Privilege E5: Privileged Accounts 6](#_Toc442090767)

[AC-6.E9 Least Privilege E9: Auditing Use of Privileged Functions 6](#_Toc442090768)

[AC-6.E10 Least Privilege E10: Prohibit Non-Privileged Users from Executing Privileged Functions 7](#_Toc442090769)

[AC-11.E1 Session Lock E1: Pattern-Hiding Displays 7](#_Toc442090770)

[AC-12.1 Session Termination 7](#_Toc442090771)

[AC-19.E5 Access Control for Mobile Devices E5: Full Device/Container-Based Encryption 8](#_Toc442090772)

[AC-21.1 Information Sharing 8](#_Toc442090773)

[1.2 Audit and Accountability (AU) 8](#_Toc442090774)

[AU-6.E1 Audit Review, Analysis, and Reporting E1: Process Integration 8](#_Toc442090775)

[AU-6.E3 Audit Review, Analysis, and Reporting E3: Correlate Audit Repositories 9](#_Toc442090776)

[AU-6.E5 Audit Review, Analysis, and Reporting E5: Integration/Scanning and Monitoring Capabilities 9](#_Toc442090777)

[AU-6.E6 Audit Review, Analysis, and Reporting E6: Correlation with Physical Monitoring 9](#_Toc442090778)

[AU-9.E2 Protection of Audit Information E2: Audit backup on Separate Physical Systems/Components 9](#_Toc442090779)

[AU-9.E3 Protection of Audit Information E3: Cryptographic Protection 10](#_Toc442090780)

[AU-9.E4 Protection of Audit Information E4: Access by Subset of Privileged Users 10](#_Toc442090781)

[AU-12.E3 Audit Generation E3: Changes by Authorized Individuals 10](#_Toc442090782)

[1.3 Identification and Authentication (IA) 11](#_Toc442090783)

[IA-2.E11 Identification and Authentication E11: Remote Access – Separate Device 11](#_Toc442090784)

[IA-2.E12 Identification and Authentication E12: Acceptance of PIV Credentials 11](#_Toc442090785)

[IA-5.E11 Authenticator Management E11: Hardware Token-Based Authentication 11](#_Toc442090786)

[IA-8.E1 Identification and Authentication E1: Acceptance of PIV Credentials from Other Agencies 12](#_Toc442090787)

[IA-8.E2 Identification and Authentication E2: Acceptance of Third-Party Credentials 12](#_Toc442090788)

[IA-8.E3 Identification and Authentication E3: Use of FICAM-Approved Products 12](#_Toc442090789)

[IA-8.E4 Identification and Authentication E4: Use of FICAM-Issued Profiles 12](#_Toc442090790)

[1.4 System and Communications Protection (SC) 13](#_Toc442090791)

[SC-7.E18 Boundary Protection E18: Fail Secure 13](#_Toc442090792)

[SC-7.E21 Boundary Protection E21: Isolation of Information System Components 13](#_Toc442090793)

[SC-21.1 Secure Name/Address Resolution Service (Recursive or Caching Resolver) 13](#_Toc442090794)

[SC-22.1 Architecture and Provisioning for Name/Address Resolution Service 14](#_Toc442090795)

[SC-39.1 Process Isolation 14](#_Toc442090796)

[2 MANAGEMENT Controls 14](#_Toc442090797)

[2.1 Security Assessment and Authorization (CA) 14](#_Toc442090798)

[CA-3.E5 System Interconnections E5: Restrictions on External System Connections 14](#_Toc442090799)

[CA-7.E1 Continuous Monitoring E1: Independent Assessment 15](#_Toc442090800)

[CA-8.1 Penetration Testing 15](#_Toc442090801)

[CA-9.1 Internal System Connections 15](#_Toc442090802)

[2.2 Planning (PL) 15](#_Toc442090803)

[PL-2.E3 System Security Plan E3: Plan/Coordinate with Other Organizational Entities 15](#_Toc442090804)

[PL-4.E1 Rules of Behavior E1: Social Media and Networking Restrictions 16](#_Toc442090805)

[PL-8.1 Information Security Architecture 16](#_Toc442090806)

[2.3 Risk Assessment (RA) 17](#_Toc442090807)

[RA-5.E2 Vulnerability Scanning E2: Update by Frequency/Prior to New Scan/When Identified 17](#_Toc442090808)

[RA-5.E5 Vulnerability Scanning E5: Privileged Access 17](#_Toc442090809)

[2.4 System and Services Acquisition (SA) 17](#_Toc442090810)

[SA-4.E2 Acquisition Process E2: Design/Implementation Information for Security Controls 17](#_Toc442090811)

[SA-4.E9 Acquisition Process E9: Functions/Ports/Protocols/Services in Use 18](#_Toc442090812)

[SA-4.E10 Acquisition Process CE 10: Use of Approved PIV Products 18](#_Toc442090813)

[SA-9.E2 External Information System Services E2: Identification of Functions/Ports/Protocols/Services 18](#_Toc442090814)

[SA-15.1 Development Processes, Standards, and Tools 18](#_Toc442090815)

[SA-16.1 Developer-Provided Training 19](#_Toc442090816)

[SA-17.1 Developer Security Architecture and Design 19](#_Toc442090817)

[3 OPERATIONAL Controls 20](#_Toc442090818)

[3.1 Awareness and Training (AT) 20](#_Toc442090819)

[AT-2.E2 Security Awareness Training E2: Insider Threat 20](#_Toc442090820)

[3.2 Configuration Management (CM) 20](#_Toc442090821)

[CM-2.E7 Baseline Configuration E7: Configure Systems, Components, or Devices for High-Risk Areas 20](#_Toc442090822)

[CM-7.E2 Least Functionality E2: Prevent Program Execution 20](#_Toc442090823)

[CM-7.E4 Least Functionality E4: Unauthorized Software/Blacklisting 21](#_Toc442090824)

[CM-7.E5 Least Functionality E5: Authorized Software/Whitelisting 21](#_Toc442090825)

[CM-8.E3 Information System Component Inventory E3: Automated Unauthorized Component Detection 21](#_Toc442090826)

[CM-10.1 Software Usage Restrictions 21](#_Toc442090827)

[CM-11.1 User-Installed Software 22](#_Toc442090828)

[3.3 Contingency Planning (CP) 22](#_Toc442090829)

[CP-2.E3 Contingency Plan E3: Resume Essential Missions/Business Functions 22](#_Toc442090830)

[CP-2.E4 Contingency Plan E4: Resume All Missions/Business Functions 22](#_Toc442090831)

[CP-2.E5 Contingency Plan E5: Continue Essential Missions/Business Functions 23](#_Toc442090832)

[CP-2.E8 Contingency Plan E8: Identify Critical Assets 23](#_Toc442090833)

[CP-9.E5 Information System Backup E5: Transfer to Alternate Storage Site 23](#_Toc442090834)

[3.4 Incident Response (IR) 24](#_Toc442090835)

[IR-3.E2 Incident Response Testing E2: Coordination with Related Plans 24](#_Toc442090836)

[IR-4.E4 Incident Handling E4: Information Correlation 24](#_Toc442090837)

[3.5 Maintenance (MA) 24](#_Toc442090838)

[MA-5.E1 Maintenance Personnel E1: Individuals without Appropriate Access 24](#_Toc442090839)

[3.6 Media Protection (MP) 25](#_Toc442090840)

[MP-7.1 Media Use 25](#_Toc442090841)

[MP-7.E1 Media Use E1: Prohibit Use without Owner 25](#_Toc442090842)

[3.7 Physical and Environmental Protection (PE) 25](#_Toc442090843)

[PE-6.E4 Monitoring Physical Access E4: Monitoring Physical Access to Information Systems 25](#_Toc442090844)

[3.8 Personnel Security (PS) 26](#_Toc442090845)

[PS-4.E2 Personnel Termination E2: Automated Notification 26](#_Toc442090846)

[3.9 System and Information Integrity (SI) 26](#_Toc442090847)

[SI-4.1 Information System Monitoring 26](#_Toc442090848)

[SI-7.E5 Software, Firmware, and Information Integrity E5: Automated Response to Integrity Violations 27](#_Toc442090849)

[SI-7.E7 Software, Firmware, and Information Integrity E7: Integration of Detection and Response 27](#_Toc442090850)

[SI-7.E14 Software, Firmware, and Information Integrity E14: Binary or Machine Executable Code 27](#_Toc442090851)

[SI-8.E1 Spam Protection E1: Central Management 28](#_Toc442090852)

[SI-8.E2 Spam Protection E2: Automatic Updates 28](#_Toc442090853)

[SI-16.1 Memory Protection 28](#_Toc442090854)

# Technical Controls

## Access Control (AC)

### AC-2.E5 Account Management E5: Inactivity Logout

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization requires that users log out when *[Assignment: organization-defined time-period of expected inactivity or description of when to log out]*. | H | |
| Security Control Provider  **EO Managed**  Customer Managed  *EIS Service Line*  *ETM Service Line* | |
| Implementation | Determine how long the application can be inactive before the user is logged out.  Users are required to log out of the workstation at the end of the defined Tour of Duty. While at work, the use of the CTRL-ALT-DEL key combination will “lock” their workstation so that a password is required to re-enter.  Users must also secure their workstation at the end of each day. Systems are configured, as are all other VA workstations and laptops, to initiate a lock when a specific time of inactivity has elapsed, 15 minutes for a workstation and five minutes for servers and laptops. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### AC-2.E11 Account Management E11: Usage Conditions

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The information system enforces *[Assignment: organization-defined circumstances and/or usage conditions]* for *[Assignment: organization-defined information system accounts]*. | H | |
| Security Control Provider  **EO Managed**  Customer Managed  *EIS Service Line*  *ETM Service Line* | |
| Implementation | Does the application limit account usage? If so, describe the restrictions.  If not, are account usage limits enforced through another means as a compensating control (such as Active Directory or Group Policy)?  If there is only a single functioning layer of operations with the system (for example, an application that has only one class of user) that permits a single operation to occur, describe that functionality and how it would not be applicable to this control.  EO adheres to the specific conditions and circumstances under which information system accounts can be used in the VA Rules of Behavior (ROB). | Implemented |  |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### AC-2.E12 Account Management E12: Account Monitoring/ Atypical Usage

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization:   1. Monitors information system accounts for *[Assignment: organization-defined atypical use]*; and 2. Reports atypical usage of information system accounts to the ISO. | H | |
| Security Control Provider  **EO Managed**  Customer Managed  *EIS Service Line*  *ETM Service Line* | |
| Implementation | Does the application monitor and report a typical usage such as accessing the application outside of normal usage patterns? What group or role receives the report (VA 6500 specifies the ISO)?  What would the System Owner describe as a typical usage? Can it be audited and addressed in the AU controls?  EO does not monitor or report a typical usage of information system accounts. Malicious or suspicious behavior is monitored by VA-NSOC and EO Technical Security. | Implemented |  |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### AC-2.E13 Account Management E13: Disable Accounts for High-Risk Individuals

|  |  |  |  |
| --- | --- | --- | --- |
| Control | When a high-risk individual is identified, how long does it take to get the user’s account disabled (VA 6500 specifies “immediately”)?  The organization disables accounts of users posing a significant risk immediately following administrator notification after discovery of the risk. | H | |
| Security Control Provider  **EO Managed**  Customer Managed  *EIS Service Line*  *ETM Service Line* | |
| Implementation | EO disables accounts of users posing a significant risk to organizations prior to notifying the individual of personnel sanctions or termination; and within one hour, in keeping with incident response policy. This would include individuals for whom reliable evidence or intelligence indicates either the intention to use authorized access to information systems to cause harm; or through whom adversaries will cause harm. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### AC-6.E3 Least Privilege E3: Network Access to Privileged Commands

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization authorizes network access to *[Assignment: organization-defined privileged commands]* only for *[Assignment: organization-defined compelling operational needs]* and documents the rationale for such access in the security plan for the information system. | H | |
| Security Control Provider  **EO Managed**  Customer Managed  *DCO Service Line* | |
| Implementation | Within the application, how is elevated privilege authorization documented?  Per VA 6500: OIT restricts privileged accounts on the information system to designated officials/positions. Individuals who have been approved by their supervisor, the ISO, and the System Owner via the Elevated Privilege Memo. The memo ensures the user has received the necessary approvals, has the appropriate BI, signed the Elevated Privileges ROB, and has taken the system administrator TMS training. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### AC-6.E5 Least Privilege E5: Privileged Accounts

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization restricts privileged accounts on the information system to *[Assignment: organization-defined personnel or roles]*. | H, M | |
| Security Control Provider  **EO Managed**  Customer Managed  *DCO Service Line* | |
| Implementation | Discuss how configuration settings are used to restrict privileged application users from accessing key security parameters at the system level.  Enterprise Operations restricts privileged accounts on the information system to Administrator and Super-user accounts. Administrators have two accounts: One for user functions; and a non-mail-enabled account (NMEA) for system administration duties. Each account is restricted to the functions authorized for that specific purpose. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### AC-6.E9 Least Privilege E9: Auditing Use of Privileged Functions

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The information system audits the execution of privileged functions. | H, M | |
| Security Control Provider  **EO Managed**  Customer Managed  *DCO Service Line*  *EIS Service Line*  *ETM Service Line* | |
| Implementation | Discuss how the application logs privileged user functions. Are all privileged actions logged? Are only privileged actions that failed logged?  Enterprise Operations audits the execution of privileged functions. EO Systems Security Standard Operating Procedures (SOP) T012-052014-REV1.2 defines the auditing of privileged functions in the appendix. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### AC-6.E10 Least Privilege E10: Prohibit Non-Privileged Users from Executing Privileged Functions

|  |  |  |  |
| --- | --- | --- | --- |
| Control | Discuss how the application prevents non-privileged users from using accessing privileged user areas in the application?  The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/ countermeasures | H, M | |
| Security Control Provider  **EO Managed**  Customer Managed  *DCO Service Line*  *EIS Service Line*  *ETM Service Line* | |
| Implementation | Enterprise Operations prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/ countermeasures. Administrators have a non-mail-enabled account (NMEA) for system administration and all privileged functions are limited to this kind of account. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### AC-11.E1 Session Lock E1: Pattern-Hiding Displays

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image. | H, M | |
| Security Control Provider  **EO Managed**  Customer Managed  *EIS Service Line*  *ETM Service Line* | |
| Implementation | Discuss if the application has a publically viewable image implemented as a part of the session lock. Does that image obscure the information within the application that was viewable at the time of the timeout?  Enterprise Operations information systems conceal, via the session lock, information previously visible on the display with a publicly viewable image. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### AC-12.1 Session Termination

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The information system automatically terminates a user session after *[Assignment: organization-defined conditions or trigger events requiring session disconnect]*. | H, M | |
| Security Control Provider  **EO Managed**  Customer Managed  *EIS Service Line*  *ETM Service Line* | |
| Implementation | Provide details of conditions that would cause a session disconnect; such as periods of user inactivity, targeted responses to certain types of incidents, time-of-day restrictions on information system use or other trigger events requiring automatic session termination.  Enterprise Operations information systems terminate a user session after 30 minutes of inactivity or upon receiving a request from a user.  VA:   1. VA Workstation sessions are persistent until logoff; or upon a restart of the information system.   VPN sessions terminate after 24 hours of inactivity. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### AC-19.E5 Access Control for Mobile Devices E5: Full Device/Container-Based Encryption

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization employs *[Selection: full-device encryption; container encryption]* to protect the confidentiality and integrity of information on *[Assignment: organization-defined mobile devices]*. | H, M | |
| Security Control Provider  Customer Managed  *EIS Service Line*  *ETM Service Line* | |
| Implementation | EO employs *full-device encryption* to protect the confidentiality and integrity of information on *all portable computers and laptops*.  Only approved, agency-owned, writable, removable media is permitted on the network and components, in addition, these media types are required to be encrypted with FIPS 140-2 certified encryption. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### AC-21.1 Information Sharing

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization:   1. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for *[Assignment: organization-defined information sharing circumstances where user discretion is required]*; and 2. Employs *[Assignment: organization-defined automated mechanisms or manual processes]* to assist users in making information sharing/collaboration decisions. | H, M | |
| Security Control Provider  Customer Managed  *DCO Service Line* | |
| Implementation | There is currently no policy regarding AC-21 information sharing. However, the dissemination of Protected Health Information (PHI) and Personally Identifiable Information (PII) is restricted to collaboration tools that use cryptographic mechanisms to protect the confidentiality and integrity of such information (e.g., PKI). The use of peer-to-peer file sharing applications is prohibited. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

## Audit and Accountability (AU)

### AU-6.E1 Audit Review, Analysis, and Reporting E1: Process Integration

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. | H, M | |
| Security Control Provider  **EO Managed**  Customer Managed  *DCO Service Line* | |
| Implementation | Logs are sent to EO Technical Security; responsibility for monitoring and analysis of logs as well as incident response fall under their purview. Technical Security serves as the centralized collection point for audit logs. Through the use of QRadar SIEM, monitoring and reporting are handled in one location.  Technical Security also serves as part of the Incident Response process. Associated guidelines and procedures require that all VA computer security incidents be reported to VA-NSOC which is the VA Central Incident Response Capability (VA-CIRC) through the ISO within one business day of the first observation of the incident.  VA-CIRC policy requires that, upon identification of an incident or suspected incident, a preliminary report is generated. For incidents that affect critical systems and/or may have adverse global effects on VA network, VA-CIRC will dispatch a fly-away team of technical and forensic experts to assist facility personnel in impact containment. VA-CIRC is responsible for supplying incident reports to VA organizations as appropriate.  VA-NSOC also monitors and manages host-based and network-based intrusion detection sensors and firewalls at all VA network interconnection points. When attacks are detected, VA-CIRC cyber security team isolates the problem, develops and implements a fix, and tracks the source of the attack so that action can be taken, and manages the Department wide recovery effort when required. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### AU-6.E3 Audit Review, Analysis, and Reporting E3: Correlate Audit Repositories

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | H, M | |
| Security Control Provider  **EO Managed**  Customer Managed  *DCO Service Line* | |
| Implementation | QRadar can be configured to analyze and correlate audit records to vulnerabilities to gain organization-wide situational awareness in support of incident reporting. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### AU-6.E5 Audit Review, Analysis, and Reporting E5: Integration/Scanning and Monitoring Capabilities

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization integrates analysis of audit records with analysis of *[Selection (one or more): vulnerability scanning information; performance data; information system monitoring information; [Assignment: organization-defined data/information collected from other sources]]* to further enhance the ability to identify inappropriate or unusual activity. | H | |
| Security Control Provider  **EO Managed**  Customer Managed  *DCO Service Line* | |
| Implementation | EO Technical Security integrates functions for the analysis of audit records with analysis of *vulnerability scanning information and information collected from other sources* to further enhance the ability to identify inappropriate or unusual activity.  If vulnerabilities exist as indicated by scan results, remediation or compensating controls are initiated to reduce risk. This may include more frequent reviews or mitigation during scheduled patch cycles. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### AU-6.E6 Audit Review, Analysis, and Reporting E6: Correlation with Physical Monitoring

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization correlates information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity. | H | |
| Security Control Provider  **EO Managed**  Customer Managed  *DCO Service Line* | |
| Implementation | QRadar can be configured to analyze and correlate audit records to gain organization-wide situational awareness in support of incident reporting. The facility Physical Security Officer (PSO) reviews proximity reports and visitor logs and reports inappropriate or unusual activity to the ISO. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### AU-9.E2 Protection of Audit Information E2: Audit backup on Separate Physical Systems/Components

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The information system backs up audit records *[Assignment: organization-defined frequency]* onto a physically different system or system component than the system or component being audited. | H | |
| Security Control Provider  Customer Managed  *DCO Service Line* | |
| Implementation | Do you back up logs on an external device or system?  If yes, how often?  Enterprise Operations collects audit logs in near-real-time and backs them up to a centralized QRadar repository to allow for inspection of events leading to a catastrophic system failure. Audit logs are not kept on the system being audited. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### AU-9.E3 Protection of Audit Information E3: Cryptographic Protection

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The information system implements cryptographic mechanisms to protect the integrity of audit information and audit tools. | H | |
| Security Control Provider  Customer Managed  *DCO Service Line* | |
| Implementation | Please add how encryption is employed for this particular application.  Enterprise Operations implements cryptographic mechanisms to protect the integrity of audit information and audit tools.  The QRadar security information and event management (SIEM) console is the only authorized Secure Shell (SSH) connection to all of the other processors for functionality and restrictions.  One central location for SSH access protects the audit tools from compromised integrity.  The only allowed access to the logs is through the QRadar graphical user interface (GUI) and only allows read-only access for all user roles. The logs are not even in a readable format prior to encryption. QRadar performs hashing on all incoming log files and supports SHA-1, SHA-2 and MD5 encryption. QRadar does not need to employ whole-disk encryption because all data is hashed. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### AU-9.E4 Protection of Audit Information E4: Access by Subset of Privileged Users

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization authorizes access to management of audit functionality to only *[Assignment: organization-defined subset of privileged users]*. | H, M | |
| Security Control Provider  Customer Managed  *DCO Service Line* | |
| Implementation | Enterprise Operations authorizes access to management of audit functionality to only Technical Security personnel. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### AU-12.E3 Audit Generation E3: Changes by Authorized Individuals

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The information system provides the capability for *[Assignment: organization-defined individuals or roles]* to change the auditing to be performed on *[Assignment: organization-defined information system components]* based on *[Assignment: organization-defined selectable event criteria]* within *[Assignment: organization-defined time thresholds]*. | H | |
| Security Control Provider  **EO Managed**  Customer Managed  *DCO Service Line*  *EIS Service Line*  *ETM Service Line* | |
| Implementation | Enterprise Operations provides the capability for *information owners and Technical Security personnel* to change the auditing to be performed on *EO information systems* based on security, *business, and mission requirements* within *30 days.* | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

## Identification and Authentication (IA)

### IA-2.E11 Identification and Authentication E11: Remote Access – Separate Device

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets FIPS 201-1 requirements (assuming user and system administrator accounts are as described in control AC-5.E6). As such, they require the use of PIV cards. | H, M | |
| Security Control Provider  **EO Managed**  Customer Managed  *EIS Service Line*  *ETM Service Line* | |
| Implementation | Multi-factor authentication for remote access to *privileged and non-privileged accounts* (e.g., VA Citrix Access Gateway) isn’t currently supported. OMB M-07-16 requires Government remote access solutions to utilize Multifactor Authentication to confirm a remote user’s access and identity. After the retirement of One-VA VPN in 2013, VA implemented POA in February 2014 and is now compatible with all GFE VPN access methods. PIV and PIN are utilized in lieu of multifactor authentication as prescribed by OMB.  **RBD 15-028:** Enterprise Operations Wide Multifactor Authentication Vulnerabilities IA-2(1-4, 11)  This RBD was executed, effective on December 1, 2014. | Implemented |  |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision | x |
|  | |

### IA-2.E12 Identification and Authentication E12: Acceptance of PIV Credentials

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials. | H, M, L | |
| Security Control Provider  **EO Managed**  Customer Managed  *EIS Service Line*  *ETM Service Line* | |
| Implementation | Enterprise Operations information systems accept and electronically verify Personal Identity Verification (PIV) credentials. EO issued PIV ID cards comply with HSPD-12 ensuring secure access to facilities and disaster response sites; as well as enabling digital signature and encryption capabilities. EO users have the ability to use PIV for logical access (network logon) to information system resources. All workstations are equipped and accept PIV for identification and authentication (with PIN) to Windows Active Directory.  For further information on how EO uses VA implementation, see the National [Field Operations Wiki Knowledge Repository, Wiki Library (PIV)](https://vaww.sde.portal.va.gov/sites/fo/FOWiki/Wiki/PIV.aspx) | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### IA-5.E11 Authenticator Management E11: Hardware Token-Based Authentication

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The information system, for hardware token-based authentication, employs mechanisms that satisfy *[Assignment: organization-defined token quality requirements]*. | H, M, L | |
| Security Control Provider  **EO Managed**  Customer Managed  *DCO Service Line*  *EIS Service Line*  *ETM Service Line* | |
| Implementation | The eToken Universal Serial Bus (USB) is used by EO for hardware token-based authentication; and employs mechanisms that satisfy basic *multifactor authentication* requirements for Non-Mail Enabled Administrator (NMEA) accounts. Access using the NMEA account may only be accomplished with the additional authentication mechanism of the eToken USB.  VA/OI&T/SDE [Strong Authentication for IT SysAdmins Bulletin No. X](https://vaww.sde.portal.va.gov/docctr/Bulletins/Strong_Authentication_X.pdf) indicates multifactor requirements are satisfied for system administrator access to Windows servers. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### IA-8.E1 Identification and Authentication E1: Acceptance of PIV Credentials from Other Agencies

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies. | H, M, L | |
| Security Control Provider  **EO Managed**  Customer Managed | |
| Implementation | EO does not support Personal Identity Verification (PIV) credentials from other federal agencies for physical access control systems (PACS). Personal Identity Verification (PIV) credentials issued by federal agencies that conform to FIPS Publication 201 are granted access to EO facilities based upon a demonstrated need for such access (e.g. OPM). There is no public access to EO datacenters. | Implemented |  |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable | x |
| Risk Based Decision |  |
|  | |

### IA-8.E2 Identification and Authentication E2: Acceptance of Third-Party Credentials

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The information system accepts only FICAM-approved third-party credentials. | H, M, L | |
| Security Control Provider  Customer Managed  *DCO Service Line* | |
| Implementation | VA and EO trust such credentials only at their approved assurance levels. Federal Identity, Credential, and Access Management (FICAM) third-party credentials issued by non-federal government entities approved for use may include:     * State-issued driver’s licenses * US Passports * Social Security Card * Credentials issued by the DoD (Military ID)   **RBD 15-079:** EO does not accept FICAM-approved third-party credentials.  This RBD was executed, effective March 5, 2015 | Implemented |  |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision | x |
|  | |

### IA-8.E3 Identification and Authentication E3: Use of FICAM-Approved Products

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization employs only FICAM-approved information system components in *[Assignment: organization-defined information systems]* to accept third-party credentials. | H, M, L | |
| Security Control Provider  Customer Managed  *DCO Service Line* | |
| Implementation | EO-managed information systems that are public-facing for the purposes of providing VA services may use FICAM-approved third-party credentials for identity verification.  [Identity and Access Management (IAM)](http://vaww.iam.va.gov/) services describe who users are to VA, verify user identity, and use those facts to help authorize user access to VA information systems, applications, and resources.  **RBD 15-079:** EO/DCO Personnel Access Control System (PACS) does not accept third-party credentials or employ FICAM-approved information system components unless the other-agency PIV has enrolled in PACS. This is inconsistent with HSPD-12 and [OMB Memorandum M-11-11](http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf).  This RBD was executed, effective March 5, 2015 | Implemented |  |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision | x |
|  | |

### IA-8.E4 Identification and Authentication E4: Use of FICAM-Issued Profiles

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The information system conforms to FICAM-issued profiles. | H, M, L | |
| Security Control Provider  Customer Managed  *DCO Service Line* | |
| Implementation | EO does not currently use any FICAM authentication protocols such as SAML 2.0 and OpenID 2.0, or FICAM Backend Attribute Exchange.  **RBD 15-079:** FICAM-issued profiles are not implemented in EO.  This RBD was executed, effective March 5, 2015 | Implemented |  |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision | x |
|  | |

## System and Communications Protection (SC)

### SC-7.E18 Boundary Protection E18: Fail Secure

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The information system fails securely in the event of an operational failure of a boundary protection device. | H | |
| Security Control Provider  **EO Managed**  Customer Managed  *DCO Service Line*  *ETM Service Line* | |
| Implementation | Define and describe how the system responds when a boundary protection device (Firewall, Gateway, or Proxy Server) fails and the path is closed. The system should cease to send or receive traffic or route traffic to another boundary device. Ascreen shot of routing tables can provide further evidence of this control. | Implemented |  |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### SC-7.E21 Boundary Protection E21: Isolation of Information System Components

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization employs boundary protection mechanisms to separate *[Assignment: organization-defined information system components]* supporting *[Assignment: organization-defined missions and/or business functions]*. | H | |
| Security Control Provider  Customer Managed  *DCO Service Line*  *ETM Service Line* | |
| Implementation | This is a VA agency-wide control that is provided by the VA Network Security Operations Center (VA-NSOC).  Boundary protection devices separate publically accessible applications and websites from veteran information resources and databases by the use of a firewalled DMZ. Enterprise Backup (EBU) processes are separated from user accessible networks by the use of a Virtual LAN (VLAN). | Implemented |  |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### SC-21.1 Secure Name/Address Resolution Service (Recursive or Caching Resolver)

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources. | H, M, L | |
| Security Control Provider  Customer Managed  *DCO Service Line* | |
| Implementation | *This is a VA agency-wide control that is provided by VA Network Security Operations Center (VA-NSOC).*  The functionality of secure name/address resolution services is provided by VA-NSOC. Address Resolution services are inherited from VA-NSOC. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### SC-22.1 Architecture and Provisioning for Name/Address Resolution Service

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation. | H, M, L | |
| Security Control Provider  Customer Managed  *DCO Service Line* | |
| Implementation | *This is a VA agency-wide control that is provided by VA Network Security Operations Center (VA-NSOC).*  The functionality of secure name/address resolution services is provided by VA-NSOC. Address Resolution services are inherited from VA-NSOC. The VA National Directory Services Team manages the architecture and provisioning for Name/Address Resolution Services in VA. This control is implemented for EO and all DNS servers are redundant and fault-tolerant. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### SC-39.1 Process Isolation

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The information system maintains a separate execution domain for each executing process. | H, M, L | |
| Security Control Provider  **EO Managed**  Customer Managed  *EIS Service Line*  *ETM Service Line* | |
| Implementation | Define and describe how the system executes application processes separately from each other and other processes running on the system.  EO/EIS information systems maintain separate execution domains for each executing process by assigning each process a separate address space. Each information system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process. Maintaining separate execution domains for executing processes is a function of the operating system (OS) and EIS infrastructure. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

# MANAGEMENT Controls

## Security Assessment and Authorization (CA)

### CA-3.E5 System Interconnections E5: Restrictions on External System Connections

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization employs *[Selection: allow-all, deny-by-exception; deny-all, permit-by-exception]* policy for allowing *[Assignment: organization-defined information systems]* to connect to external information systems. | H, M | |
| Security Control Provider  Customer Managed  *EO Service Line* | |
| Implementation | Enterprise Operations employs a *deny-all, permit-by-exception* policy for allowing connections to external information systems.  VA Enterprise Security Change Control Board (ESCCB) was established to ensure all proposed interconnections to VA networks and systems have been reviewed and approved prior to initiating a connection; and ensuring there will be no adverse impact to the operation of existing systems, the operating environment, or subsystems. No external connections are allowed without an signed ISA/MOU and subsequent ESCCB approval. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### CA-7.E1 Continuous Monitoring E1: Independent Assessment

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization employs assessors or assessment teams with *[Assignment: organization-defined level of independence]* to monitor the security controls in the information system on an ongoing basis. | H, M | |
| Security Control Provider  Customer Managed  *EO Service Line* | |
| Implementation | EO employs assessors or assessment teams as appointed by OIS. The assessors are contractors with OI&T Enterprise Risk Management to perform Security Control Assessment (SCA) on a periodic basis; and the assigned ISO is responsible to do ad hoc assessments and monitor the security controls in EO information systems on an ongoing basis. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### CA-8.1 Penetration Testing

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization conducts penetration testing *[Assignment: organization-defined frequency]* on *[Assignment: organization-defined information systems or system components]*. | H | |
| Security Control Provider  Customer Managed  *EO Service Line* | |
| Implementation | Penetration testing of EO information systems is limited to a simple TCP/UDP port scan in addition to the monthly vulnerability scanning with Tenable Nessus. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### CA-9.1 Internal System Connections

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization:   1. Authorizes internal connections of *[Assignment: organization-defined information system components or classes of components]* to the information system; and 2. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated. | H, M, L | |
| Security Control Provider  **EO Managed**  Customer Managed  *DCO Service Line* | |
| Implementation | EO:   1. Authorizes internal connections to *VA information systems*; and   Documents, for each internal connection, the platform, interface characteristics, dependencies, and topology. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

## Planning (PL)

### PL-2.E3 System Security Plan E3: Plan/Coordinate with Other Organizational Entities

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization plans and coordinates security-related activities affecting the information system with *[Assignment: organization-defined individuals or groups]* before conducting such activities in order to reduce the impact on other organizational entities. | H, M | |
| Security Control Provider  **EO Managed**  Customer Managed  *DCO Service Line*  *EIS Service Line*  *ETM Service Line* | |
| Implementation | Explain how Managers coordinate across the various groups anytime activities can affect the application. Provide that list of defined groups and individuals here.  Note: VA Handbook 6500 states that the system owner is responsible for identifying these organization-defined individuals or groups.  Enterprise Operations plans and coordinates security-related activities affecting hosted information system with Continuous Readiness Information Security Program (CRISP) and National Service Desk (NSD) before conducting such activities in order to reduce the impact on other organizational entities. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### PL-4.E1 Rules of Behavior E1: Social Media and Networking Restrictions

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites. | H, M | |
| Security Control Provider  Customer Managed  *EO Service Line* | |
| Implementation | VA encourages the use of social media in VA Directive 6515 *Use of Web-based Collaboration Technologies;* and defines acceptable behavior for the use of social media technologies.  VA personnel and organizations must exercise sound judgment when utilizing web-based collaboration tools. The use of VA web-based collaboration tools must promote the mission, goals, and objectives of VA. Such use must also be consistent with applicable laws, regulations, and policy, as well as prudent operational, security, and privacy considerations. VA 6515 states: “When interacting with the public online, VA employees must draw a clear distinction between their personal views and their professional duties. Employees who are not officially authorized to speak on behalf of VA must never state or infer their communications represent an official position.”  <http://vaww.va.gov/opa/Social_Media_Policy.asp> | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### PL-8.1 Information Security Architecture

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization:   1. Develops an information security architecture for the information system that:    1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;    2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and    3. Describes any information security assumptions about, and dependencies on, external services; 2. Reviews and updates the information security architecture *[Assignment: organization-defined frequency]* to reflect updates in the enterprise architecture; and 3. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions. | H, M | |
| Security Control Provider  Customer Managed  *DCO Service Line* | |
| Implementation | Enterprise Operations:   1. Has developed an information security architecture for EO that:    1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;    2. Describes how service line architecture is integrated into and supports the enterprise architecture; and    3. Describes any information security assumptions about, and dependencies on, external services (currently none for the EO Service Line – see implementation detail for control SA-17); 2. Reviews and updates the information security architecture *at least annually* to reflect updates in the enterprise architecture; and 3. Ensures that planned security architecture changes are reflected in this security plan, the security Concept of Operations (CONOPS – see SSP section 1.6), and organizational procurements/acquisitions. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

## Risk Assessment (RA)

### RA-5.E2 Vulnerability Scanning E2: Update by Frequency/Prior to New Scan/When Identified

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization updates the information system vulnerabilities scanned *[Selection (one or more): [Assignment: organization-defined frequency]; prior to a new scan; when new vulnerabilities are identified and reported].* | H, M | |
| Security Control Provider  Customer Managed  *DCO Service Line* | |
| Implementation | *This control is provided by EO Technical Security and the EO Continual Readiness in Information Security Program (CRISP).*  The EO implementation of Tenable Nessus vulnerability scanning tools updates the information system vulnerabilities scanned daily. Scans are performed every thirty (30) days and when a custom/ad hoc scan is requested, or when new vulnerabilities are identified and reported. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### RA-5.E5 Vulnerability Scanning E5: Privileged Access

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The information system implements privileged access authorization to *[Assignment: organization-identified information system components]* for selected *[Assignment: organization-defined vulnerability scanning activities]*. | H, M | |
| Security Control Provider  **EO Managed**  Customer Managed  *DCO Service Line* | |
| Implementation | Which specific system components has the System Owner identified as requiring privileged access? How as privileged access granted? How is it documented?  What specific vulnerability scanning activities are performed on those components?  *This control is provided by EO Technical Security and the EO Continual Readiness in Information Security Program (CRISP).*  EO implements privileged access authorization to *hosted information systems* for monthly scans. System Owners are responsible to provide scan credentials for the information system per EO Technical Security guidelines.  All systems are scanned to the extent of ability/technology (i.e., some legacy systems and network appliances do not allow for the configuration of scanning credentials). | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

## System and Services Acquisition (SA)

### SA-4.E2 Acquisition Process E2: Design/Implementation Information for Security Controls

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: *[Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design/implementation information]]* at *[Assignment: organization-defined level of detail]*. | H, M | |
| Security Control Provider  Customer Managed  *DCO Service Line* | |
| Implementation | *This control is provided VA-wide by the Office of Information & Technology (OI&T) and locally by Data Center Operations (DCO).*  DCO requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes system interconnection agreements, system diagrams, control implementation detail, and a Privacy Threshold Analysis (PTA).  VA/OI&T has created standardized information system security and privacy language for design and implementation that is included in information system acquisition contracts that involve non-VA entities.  The requirements are included in VA Handbook 6500.6 *Contract Security*, Appendix C. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### SA-4.E9 Acquisition Process E9: Functions/Ports/Protocols/Services in Use

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use. | H, M | |
| Security Control Provider  Customer Managed  *DCO Service Line* | |
| Implementation | *This control is provided VA-wide by the Office of Information & Technology (OI&T) and locally by Data Center Operations (DCO).*  EO/DCO requires developers of information systems, system components, or services to identify early in the SDLC, the functions, ports, protocols, and services intended for organizational use.  EO systems are required to use the SDE/ESE approved baselines and hardening guides provided by EO Technical Security. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### SA-4.E10 Acquisition Process CE 10: Use of Approved PIV Products

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems. | H, M, L | |
| Security Control Provider  Customer Managed  *DCO Service Line* | |
| Implementation | *This control is provided VA-wide by the Office of Information & Technology (OI&T) and locally by Data Center Operations (DCO).*  EO/DCO employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems. Additionally, products must be approved by VA Technical Reference Model (VA-TRM) as established by OI&T/ASD.  [VA-PIV](https://vaww.sde.portal.va.gov/sites/fo/svcs/ectm/fis/piv/default.aspx)  [VA-PKI](https://vaww.portal.va.gov/sites/PKI/_layouts/viewlsts.aspx) | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### SA-9.E2 External Information System Services E2: Identification of Functions/Ports/Protocols/Services

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization requires providers of *[Assignment: organization-defined external information system services]* to identify the functions, ports, protocols, and other services required for the use of such services. | H, M | |
| Security Control Provider  Customer Managed  *DCO Service Line* | |
| Implementation | ***This control is provided VA-wide by the Office of Information & Technology (OI&T) and locally by Data Center Operations (DCO).***  DCO requires third-party service providers to identify the functions, ports, protocols, and other services required for the use of such services. | Implemented |  |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### SA-15.1 Development Processes, Standards, and Tools

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization:   1. Requires the developer of the information system, system component, or information system service to follow a documented development process that:    1. Explicitly addresses security requirements;    2. Identifies the standards and tools used in the development process;    3. Documents the specific tool options and tool configurations used in the development process; and    4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and 2. Reviews the development process, standards, tools, and tool options/configurations *[Assignment: organization-defined frequency]* to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy *[Assignment: organization-defined security requirements]*. | H | |
| Security Control Provider  Customer Managed  *DCO Service Line* | |
| Implementation | *This control is provided VA-wide by the Office of Information & Technology (OI&T) and locally by Data Center Operations (DCO).*  The Program Management Accountability System, (PMAS) is a performance-based project management tool; and use is mandated by the Assistant Secretary, Office of Information & Technology (AS/IT) for all product delivery projects.  PMAS requires the use of incremental product build techniques for IT projects in cycles of six months or less. Projects managed under PMAS are closely monitored and subject to being halted when significant deviations to plans occur and insufficient remediation plans are presented.  EO:   1. Requires information system developers to follow the PMAS process that:    1. Explicitly addresses security requirements;    2. Identifies the standards and tools used in the development process;    3. Documents the specific tool options and tool configurations used in the development process; and    4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and 2. Reviews the development process, standards, tools, and tool options/configurations on a continuous basis to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy PMAS process and security requirements. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### SA-16.1 Developer-Provided Training

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization requires the developer of the information system, system component, or information system service to provide *[Assignment: organization-defined training]* on the correct use and operation of the implemented security functions, controls, and/or mechanisms. | H | |
| Security Control Provider  Customer Managed  *DCO Service Line* | |
| Implementation | *This control is provided VA-wide by the Office of Information & Technology (OI&T) and locally by Data Center Operations (DCO).*  EO/DCO requires the vendor/developer of the information system, component, or service to provide *user-acceptance training (UAT)* on the features, correct use, and operation of the implemented security functions, controls, and/or mechanisms. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### SA-17.1 Developer Security Architecture and Design

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that:   1. Is consistent with and supportive of the organization’s security architecture which is established within and is an integrated part of the organization’s enterprise architecture; 2. Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and 3. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection. | H | |
| Security Control Provider  Customer Managed  *DCO Service Line* | |
| Implementation | Enterprise Operations requires developers to produce a design specification and security architecture using the PMAS process that:   1. Describes how service line architecture is integrated into and supports the enterprise architecture using SDE/ESE approved baseline documents; 2. Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and 3. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and VA standard RMF approach to protection. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

# OPERATIONAL Controls

## Awareness and Training (AT)

### AT-2.E2 Security Awareness Training E2: Insider Threat

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization includes security awareness training on recognizing and reporting potential indicators of insider threat. | H, M | |
| Security Control Provider  Customer Managed  *EO Service Line* | |
| Implementation | *This control is provided VA-wide by the VA Human Resources & Administration (HRA), VA Learning University (VALU) Talent Management System (TMS).*  VA includes security awareness training on recognizing and reporting potential indicators of insider threat. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

## Configuration Management (CM)

### CM-2.E7 Baseline Configuration E7: Configure Systems, Components, or Devices for High-Risk Areas

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization:   1. Issues *[Assignment: organization-defined information systems, system components, or devices]* with *[Assignment: organization-defined configurations]* to individuals traveling to locations that the organization deems to be of significant risk; and 2. Applies *[Assignment: organization-defined security safeguards]* to the devices when the individuals return. | H, M | |
| Security Control Provider  Customer Managed  *DCO Service Line* | |
| Implementation | Enterprise Operations does not issue information systems or devices to individuals traveling to locations with significant risk. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### CM-7.E2 Least Functionality E2: Prevent Program Execution

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The information system prevents program execution in accordance with *[Selection (one or more): [Assignment: organization-defined policies regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage]*. | H, M | |
| Security Control Provider  **EO Managed**  Customer Managed  *EIS Service Line*  *ETM Service Line* | |
| Implementation | *This control is provided by Enterprise Operations (EO) and is implemented by DCO personnel.*  Software list features:   1. The VA has developed and maintains the One-VA Technical Reference Model (TRM) website at <http://trm.oit.va.gov>. TRM presents lists of prospective technologies for use in the development of VA IT solutions. The lists provide guidance, with constraints, on the permissible range of technologies that a development project may select to meet project requirements. The lists are not intended to direct procurements, although reference is made, where known, to existing VA licensing. 2. EO also provides a ‘Master Software List’ of approved software at <https://portal.cdco.va.gov/sites/CDCO-Internal/COMM/CAD/Lists/Master%20Software%20List1/Approved.aspx>.   EO maintains a listing of authorized software as the Technical Architecture Board (TAB) Software Master List, which designates prospective technologies as approved or not approved for the development of EO IT solutions. Tenable Nessus scans are conducted monthly for EO information systems and will flag any vulnerability that manifests itself due to unauthorized program execution. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### CM-7.E4 Least Functionality E4: Unauthorized Software/Blacklisting

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization:   1. Identifies *[Assignment: organization-defined software programs not authorized to execute on the information system]*; 2. Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system; and 3. Reviews and updates the list of unauthorized software programs *[Assignment: organization-defined frequency]*. | M | |
| Security Control Provider  Customer Managed  *DCO Service Line* | |
| Implementation | EO:   1. Identifies software programs not authorized to execute on EO information systems only with respect to malware protection; a comprehensive list is not maintained; 2. Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on EO information systems; and 3. Reviews and updates the list of unauthorized software programs on a continual basis.   This lists prospective technologies allowed and disallowed use in the development of EO solutions. EO denies the execution of all software programs identified by VA, OI&T, and industry best practices as potentially harmful to the information system or components and specific programs are denied authorization to execute through the use of approved baseline configurations, Group Policy Objects (GPO), and IE Profiles.  \*\*\* NOTE: Not Applicable to Low or High systems (Moderate only) \*\*\*  **RBD 15-140:** EO Unauthorized Software List - EO has not established a formal strategy that includes a “white” list and “black” list to manage software allowed to install and execute on organizational information systems.  However, the following safeguards have been implemented:   * Visibility to Servers (V2S) provides unified monitoring consoles, national management views, and reporting capabilities to compensate for no list of unauthorized software and EO is continuously scanning for malware and malicious software code. * EO does not utilize automated mechanisms to detect and notify designated officials of unauthorized software but FireEye and Nessus scans continue to identify vulnerabilities for all software in use, including unauthorized software. * EO has implemented a formal continuous monitoring program utilizing the Governance, Risk and Compliance (GRC) application approved for VA, Agiliance RiskVision™, to improve the process of identifying and remediating vulnerabilities. This application allows EO to implement and integrate continuous monitoring into risk management and the A&A processes. * EO adheres to VA Technical Reference Model (TRM), which provides guidance and constraints on the permissible software that development projects may select to meet application requirements. * EO adheres to Service Delivery & Engineering (SDE) Enterprise Systems Engineering (ESE) approved baselines. * EO maintains the [Technical Architecture Board (TAB)](https://vaww.sde.portal.va.gov/sites/eoservices/COMM/CAD/Pages/default.aspx) Software Master List, which lists approved technologies for the development of EO information technology solutions.   This RBD was executed, effective April 6, 2015. | Implemented |  |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision | x |
|  | |

### CM-7.E5 Least Functionality E5: Authorized Software/Whitelisting

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization:   1. Identifies *[Assignment: organization-defined software programs authorized to execute on the information system]*; 2. Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and 3. Reviews and updates the list of authorized software programs *[Assignment: organization-defined frequency]*. | H | |
| Security Control Provider  Customer Managed  *DCO Service Line* | |
| Implementation | EO:   1. Identifies software programs not authorized to execute on EO information systems only with respect to malware protection; a comprehensive list is not maintained; 2. Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on EO information systems; and 3. Reviews and updates the list of unauthorized software programs on a continual basis.   This lists prospective technologies allowed and disallowed use in the development of EO solutions. EO denies the execution of all software programs identified by VA, OI&T, and industry best practices as potentially harmful to the information system or components and specific programs are denied authorization to execute through the use of approved baseline configurations, Group Policy Objects (GPO), and IE Profiles.  \*\*\* NOTE: Not Applicable to Low or High systems (Moderate only) \*\*\*  **RBD 15-140:** EO Unauthorized Software List - EO has not established a formal strategy that includes a “white” list and “black” list to manage software allowed to install and execute on organizational information systems.  However, the following safeguards have been implemented:   * Visibility to Servers (V2S) provides unified monitoring consoles, national management views, and reporting capabilities to compensate for no list of unauthorized software and EO is continuously scanning for malware and malicious software code. * EO does not utilize automated mechanisms to detect and notify designated officials of unauthorized software but FireEye and Nessus scans continue to identify vulnerabilities for all software in use, including unauthorized software. * EO has implemented a formal continuous monitoring program utilizing the Governance, Risk and Compliance (GRC) application approved for VA, Agiliance RiskVision™, to improve the process of identifying and remediating vulnerabilities. This application allows EO to implement and integrate continuous monitoring into risk management and the A&A processes. * EO adheres to VA Technical Reference Model (TRM), which provides guidance and constraints on the permissible software that development projects may select to meet application requirements. * EO adheres to Service Delivery & Engineering (SDE) Enterprise Systems Engineering (ESE) approved baselines. * EO maintains the [Technical Architecture Board (TAB)](https://vaww.sde.portal.va.gov/sites/eoservices/COMM/CAD/Pages/default.aspx) Software Master List, which lists approved technologies for the development of EO information technology solutions.   This RBD was executed, effective April 6, 2015. | Implemented |  |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision | x |
|  | |

### CM-8.E3 Information System Component Inventory E3: Automated Unauthorized Component Detection

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization:   1. Employs automated mechanisms *[Assignment: organization-defined frequency]* to detect the presence of unauthorized hardware, software, and firmware components within the information system; and 2. Takes the following actions when unauthorized components are detected: *[Selection (one or more): disables network access by such components; isolates the components; notifies [Assignment: organization-defined personnel or roles]].* | H, M | |
| Security Control Provider  Customer Managed  *DCO Service Line*  *EIS Service Line*  *ETM Service Line* | |
| Implementation | *This control is provided by Enterprise Operations (EO) and implemented by DCO personnel.*  EO:   1. Employs automated mechanisms quarterly to detect the addition of unauthorized components/devices into the information system. The detection of unauthorized network components is performed by two organizationally separated work centers; and 2. On a quarterly basis, The EO Technical Security work center uses Tenable Nessus in “Discovery” mode to detect any unauthorized components in the network; and 3. The Configuration Management (CM) work center uses the SolarWinds Orion networks discovery program and the VEEAM VMware reporting tool to search for unauthorized components; 4. Upon discovery of an unauthorized component two steps are immediately taken: 5. All open ports on the component are disabled; 6. A NSD SDM Change Order (CO) is opened. The component is analyzed off line to determine component characteristics. The CM work center and the appropriate technical work center are assigned the CO to ensure a fully populated Configuration Item (CI) record entry is added to the CMDB; and 7. Additionally, the CM work center regularly audits the CMDB against Discovery tool reports. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### CM-10.1 Software Usage Restrictions

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization:   1. Uses software and associated documentation in accordance with contract agreements and copyright laws; 2. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and 3. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work. | H, M, L | |
| Security Control Provider  **EO Managed**  Customer Managed  *DCO Service Line* | |
| Implementation | a) Verify with the Build/Application Manager at AITC which software is covered by enterprise licenses. Verify with Product Development (PD) which software is covered by other licenses. For commercial off-the-shelf (COTS) software, the licensing for the various components is typically covered by the purchase price of the OTS software. The PD Project Manager can verify this.  b) Enterprise licenses are tracked by the Infrastructure team. PD PMs track licenses specific to their application/system.  c) Peer-to-peer file sharing technology is prohibited within the VA. Users do not have access to install the software on their workstations. (Verify with EO Technical Security how peer-to-peer file sharing is blocked).  EO follows all software usage restrictions as identified by manufacturers and VA Policy. Before being granted access to the system, all users are required to sign the VA National Rules of Behavior (ROB) that complies with VA software usage restrictions:   1. Use software and associated documentation in accordance with contract agreements and copyright laws; only system administrators are authorized to download or install any software to the information system; documentation is available to users according to least privilege; and EO complies with all software licensing agreements installing only those applications necessary for least functionality; 2. Employs SMS/SCCM and other workstation-resident tracking systems for software, license, and associated documentation protected by quantity licenses (to control copying and distribution); and 3. Limits/controls/documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted/patented work in accordance with the VA Rules of Behavior.   All VA users are accountable for their actions while accessing the information system. A ROB is signed by all users before they are authorized any access; and the ROB states policy concerning unauthorized software installation, including a section entitled “Prohibited Internet Uses,” that prohibits the “downloading, installing, storing, or use of any software that is in violation of patent, copyright, or license agreements.  EO runs reports (on an ad hoc basis) to verify how many instances of a particular piece of software have been installed. Microsoft usage is verified and validated on an annual basis and reported to VA Enterprise Systems Engineering (ESE). When usage is greater than the current license amount, the office or group is contacted and made aware of the situation; the number of installations is reduced or additional licenses are purchased.  VA Handbook 6500 directs that all VA employees shall ensure that government-acquired commercial software is used only in accordance with licensing agreements. It is the responsibility of management and individual employees to ensure that proprietary software is properly licensed before being installed on VA equipment.  Furthermore, VA employees are required to protect government and public interests as they perform their duties. This includes assuring that government-acquired software protected under the Copyright Act is used in accordance with the law and the software licensing agreement. This policy may not apply to software developed by the Department or for use under a Department-wide license. VA personnel in violation of software use policies may be at risk of personnel sanctions, termination, or civil/criminal prosecution. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### CM-11.1 User-Installed Software

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization:  Establishes *[Assignment: organization-defined policies]* governing the installation of software by users;  Enforces software installation policies through *[Assignment: organization-defined methods]*; and  Monitors policy compliance at *[Assignment: organization-defined frequency]*. | H, M, L | |
| Security Control Provider  Customer Managed  *DCO Service Line* | |
| Implementation | EO prohibits end-users from installing any software on their desktops by limiting desktop admin rights to only the Customer Support Staff. All requests for non-standard software are received and tracked through NSD. Software is only installed if it is approved by the TRM.  EO personnel do not have local administrative rights to user workstations. All software installations must utilize NSD and the change control process. VA Employees/Contractors in violation of software use policies may be at risk of personnel sanctions, termination, or civil/criminal prosecution.  Policy prohibits end-users from installing any software on their desktops by limiting desktop admin rights to only Operations Staff. All requests for non-standard software are received and tracked through the NSD Helpdesk.  The VA Rules of Behavior specifies the following regarding user installed software:   * Downloading, installing, storing, or using the software from the Internet in violation of any patent, copyright, or license agreement is prohibited. * Installing unauthorized software is prohibited. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

## Contingency Planning (CP)

### CP-2.E3 Contingency Plan E3: Resume Essential Missions/Business Functions

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization plans for the resumption of essential missions and business functions within *[Assignment: organization-defined time period]* of contingency plan activation. | H, M | |
| Security Control Provider  Customer Managed  *DCO Service Line* | |
| Implementation | EO plans for the resumption of essential missions and business functions for high, moderate and low systems respectively:   * Critical: For critical support, they have 12 hours. * Essential: For essential support, they have 72 hours. * Routine: For routine support, they have 30 days.   Information System RTO and RPO are contingent on the specific EO Hosting Agreements and SLA. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### CP-2.E4 Contingency Plan E4: Resume All Missions/Business Functions

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization plans for the resumption of all missions and business functions within *[Assignment: organization-defined time period]* of contingency plan activation. | H | |
| Security Control Provider  Customer Managed  *DCO Service Line*  *EIS Service Line*  *ETM Service Line* | |
| Implementation | EO plans for the resumption of essential missions and business functions for high, moderate and low systems respectively:   * Critical: For critical support, they have 12 hours. * Essential: For essential support, they have 72 hours. * Routine: For routine support, they have 30 days.   Information System RTO and RPO are contingent on the specific EO Hosting Agreements and SLA. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### CP-2.E5 Contingency Plan E5: Continue Essential Missions/Business Functions

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites. | H | |
| Security Control Provider  Customer Managed  *DCO Service Line*  *EIS Service Line*  *ETM Service Line* | |
| Implementation | EO plans for the continuance of essential missions and business functions at the designated alternate processing site with little or no loss of operational continuity and sustains that continuity until full information system restoration/site restoration at primary processing and/or storage sites. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### CP-2.E8 Contingency Plan E8: Identify Critical Assets

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization identifies critical information system assets supporting essential missions and business functions. | H, M | |
| Security Control Provider  Customer Managed  *DCO Service Line* | |
| Implementation | EO identifies critical information system assets supporting essential missions and business functions in the associated ISCP or Disaster Recovery Plan (DRP).  EO has no critical infrastructure as defined by DHS. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### CP-9.E5 Information System Backup E5: Transfer to Alternate Storage Site

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization transfers information system backup information to the alternate storage site *[Assignment: organization-defined time period and transfer rate consistent with the recovery time and recovery point objectives]*. | H | |
| Security Control Provider  Customer Managed  *DCO Service Line* | |
| Implementation | *This control is provided by SDE Enterprise Operations and implemented by DCO personnel.*  EO/DCO transfers backup tapes to the alternate storage site *daily.* | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

## Incident Response (IR)

### IR-3.E2 Incident Response Testing E2: Coordination with Related Plans

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization coordinates incident response testing with organizational elements responsible for related plans. | H, M | |
| Security Control Provider  Customer Managed  *DCO Service Line* | |
| Implementation | *This control is provided EO-wide by Data Center Operations (DCO).*  As part of the annual COOP exercise, DCO tests and/or exercises the incident response capability for EO to determine the incident response effectiveness and documents the results. DCO has an annual incident response training program in place that occurs during contingency testing. Results are documented and maintained on file. As a part of VA-CIRC procedures, OIS and CIRC routinely test its Incident Response capabilities. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### IR-4.E4 Incident Handling E4: Information Correlation

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response. | H | |
| Security Control Provider  Customer Managed  *DCO Service Line* | |
| Implementation | *This control is provided EO-wide by Data Center Operations (DCO).*  DCO uses the VA-NSOC’s provided FERET (Formal Event And Evaluation Tool) ticketing / tracking system to achieve an organization-wide perspective on incident awareness and response. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

## Maintenance (MA)

### MA-5.E1 Maintenance Personnel E1: Individuals without Appropriate Access

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization:   1. Implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:    1. Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified;    2. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and 2. Develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system. | H | |
| Security Control Provider  Customer Managed  *EO Service Line* | |
| Implementation | *This control is provided EO-wide by Data Center Operations (DCO).*  DCO:   1. Implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:      * 1. Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified;   2. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and  1. Develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system.   If maintenance is performed by a vendor or third party maintenance personnel who do not have needed access authorizations, Once the maintenance has been completed, the maintenance tools are inspected to verify that no data has been retained.  If the data cannot be sanitized, the tools will remain at the Facility or be destroyed. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

## Media Protection (MP)

### MP-7.1 Media Use

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization *[Selection: restricts; prohibits]* the use of *[Assignment: organization-defined types of information system media]* on *[Assignment: organization-defined information systems or system components]* using *[Assignment: organization-defined security safeguards]*. | H, M, L | |
| Security Control Provider  Customer Managed  *DCO Service Line* | |
| Implementation | *This control is provided EO-wide by Data Center Operations (DCO).*  DCO restricts the use of media and uses the following safeguards:  VA policy prohibits the use of any non-VA approved media in organizational information systems. VA has installed a software package called *Lumension Endpoint Security* that controls access to all USB ports, serial / parallel ports, and CD/DVD devices.  *Lumension Endpoint Security* is installed on all desktops, laptops, and servers; and is configured to allow selected devices to function, but will block any attempt to write data to unapproved removable media. For example, USB keyboards/mice will function, but writing data to a USB flash drive is blocked unless it is VA-issued with FIPS 140-2 approved encryption. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### MP-7.E1 Media Use E1: Prohibit Use without Owner

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner. | H, M | |
| Security Control Provider  Customer Managed  *DCO Service Line* | |
| Implementation | *This control is provided EO-wide by Data Center Operations (DCO).*  DCO prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner. All media is scanned using antivirus software prior to use. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

## Physical and Environmental Protection (PE)

### PE-6.E4 Monitoring Physical Access E4: Monitoring Physical Access to Information Systems

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization monitors physical access to the information system in addition to the physical access monitoring of the facility as *[Assignment: organization-defined physical spaces containing one or more components of the information system]*. | H | |
| Security Control Provider  Customer Managed  *DCO Service Line* | |
| Implementation | *This control is provided EO-wide by Data Center Operations (DCO).*  DCO Physical Security Officer (PSO) monitors physical access to the datacenter computer rooms in addition to the physical access monitoring of the facility.  **PITC and CRRC:**  Monitoring is done by GSA personnel. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

## Personnel Security (PS)

### PS-4.E2 Personnel Termination E2: Automated Notification

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization employs automated mechanisms to notify *[Assignment: organization-defined personnel or roles]* upon termination of an individual. | H | |
| Security Control Provider  Customer Managed  *DCO Service Line* | |
| Implementation | ***This control is provided VA-wide by the Office of Information Security (OIS).***  DCO employs automated mechanisms to notify supervisors/COR upon termination of an individual. This is done via NSD and the VA 9957 process. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

## System and Information Integrity (SI)

### SI-4.1 Information System Monitoring

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization:   1. Monitors the information system to detect:    1. Attacks and indicators of potential attacks in accordance with *[Assignment: organization-defined monitoring objectives]*; and    2. Unauthorized local, network, and remote connections; 2. Identifies unauthorized use of the information system through *[Assignment: organization-defined techniques and methods]*; 3. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization; 4. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; 5. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; 6. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and 7. Provides *[Assignment: organization-defined information system monitoring information]* to *[Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].* | H, M, L | |
| Security Control Provider  Customer Managed  *DCO Service Line* | |
| Implementation | *Explain how Signature definitions (DAT files) are automatically updated by the AV software. Describe how often this happens and where the new definitions are obtained (automatic download from McAfee, etc…).*  *This control is provided EO-wide by DCO/VA-NSOC.*  Datacenter Operations:   1. Monitors events on the information system in accordance with the [Field Security Operations (FSO)](https://vaww.sde.portal.va.gov/sites/fo/Pages/Default.aspx) Critical Infrastructure Protection (CIP) service guidelines;and detects information system attacks through the deployment of an enterprise-wide Intrusion Detection System (IDS); 2. Identifies unauthorized use of the information system; 3. Deploys monitoring devices: (i) strategically, with the deployment of server-based Host Intrusion Protection System (HIPS) to collect operating environment essential information; and (ii) at ad hoc locations determined by VA-CIRC/NSOC to track specific types of transactions of interest; 4. Heightens the level of information system monitoring activity by real-time audit log monitoring (QRadar) whenever there is an indication of increased risk to datacenter operations and assets, individuals, hosted applications, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; and 5. Obtains legal opinion from the Office of the General Counsel (OGC) with regard to information system monitoring activities: In accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and prior to conducting such activities.   The Office of Information Security (OIS) Critical Infrastructure Protection (CIP) service is responsible for developing and deploying data integrity controls on an enterprise basis that protect VA networks from accidental or malicious alteration or destruction, such as anti-virus, national gateways, intrusion detection systems, and authentication and authorization technologies.  VA IT SDE (005OP) email directive, dated 8/9/2012, approved by the National Change Control Board (NCCB) resulted in a National Change Order requiring all servers running McAfee Host Intrusion Prevention System (HIPS) to implement 100% Blocking Mode.  OIS has also installed, configured, and maintains an enterprise IDS solution. All IDS systems are centrally controlled and monitored at VA-CIRC.  A centralized monitoring console (ISS SiteProtector) for all NIDS, NIPS and HIDS is deployed which is the central management and reporting system for the network-based IDS/IPS and host-based IDS. VA-NSOC also performs VA network monitoring 24 hours a day, seven days a week using deployed sensor equipment throughout VA.  Datacenters reside on VA networks and therefore will be included in VA-CIRC intrusion detection. DCO uses the QRadar Log Manager and ANR to monitor and generate electronic notifications.  Dashboard capabilities have been implemented and are accessible to EO Technical Security and National Service Desk (NSD) personnel. The systems generated notifications are reviewed by all relevant staff. Once detected, formal email notifications are submitted to ISOs, local security and network staff via CIRC and/or ANR email distribution for remediation action. Systems have been fine-tuned to disregard normal traffic and avoid false positives. The scheduled collection of logs runs every 24 hrs.  DCO consults VA OGC for guidance and the legal limitations to information system monitoring activities, prior to the deployment of monitoring tools:  <http://vaww.ogc.vaco.portal.va.gov/Pages/Default.aspx> | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### SI-7.E5 Software, Firmware, and Information Integrity E5: Automated Response to Integrity Violations

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The information system automatically shuts the information system down; restarts the information system; implements *[Assignment: organization-defined security safeguards]]* when integrity violations are discovered. | H | |
| Security Control Provider  **EO Managed**  Customer Managed  *EIS Service Line*  *ETM Service Line* | |
| Implementation | EO information systems automatically *implements security safeguards* when integrity violations are discovered.  Tools employed by the organization include, but are not limited to:   * ISS Intrusion Prevention / Detection System – Utilized throughout the Enterprise by NSOC to identify/block/alert on network based attacks. * Nessus – Enterprise wide vulnerability identification, used to perform monthly scans of the enterprise in support of ongoing Vulnerability Identification and Remediation (VIAR) across the environment. * QRadar Log Manager – provides centralized logging of all systems. Utilization of centralized monitoring provides automated review and alerting of system activity across the enterprise. The scheduled collection of logs runs every 24 hrs. * Real Time Network Analyzer (RNA) – Utilized across the environment by NSOC to monitor, detect and alert on network activity to include anomalous network behavior and unexpected spikes in network traffic.   FireEye - FireEye Alerts can use heuristics to detail activity related to callback activity or Malware. VA-NSOC is notified for all callback activities which would indicate malware resident on a VA system. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### SI-7.E7 Software, Firmware, and Information Integrity E7: Integration of Detection and Response

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization incorporates the detection of unauthorized *[Assignment: organization-defined security-relevant changes to the information system]* into the organizational incident response capability. | H, M | |
| Security Control Provider  Customer Managed  *DCO Service Line* | |
| Implementation | EO incorporates the detection of unauthorized security-relevant changes to the information system into the organizational incident response capability by way of QRadar SEIM alerts by event threshold. Software and information integrity is controlled through a combination of user rights and Operating System permissions. User permissions are assigned according to the concept of least-privilege. A user is incapable of making changes to the system unless they are specifically authorized. Violation of the Rules of Behavior and unauthorized changes to information systems would constitute a security incident. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |
|  | |

### SI-7.E14 Software, Firmware, and Information Integrity E14: Binary or Machine Executable Code

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization:   1. Prohibits the use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code; and 2. Provides exceptions to the source code requirement only for compelling mission/operational requirements and with the approval of the authorizing official. | H | |
| Security Control Provider  Customer Managed  *DCO Service Line* | |
| Implementation | EO:   1. Prohibits the use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code; and   Does not provide exceptions to the source code requirement. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |
|  | |

### SI-8.E1 Spam Protection E1: Central Management

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The organization centrally manages spam protection mechanisms. | H, M | |
| Security Control Provider  Customer Managed  *DCO Service Line* | |
| Implementation | *This is a VA Agency-wide control for the facility that is provided by VA-NSOC (Spam and spyware control).*  VA-NSOC manages the IronPort™ spam protection devices at the ECSIP gateways. This is centrally managed. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### SI-8.E2 Spam Protection E2: Automatic Updates

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The information system automatically updates spam protection mechanisms. | H, M | |
| Security Control Provider  Customer Managed  *DCO Service Line* | |
| Implementation | *This is a VA Agency-wide control for the facility that is provided by VA-NSOC (Spam and spyware control).*  VA-NSOC automatically updates spam protection mechanisms. | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

### SI-16.1 Memory Protection

|  |  |  |  |
| --- | --- | --- | --- |
| Control | The information system implements *[Assignment: organization-defined security safeguards]* to protect its memory from unauthorized code execution. | H, M | |
| Security Control Provider  **EO Managed**  Customer Managed  *DCO Service Line*  *EIS Service Line*  *ETM Service Line* | |
| Implementation | EO/EIS information systems implement security safeguards to protect its memory from unauthorized code execution. This is primarily a function of the operating system (OS). | Implemented | x |
| Planned |  |
| Compensating |  |
| Not Implemented |  |
| Not Applicable |  |
| Risk Based Decision |  |
|  | |

# 