

**RISK MANAGEMENT FRAMEWORK FOR VA INFORMATION SYSTEMS – TIER 3:
VA INFORMATION SECURITY PROGRAM**

1. REASON FOR ISSUE: To provide the risk-based process for selecting the Department of Veterans Affairs (VA) system security controls and operational requirements for VA information technology systems per VA Directive 6500, *Managing Information Security Risk: VA Information Security Program* and to update the VA National Rules of Behavior. This policy is consistent with VA's information security statutes, 38 United States Code (U.S.C.) §§ 5721-5727, *Veteran's Benefits, Information Security*; the Federal Information Security Management Act of 2002, 44 U.S.C. §§ 3541-3549, *Coordination of Federal Information Policy, Information Security*; and Office of Management and Budget Circular A-130, Appendix III, *Security of Federal Automated Information Resources*.

2. SUMMARY OF CONTENTS/MAJOR CHANGES: This Handbook provides the risk-based process for selecting VA information technology system security controls and operational requirements to implement VA Directive 6500. The Handbook is based on National Institute of Standards and Technology Special Publication 800-53, Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations*, system security controls.

3. RESPONSIBLE OFFICE: The Office of the Assistant Secretary for Information and Technology (005), Information Security (005R), Cyber Security (005R2), is responsible for the content of this Handbook.

4. RELATED DIRECTIVE: VA Directive 6500, *Managing Information Security Risk: VA Information Security Program*.

5. RESCISSIONS: VA Handbook 6500, *Information Security Program*, September 18, 2007, and its Appendices. Note: This rescission does not include the other handbooks in the VA 6500 series.

CERTIFIED BY:

/s/
Roger W. Baker
Assistant Secretary for Information and
Technology

**BY DIRECTION OF THE SECRETARY
OF VETERANS AFFAIRS:**

/s/
Roger W. Baker
Assistant Secretary for Information and
Technology

Distribution: Electronic Only

**RISK MANAGEMENT FRAMEWORK FOR VA INFORMATION SYSTEMS – TIER 3
VA INFORMATION SECURITY PROGRAM**

CONTENTS

PARAGRAPH	PAGE
1. PURPOSE.....	5
2. SCOPE.....	5
3. BACKGROUND/OVERVIEW.....	6
4. INFORMATION SECURITY RESPONSIBILITIES.....	9
Assistant Secretary for Information and Technology	9
Assistant Secretary for Operations, Security, and Preparedness	9
Director, Personnel Security and Identity Management.....	9
Director for the Office of Security and Law Enforcement.....	10
Deputy Assistant Secretary for Human Resources Management.....	10
Deputy Assistant Secretary of Acquisition and Logistics	10
Deputy Assistant Secretary for IT Resource Management.....	10
Deputy Chief Information Officer for Architecture, Strategy, and Design	11
Deputy Chief Information Officer for Product Development.....	11
Deputy Chief Information Officer for Service Delivery and Engineering and Information System Owners	11
Deputy Assistant Secretary for Information Security	12
Executive Director for Quality, Performance, and Oversight.....	16
Information Owners/Stewards (VHA, VBA, and NCA)	16
Under Secretaries, Assistant Secretaries, and Other Key Officials	17
Program Directors/Facility Directors	18
Information Security Officers	18
Local Program Management	19
Local Chief Information Officers/System Administrators/Network Administrators/Database Managers.....	20
Contracting Officers/Contracting Officer Representatives	22
Local Human Resources Staff/Security and Law Enforcement Staff	22
Users of VA Information and Information Systems	22
5. SYSTEM DEVELOPMENT LIFE CYCLE AND ESTABLISHING SYSTEMS BOUNDARIES	22

**RISK MANAGEMENT FRAMEWORK FOR VA INFORMATION SYSTEMS - TIER 3
VA INFORMATION SECURITY PROGRAM**

CONTENTS, cont.

PARAGRAPH	PAGE
6. CATEGORIZATION OF SYSTEMS – RMF STEP 1	23
7. SELECTION OF SECURITY CONTROLS – RMF STEP 2.....	24
8. IMPLEMENT SECURITY CONTROLS – RMF STEP 3.....	29
9. ASSESS SECURITY CONTROLS – RMF STEP 4.....	29
10. AUTHORIZE INFORMATION SYSTEM – RMF STEP 5	30
11. MONITOR SECURITY CONTROLS – RMF STEP 6	30
 FIGURES	 PAGE
1. Risk Management Framework.....	8
2. RMF 2 – Selection Chart	25
3. Security Control Selection Process	F-4
 TABLES	 PAGE
1. Security Controls Baselines.....	F-5
 APPENDICES	 PAGE
A. Terms and Definitions	A-1
B. Acronyms and Abbreviations.....	B-1
C. References.....	C-1
D. VA National Rules of Behavior	D-1
E. Security Control Classes, Families, and Identifiers	E-1
F. VA System Security Controls	F-1
F.1. Common Controls	ATT-1.1
F.2. Hybrid Controls	ATT-2.1
F.3. System Specific Controls	ATT-3.1

RISK MANAGEMENT FRAMEWORK FOR VA INFORMATION SYSTEMS VA INFORMATION SECURITY PROGRAM

1. PURPOSE

a. This Handbook establishes the foundation for Department of Veterans Affairs (VA) comprehensive information security program and its practices, based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, and SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, that will protect the confidentiality, integrity, and availability of information created, processed, stored, aggregated, and transmitted by VA's information systems and business processes.

b. This Handbook provides the minimum mandatory security control standards for implementation of VA Directive 6500, *Managing Information Security Risk: VA Information Security Program*.

c. This Handbook also provides the criteria to assist management in making governance and integration decisions for VA's security programs.

d. This Handbook represents VA's information technology (IT) overarching security policy that is consistent, and in alignment, with NIST standards and guidelines and other related requirements set forth in Office of Management and Budget (OMB) memorandums and circulars.

2. SCOPE

a. The security requirements and controls in this Handbook apply to all VA IT systems, (also known as Tier 3 controls of VA's Risk Management Framework (RMF)). See VA Directive 6500 for information regarding Tier 1 and Tier 2 of VA's RMF.

b. The requirements in this Handbook and appendices also apply to VA or contractor-operated services and information resources located and operated at contract facilities or any other third party utilizing VA information or VA information systems in order to perform a VA authorized activity.

c. The Handbook's audience includes individuals involved in the planning, developing, purchasing, approving, monitoring, managing, maintaining and disposing of VA IT systems.

d. VA's National Rules of Behavior (ROB), Appendix D, provides the specific responsibilities and expected behavior for users of VA systems or VA sensitive information. Contractors are required to sign VA's Contractor ROB which provide the responsibilities and expected behavior of contractors that use VA systems or VA sensitive information. The Contractor ROB is located in VA Handbook 6500.6, *Contract Security*.

e. These security controls apply to all information resources used to carry out the VA mission. For example, the controls apply to desktop workstations, laptop computers, other portable devices, servers, network devices, and office automation equipment (such as copiers and fax machines with communication capabilities), operated by or on behalf of VA.

f. This Handbook applies to all information collected, transmitted, used, stored, or disposed of, by or on behalf of VA.

g. The Office of Information and Technology (OIT) develops, disseminates, and updates additional VA directives, VA handbooks, Standard Operating Procedures (SOP), memoranda, notices, and best practices, as required, to implement these policies, or institute additional requirements to maintain the information assurance program.

3. BACKGROUND/OVERVIEW

a. The Federal Information Security Management Act (FISMA) of 2002, 44 United States Code (U.S.C.) §§ 3541-3549, recognized the importance of information security to the economic and national security interests of the United States (U.S.). This legislation emphasized the need for all Federal agencies to develop, document, implement, and maintain an enterprise-wide program to provide an integrated security program to protect Federal information and information systems that support the Federal Government's mission. FISMA directed all Federal agencies to follow specific security guidance and implement specific requirements issued by NIST in its Federal Information Processing Standards (FIPS) and SP documents. Specifically, VA is required within its FISMA security program to implement FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems* and FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, to:

(1) Categorize VA information systems based on the sensitivity of the information, the mission criticality of the business process for which information systems provide support, and the levels of risk faced; and

(2) Use security requirements outlined in FIPS 200 and the current version of SP 800-53.

b. The RMF outlined in SP 800-37 and VA Directive 6500 provides VA a process for integrating required security controls into information systems as part of the system development life cycle (SDLC). Through performance of the risk management activities, included as part of the framework, the controls specified within this Handbook are integrated into information systems. The framework, as illustrated in Figure 1: Risk Management Framework below, requires that for each information system VA must:

(1) Categorize the information system;

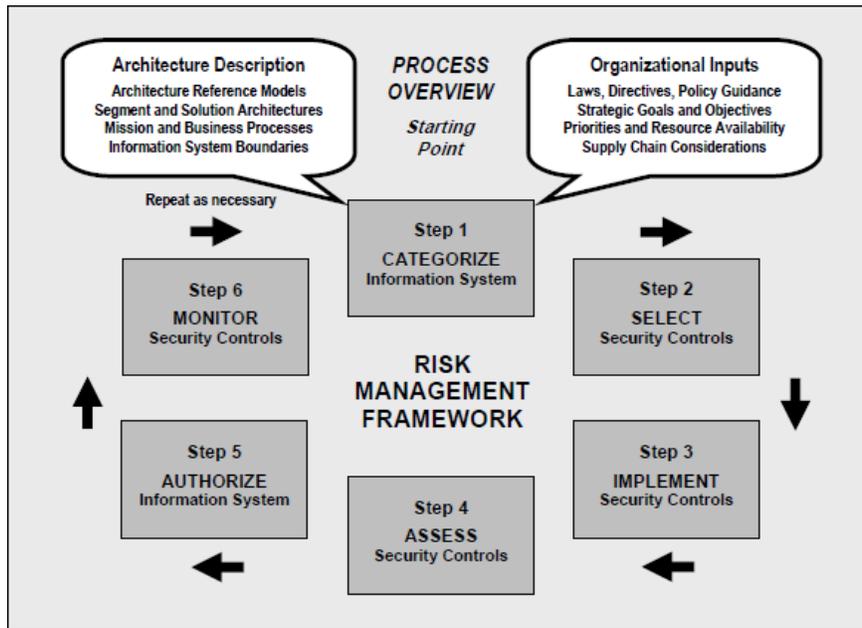
(2) Select the security controls;

(3) Implement the security controls;

- (4) Assess the security controls;
- (5) Authorize the information system; and
- (6) Monitor the security controls.

c. Additional information on each of the six risk framework steps listed above is covered in Sections 6-11 of this Handbook.

Figure 1: Risk Management Framework



The RMF, as illustrated in Figure 1 above, demonstrates the six steps required within the framework:

- Step 1: Categorize the information system
- Step 2: Select the security controls
- Step 3: Implement the security controls
- Step 4: Assess the security controls
- Step 5: Authorize the information system
- Step 6: Monitor the security controls

4. INFORMATION SECURITY RESPONSIBILITIES

a. VA Directive 6500 describes the responsibilities for VA senior officials, information owners, information system users, and the Office of Inspector General (OIG) for information security. Each subordinate VA directive and VA handbook issued by the Office of Cyber Security (OCS) will support the overall VA information security program and will include definitive roles and responsibilities for specific security control families that will require additional responsibilities to protect VA information and information systems.

b. Additional roles and responsibilities with significant information and information security responsibilities necessary for implementing VA's RMF include the following:

(1) **Assistant Secretary for Information and Technology.** The Assistant Secretary for Information and Technology, as the VA Chief Information Officer (CIO), is responsible for:

(a) Assuming the responsibility as the Authorizing Official (AO) to ensure that operating systems under OIT's area of responsibility operate at an acceptable level of risk;

(b) Designating a Chief Information Security Officer (CISO);

(c) Developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements;

(d) Overseeing personnel with significant responsibilities for information security and ensuring that the personnel are adequately trained;

(e) Assisting senior VA officials concerning their security responsibilities; and

(f) In coordination with other senior officials, reporting annually to the head of VA on the overall effectiveness of VA's information security program, including progress of remedial actions.

(2) **Assistant Secretary Operations, Security, and Preparedness.** The Assistant Secretary Operations, Security, and Preparedness is responsible for the:

(a) Director, Personnel Security and Identity Management - who is responsible for:

1. Processing background investigations (BI) as required for VA employees, contractors, and affiliates. The BIs are conducted at a level commensurate with the risk level designated for either the VA employee's position description and/or the contract statement of work (SOW)/task order, etc.;

2. Developing and implementing VA Directive and Handbook 0710, *Personnel Security and Suitability Program*;

3. Disseminating VA Directive and Handbook 0710 guidance to the field, as required; and

4. Disseminating Physical Access Control Systems (PACS) requirements and PACS Migration Plan for Personal Identity Verification (PIV) Compliance guidance and direction to the field security and law enforcement staff, as required.

(b) Director of the Office of Security and Law Enforcement – who is responsible for:

1. Conducting an annual physical security survey in accordance with VA Directive and Handbook 0730, *Security and Law Enforcement*; and

2. Establishing physical security standards and practices (VA Directive and Handbook 0730).

(3) **Deputy Assistant Secretary (DAS) for Human Resources Management** is responsible for:

(a) Providing guidance based on VA's Human Resources (HR) policy to field supervisors and managers regarding personnel actions or other actions to be taken when employees have violated information security practices, laws, regulations, policies, and VA National ROB; and

(b) Providing advice to field supervisors and managers regarding appropriate information security-related performance standards and position descriptions for employees who are authorized to access any information system(s).

(4) **DAS for Acquisition and Logistics** is responsible for:

(a) Providing acquisition policy/procedures to VA Contracting Officers (CO), Program Managers and CO Representatives (COR) to facilitate implementation of VA's information security program within the Department as outlined in VA Handbook 6500.6. This applies to all contracts in which VA sensitive information is stored, generated, transmitted, or exchanged by a VA contractor, subcontractor or a third party, acting on behalf of any of these entities;

(b) Ensuring policy/procedures require that the approved VA Acquisition Regulation security clause is included in all applicable contracts; and

(c) Ensuring policy/procedures require the CO to consult with the COR and the facility Information Security Officer (ISO) and Privacy Officer (PO), as necessary, to monitor contracts to ensure that all Federal and VA security and privacy requirements are being met per the contract.

(5) **DAS for IT Resource Management** is responsible for:

(a) Aggregating all capital planning and investment requests for the DAS for Information Security needed to implement the information security program and documents all exceptions to this requirement;

(b) Aggregating the business case/Exhibit 300/Exhibit 53 for the DAS for Information Security to record the resources required; and

(c) Ensuring that information security resources are available for the DAS for Information Security as planned and approved.

(6) **Deputy CIO for Architecture, Strategy, and Design** is responsible for ensuring that the information security requirements necessary to protect the organizational missions/business functions are adequately addressed in all aspects of enterprise architecture (EA) including reference models, segment and solution architectures, and the resulting information systems supporting those missions and business processes.

(7) **Deputy CIO for Product Development** is responsible for:

(a) Conducting information system security engineering activities; and

(b) Employing best practices when implementing security controls within an information system including software engineering methodologies, system/security engineering principles, secure design, secure architecture, and secure coding techniques.

(8) **Deputy CIO for Service Delivery and Engineering and Information System Owners** are responsible for the overall procurement, development, integration, modification, daily operations, maintenance, and disposal of VA information and information systems, including:

(a) Ensuring that each system is assigned a System Owner and that the System Owner is responsible for the security of the system;

(b) Ensuring that each system has developed a secure baseline of security controls by scoping, tailoring, compensating, and supplementing the controls as outlined in this Handbook;

(c) Ensuring that the secure baseline configuration outlined in (b) above is documented in the System Security Plan (SSP) and approved by the VA AO (CIO) or designee prior to implementation;

(d) Providing appropriate access to VA systems (including types of privileges or access);

(e) Ensuring compliance with Federal security regulations and VA security policies;

(f) Ensuring that the system is deployed and operated in accordance with the agreed-upon security controls;

(g) Ensuring the development and maintenance of SSPs and contingency plans in coordination with local information owners, the local system administrators, ISO, and functional "end user" for nationally deployed systems;

(h) Reviewing and updating the SSP as required by the Certification Program Office and when a significant change to the system occurs;

(i) Reviewing, updating and testing the system contingency plan as specified in the SSP and when a significant change to the system occurs;

- (j) Developing and maintaining an IT system Configuration, Change, and Release Management Plan;
 - (k) Ensuring that system users and support personnel receive required security training;
 - (l) Assisting the local system administrators in the identification, implementation, and assessment of security controls;
 - (m) Ensuring risk assessments are accomplished per the SSP, reviewed/updated, and when there is a major change to the system, reviewed and updated as required;
 - (n) Ensuring an authorization of the information system is completed prior to operational deployment and re-authorized as required, or whenever a major change occurs;
 - (o) Ensuring the remediation and updating of the plan of action and milestones (POA&M) identified during the authorization process and other reviews, conduct periodic compliance validation reviews, and complete the FISMA annual assessment to reduce or eliminate system vulnerabilities;
 - (p) Ensuring continuous monitoring activities are performed;
 - (q) Notifying the responsible VA ISO, PO, VA Network and Security Operations Center (NSOC) and the OIG as appropriate per VA Handbook 6500.2/1, *Management of Data Breaches Involving Sensitive Personal Information (SPI)*, of any suspected incidents immediately upon identifying that an incident has occurred and assisting in the investigation of incidents, as necessary;
 - (r) Ensuring compliance with the Enterprise and Security Architecture throughout the system life cycle;
 - (s) Conducting privacy impact assessments (PIA) with the assistance of the PO, as required; and
 - (t) Chartering, organizing, and maintaining VA's Patch and Vulnerability Team (PVT) and Program.
- (9) **DAS for Information Security**, created under the IT single authority by the VA CIO, is responsible for:
- (a) Serving as the CISO for VA;
 - (b) Carrying out the VA CIO security responsibilities under FISMA;
 - (c) Serving as primary liaison for the VA CIO (AO) to the Information System Owners and Information System Security Officers;

- (d) Advising the VA CIO in privacy-related matters;
- (e) Establishing, maintaining, and monitoring Department-wide information security policies, procedures, control techniques, training, and inspection requirements as elements of the Department information security program;
- (f) Approving all policies and procedures related to information security for those areas of responsibility currently under the management and oversight of other Department organizations;
- (g) Establishing the VA National and Contractor ROB for appropriate use and protection of VA information systems and VA sensitive information which are used to support Department missions and functions;
- (h) Managing and ensuring that the ISOs of the Department comply with VA cyber security directives and handbooks. The responsibilities of the ISOs are included in a separate section;
- (i) Providing oversight and guidance for VA compliance with applicable privacy and confidentiality laws, regulations, and policies, including the Privacy Act, 5 U.S.C. § 552a, and 38 U.S.C. §§ 5701, *Confidential Nature of Claims*, 5705, *Confidentiality of Medical Quality-Assurance Records*, and 7332, *Confidentiality of Certain Medical Records*;
- (j) Providing guidance and procedures for protecting information as required by 38 U.S.C. §§ 5721-28;
- (k) Coordinating with the Veterans Health Administration (VHA) to ensure reasonable privacy/security safeguards are in place as required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104-191, 110 Stat. 1936; the Health Information Technology for Economic and Clinical Health (HITECH) Act, Pub. L. 111-5, 123 Stat. 226, and their implementing regulations at 45 C.F.R. Parts 160 and 164, *HIPAA Privacy and Security Rules*;
- (l) Establishing VA requirements and providing guidance regarding the development, completion, and updating of PIA;
- (m) Ensuring that Privacy Awareness Training is provided and available for VA employees, contractors, volunteers, and interns;
- (n) Ensuring that VA privacy and information system security policies complement and support each other;
- (o) Directing that any incidents of failure to comply with established information security policies be immediately reported to the Assistant Secretary;
- (p) Reporting any compliance failure or policy violation directly to the appropriate Under Secretary, Assistant Secretary, or Other Key Officials of the Department for appropriate administrative or disciplinary action;

- (q) Requiring any Key Official of the Department who is notified to report to the Assistant Secretary on any action to be taken in response to compliance failure or policy violation identified by the Assistant Secretary;
- (r) Tracking and auditing of VA privacy complaints; Coordinating with Federal oversight agencies and VA management regarding privacy violations and their resolution, as required;
- (s) Submitting to the Secretary, at least once every quarter, a report on deficiencies of the Department or any Administration, office, or facility of the Department, in compliance with 44 U.S.C. §§ 3541-3549;
- (t) Reporting immediately to the Secretary on any significant deficiency in accordance with paragraph (t) above;
- (u) Evaluating, monitoring, and coordinating data breach quarterly reports. These data breach reports are provided to Congress by the Secretary of VA;
- (v) Providing central coordination and incident response functions for all security and privacy events impacting and affecting VA;
- (w) Coordinating incident response with outside agencies such as the United States Computer Emergency Readiness Team (US-CERT);
- (x) Establishing and maintaining a formal incident response capability;
- (y) Establishing and providing supervision over an effective incident reporting system;
- (z) Approving and managing all VA information and information systems incident response efforts based on VA-NSOC SOPs or as directed by the guidance of VA OIT or the US-CERT;
- (aa) Actively monitoring all VA network intrusion detection sensors, firewall alerts, network operations, and security logs for abnormal activity, attempted intrusions or compromises and other manners of security alerts that may be generated, and follow up as appropriate to minimize the impact of security incidents on VA information systems;
- (bb) Identifying, validating and managing all information and information system incidents (security and privacy) reporting and response efforts;
- (cc) Providing immediate notice to the VA Secretary of any presumptive data breach;
- (dd) Reporting all privacy related incidents to the US-CERT within one hour of discovery of event;
- (ee) Facilitating the information resolution core team, which is made up of all security entities in VA, to review, discuss and provide resolution in enterprise VA incidents;

(ff) Responding to incidents and events, which could cause an interruption to or reduction in the quality of risk management services, and identifying the root cause(s) of the incidents/events in order to mitigate the same or similar events from impacting service in the future;

(gg) Ensuring information security incidents are assigned a risk severity level rating;

(hh) Tracking the progress of event activity and performing all necessary documentation of incident progress;

(ii) Providing pertinent information on incidents to the appropriate organizations;

(jj) Working directly with the OIG to support activities involving information protection;

(kk) Generating situation reports, trending reports suitable for upper management review, final Incident Reports, and Lessons Learned briefings for major incidents as required by VA Handbook 6500.2/1;

(ll) Evaluating, monitoring, and assigning risk values, and developing impact assessments of the internal risk environment from an employee, information systems, internal control, and research and development perspective;

(mm) Working with other IT organizations to establish risk action plans and with stakeholders to implement;

(nn) Working with IT governance structure to incorporate management approval of risk acceptance;

(oo) Facilitating and providing risk tolerance measures and security awareness, participating in overall risk management, and providing mitigation techniques for efficiency, effectiveness, and continuous improvement;

(pp) Developing guidance and assisting in the identification, implementation, and maintenance of enterprise-wide information identity protection and risk assessment policies and procedures in coordination with stakeholders;

(qq) Executing initial and periodic information identity risk assessments and conducting related on-going compliance monitoring activities in coordination with other compliance and operational assessment functions;

(rr) Working closely with IT and other business units to develop program initiatives to meet the requirement to develop and maintain an enterprise business continuity program to ensure a state of readiness in the event of a disaster or business disruption;

(ss) Managing the planning, design, and maintenance of business continuity program projects and ensuring compliance with industry standards and regulatory requirements;

(tt) Managing, guiding, and directing business continuity preparedness through business centered teams; reviews team plans to ensure compliance; monitors plan development ; and evaluates plan changes and updates;

(uu) Providing business and technical guidance to senior and executive staff, subcontractors, business continuity team members, and enterprise staff relative to business continuity;

(vv) Managing and resolving all business continuity problems involving one or more IT or business units, systems or functions; and

(ww) Overseeing the process of defining business continuity problems and implementing solutions.

(10) **Executive Director for Quality, Performance and Oversight** in OIT is responsible for:

(a) Ensuring VA compliance with 44 U.S.C. §§ 3541-3549 and 38 U.S.C. §§ 5721-5728 and other related security, privacy, and record management requirements promulgated by NIST, OMB, and VA information and information security policies;

(b) Validating the remediation of POA&Ms identified in the VA approved FISMA database;

(c) Conducting a comprehensive assessment of the management, operational, and technical security controls employed within or inherited by an information system to determine the overall effectiveness of the controls (i.e., the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security requirements for the system);

(d) Ensuring VA systems that have undergone an assessment and authorization (A&A – formerly known as certification and accreditation (C&A)), are continuing to operate at their authorized level of risk; and

(e) Preparing the final security assessment report containing the results and findings from the assessment.

(11) **Information Owners (e.g., VHA, Veterans Benefits Administration (VBA), and National Cemetery Administration (NCA))** are VA officials with statutory, management, or operational authority for specified information and the responsibility for establishing the policies and procedures governing the organization's generation, collection, processing, dissemination, and disposal. In accordance with the criteria of the Centralized IT Management System, the information owners are also responsible for the following:

(a) Providing assistance to the Assistant Secretary for Information and Technology in identifying the security requirements and appropriate level of security controls for the information system or systems where sensitive personal information (SPI) is currently created, collected, processed, disseminated, stored, or subject to disposal;

(b) Determining who has access to the system or systems containing SPI, including types of privileges and access rights based upon expressed job duties; and

(c) Providing assistance to Administration and staff office personnel involved in the development of new systems regarding the appropriate level of security controls for their information.

(12) **Under Secretaries, Assistant Secretaries, and Other Key Officials** in accordance with 44 U.S.C. § 3544 and 38 U.S.C. §§ 5723(e), are responsible for the following:

(a) Implementing the policies, procedures, practices, and other countermeasures identified in the Department information security program that comprise of activities that are under their day-to-day operational control or supervision;

(b) Periodically testing and evaluating information security controls that comprise activities that are under their day-to-day operational control or supervision to ensure effective implementation;

(c) Providing POA&Ms to the Assistant Secretary for Information and Technology on at least a quarterly basis detailing the status of actions being taken to correct any security compliance failure or policy violation;

(d) Complying with the provisions of 44 U.S.C. §§ 3541-3549 and other related information security laws and requirements in accordance with orders of the Assistant Secretary for Information and Technology to execute the appropriate security controls commensurate to responding to a security bulletin of the VA-NSOC, with such orders to supersede and take priority over all operational tasks and assignments and be complied with immediately;

(e) Ensuring that all employees within their organizations take immediate action to comply with orders from the Assistant Secretary for Information and Technology to mitigate the impact of any potential security vulnerability, respond to a security incident, or implement the provisions of a bulletin or alert of the VA-NSOC and ensuring that organizational managers have all necessary authority and means to direct full compliance with such orders from the Assistant Secretary;

(f) Communicating this policy to all employees in their organizations and evaluating the security and privacy awareness activities of each organization in order to set clear expectations for compliance with security and privacy requirements and to ensure adequate resources;

(g) Developing mechanisms for communicating, on an ongoing basis, each workforce member's role and responsibilities specific to information security and privacy policies and practices that will enhance VA's security and privacy culture;

(h) Ensuring that all employees in their respective organizations sign the VA National ROB annually; and

(i) Ensuring that all employees in their respective organizations complete required security and privacy awareness training initially and annually thereafter. This also includes employees completing role-base training as required by their specific duties/responsibilities.

(13) **Program Directors/Facility Directors**, are responsible for:

(a) Providing the necessary support to the information security program in their organizations and ensuring that the facility meets all the information security requirements mandated by Executive and VA policy and other Federal requirements (e.g., FISMA, HIPAA);

(b) Ensuring a VA ISO and a VHA Health Care Security Requirements Compliance, Advisory, and Security Engineering Security Engineer (for VHA projects) are fully involved in all new projects concerning the development or acquisition of systems, equipment, or services including risk analysis, SSPs, request(s) for proposal, and other procurement documents that require security's participation;

(c) Ensuring that respective staff, with defined FISMA security roles, provides the ISO in a timely manner the information required to complete the quarterly FISMA reporting to OIT and OMB; and

(d) Ensuring all assigned POA&M corrective actions are completed by their respective staff.

(14) **ISOs** are the agency officials assigned responsibility by OIT Field Security Operations to ensure that the appropriate operational security posture is maintained for an information system or program. VA ISOs are responsible for:

(a) Ensuring compliance with Federal security requirements and VA security policies;

(b) Reviewing proposed SOWs for VA contracts to ensure that the resulting contracts sufficiently define information security requirements, as appropriate;

(c) Managing their local information security programs and serving as the principal security advisor to System Owners regarding security considerations in applications, systems, procurement or development, implementation, operation and maintenance, or disposal activities (i.e., SDLC management);

(d) Assisting in the determination of the appropriate security categorization of the IT system commensurate with the impact level;

(e) Coordinating, advising, and participating in the development and maintenance of information SSPs, system risk analysis, and contingency plans for systems within their area of responsibility;

(f) Verifying and validating, in conjunction with the System Owners and managers, that appropriate security measures are implemented and functioning as intended;

(g) Working with the System Owner and manager, according to the information systems at the site to ensure controls remain in place, operate correctly and produce the desired results. Controls most apt to change over time must be included and these tests and results must be documented to support the continuous monitoring program;

(h) Participating in security self-assessments, external and internal audits of system safeguards and program elements, and in A&A of the systems supporting the offices and facilities within their area of responsibility;

(i) Assisting other VA officials with significant information security responsibilities (i.e., system managers, contracting staff, HR staff, police) in remediating and updating the POA&Ms identified during the A&A process, periodic compliance validation reviews and the FISMA annual assessment reporting;

(j) Notifying the VA-NSOC of any suspected incidents within one hour of discovering an incident and assisting in the investigation of incidents, if necessary;

(k) Maintaining cooperative relationships with business partners or other interconnected systems;

(l) Monitoring compliance with the security awareness training requirements for each employee/contractor;

(m) Coordinating, monitoring, and conducting periodic reviews to ensure compliance with the VA National or Contractor ROB requirement for users of VA information systems or VA sensitive information;

(n) Serving as the liaison to the VA Training Manager to ensure security awareness training is provided within their area of responsibility;

(o) Coordinating with the facility PO for the assurance of reasonable safeguards as required by the Privacy Act, the HIPAA Privacy and Security Rules, and other Federal privacy statutes;

(p) Working with the facility PO to ensure information security and privacy procedures complement and support each other;

(q) Coordinate with OIT staff to add, change, suspend, or revoke access privileges according to the Director's guidance and concurrence when a system user under their oversight no longer requires access privileges or fails to comply with this policy; and

(r) Reviewing human subject research protocols (VHA ISOs) as outlined in VHA Directive 2007-040, *Appointment of Facility Information Security Officer and Privacy Officer to the Institutional Review Board (IRB) or the Research and Development (R&D) Committee*, and VHA Handbook 1200.05, *Requirements for the Protection of Human Subjects in Research*.

(15) **Local Program Management** must determine whether Federal employees and contractors require information system access in the accomplishment of the VA mission. Specifically, the managers and/or supervisors are responsible for:

(a) Ensuring that all users are adequately instructed, trained, and supervised on IT security and information protection issues;

(b) Ensuring their offices and staff are in compliance with Federal security regulations and VA security policies;

(c) Determining the Federal employee's or contractor's "need-to-know" before access is granted. Access to any VA information or information system must not be authorized for a Federal employee or contractor who does not have a need for access to the system in the normal performance of his/her official duties;

(d) Ensuring users under their oversight comply with this policy and pursue appropriate disciplinary action for noncompliance;

(e) Ensuring users of VA information systems or VA sensitive information under their oversight complete all security and privacy training requirements;

(f) Ensuring users of VA information systems or VA sensitive information under their supervision or oversight review and sign VA's National or Contractor ROB on an annual basis;

(g) Notifying system administrators and ISOs of new users per locally approved procedures;

(h) Notifying system managers and ISOs to revoke access privileges in a timely manner when a user under their supervision or oversight no longer requires access privileges or the user fails to comply with this policy;

(i) Participating in internal audits, as required, to ensure users have appropriate access;

(j) Authorizing remote access privileges for authorized users and reviewing remote access user security agreements on an annual basis, determined by the date of authorized agreement for remote access, at a minimum to verify the continuing need for access, and the appropriate level of privileges;

(k) Ensuring users report any suspected or potential incidents immediately upon discovery to management officials and ISOs and/or POs;

(l) Assisting other VA officials with significant information system responsibilities in the remediation and updating of the POA&M identified during the A&A process, periodic compliance validation reviews, and the FISMA annual assessment reporting to reduce or eliminate system vulnerabilities; and

(m) Notifying the responsible ISO of any suspected incidents immediately upon discovery and assisting in the investigation of incidents if necessary.

(16) Local CIOs/System Administrators/Network Administrators/Database Managers are responsible for day-to-day operations of the systems. The role of a system administrator must include security of local area network (LAN) or application administration and account administration. The system/network administrator is responsible for:

- (a) Ensuring compliance with Federal security requirements and VA security policies;
- (b) Assisting in the development and maintenance of SSPs and contingency plans for all systems within their area of responsibility;
- (c) Participating in risk assessments as outlined in the SSP;
- (d) Participating in self-assessments, external and internal audits of system safeguards and program elements, and in A&A of the system;
- (e) Evaluating proposed technical security controls to assure proper integration with other system operations;
- (f) Identifying requirements for resources needed to effectively implement technical security controls;
- (g) Ensuring the integrity in implementation and operational effectiveness of technical security controls by conducting technical control testing;
- (h) Developing system administration and operational procedures and manuals as directed by the System Owner;
- (i) Evaluating and developing procedures that assure proper integration of service continuity with other system operations;
- (j) Notifying the responsible ISO of any suspected incidents within one hour upon discovery and assisting in the investigation of incidents if necessary;
- (k) Reading and understanding all applicable training and awareness materials;
- (l) Providing information on users and/or the system in support of any reports or documents necessary for oversight and authorization;
- (m) Reading and understanding all applicable use policies or other ROB, including the VA National or Contractor ROB, regarding use or abuse of the Operating Unit's information system resources;
- (n) Understanding which systems, or parts of systems, for which they are directly responsible (e.g., network equipment, servers, LAN), the sensitivity of the information contained in these systems, and the appropriate measures to take to protect the information;
- (o) Periodically repeating selected test procedures from the system's security authorization to ensure the security controls continue to operate effectively at the proper levels of assurance per NIST guidance and over the life cycle of the system; and
- (p) Assisting other VA officials with significant IT responsibilities in the remediation and updating the POA&Ms identified during the A&A process, periodic compliance validation reviews and the FISMA annual assessment reporting to reduce or eliminate system vulnerabilities.

(17) **CO/COR** are responsible for:

- (a) Ensuring that security requirements and security specifications are explicitly included in VA contracts, as appropriate;
- (b) Working with the ISO and PO to ensure that contracts contain the required security clause and security language necessary for compliance with FISMA and 38 U.S.C. §§ 5721-28 and to provide adequate security for information and information systems used by the contractor, including the requirement for signing VA Contractor ROB, when applicable;
- (c) Ensuring contractors meet the appropriate BI requirements in accordance with VA Directive and Handbook 0710;
- (d) Ensuring contractors complete VA's security/privacy awareness training and any additional role-based training, as outlined in the contract;
- (e) Monitoring the contract to ensure that security requirements are being met, consulting the ISO and/or PO as necessary; and
- (f) Assisting other VA officials with significant IT responsibilities in the remediation and updating the POA&Ms identified during the A&A process of a contractor's system when required, including periodic compliance validation reviews and the FISMA annual assessment reporting to reduce or eliminate system vulnerabilities.

(18) **Local HR Staff/Security and Law Enforcement Staff** are responsible for implementing specific security role based functions and are responsible for the following:

- (a) Complying with all Department information security program policies, procedures, and practices that pertain to their specific positions; and
- (b) Assisting other VA officials with significant IT responsibilities in the remediation and updating the POA&Ms identified during the A&A process, periodic compliance validation reviews, and the FISMA annual assessment reporting to reduce or eliminate system vulnerabilities.

(19) **Users of VA Information Systems or VA Sensitive Information** – In reference to the security requirements outlined in this Handbook, the responsibilities for general users (end users) have been extracted from this Handbook and are included in Appendix D, VA National ROB. VA contractors are responsible for complying with the VA Contractor ROB. The VA Contractor ROB is located in VA Handbook 6500.6.

5. SYSTEM DEVELOPMENT LIFE CYCLE AND ESTABLISHING SYSTEMS BOUNDARIES

a. VA will follow NIST's RMF in developing, operating, modifying, and removing systems. Procedures in this Handbook and other related OIT handbooks will be followed.

b. All VA systems are in a phase of the SDLC. Processes outlined in VA Handbook 6500.5, *Incorporating Security and Privacy in System Development Life Cycle*, will be followed.

c. The first step in VA's RMF is to establish the information system's boundaries. Information system boundaries are established in coordination with the security categorization process and before the deployment of SSPs.

d. Information resources (information and related resources including personnel, equipment, funds, and IT) allocated to an information system defines the boundary for that system.

e. In determining a system's boundaries the resources are generally:

(1) Under the same direct management control;

(2) Support the same mission/business objectives or functions and essentially the same operating characteristics and information security requirements; and

(3) Reside in the same general operating environment (or in the case of a distributed information system, reside in various locations with similar operating environments).

f. System boundaries should be revisited periodically as part of the continuous monitoring process carried out by VA.

g. Information System Owners will consult with the AO or designee, the local CIO and ISO when establishing or changing system boundaries. Additional guidance regarding the determination of system boundaries is outlined in SP 800-37 and should be used if there are questions regarding a system's boundary.

6. CATEGORIZATION OF SYSTEMS - RMF STEP 1

a. VA requires, per FIPS 199, System Owners (in coordination with information data owners and the ISO) to categorize their information systems as low-, moderate-, or high-impact for the security objectives of confidentiality, integrity, and availability. The potential impact values assigned to the respective security objectives are the highest values (i.e., high water mark) from among the security categories that have been determined for each type of information processed, stored, or transmitted by those information systems. The generalized format for expressing the security category of an information system is:

Security Category information system = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)}, where the acceptable values for potential impact are low, moderate, or high.

b. Since the potential impact values for confidentiality, integrity, and availability may not always be the same for a particular information system, the high water mark concept introduced in FIPS 200 to determine the impact level of the information system for the express purpose of selecting an initial set of security controls from one of the three security controls baselines will be used.

c. To determine the overall impact level of the information system:

(1) Determine the different types of information that are processed, stored, or transmitted by the information system. SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories : (2 Volumes) – Volume 1: Guide Volume 2: Appendices*, provides guidance on a variety of information types;

(2) Use the impact levels in FIPS 199, and the recommendations of SP 800-60, to categorize the confidentiality, integrity, and availability of each information type;

(3) Determine the information system security categorization, that is, the highest impact level for each security objective (i.e., confidentiality, integrity, and availability) from among the categorizations for the information types associated with the information system; and

(4) Determine the overall impact level of the information system from the highest impact level among the three security objectives in the system security categorization.

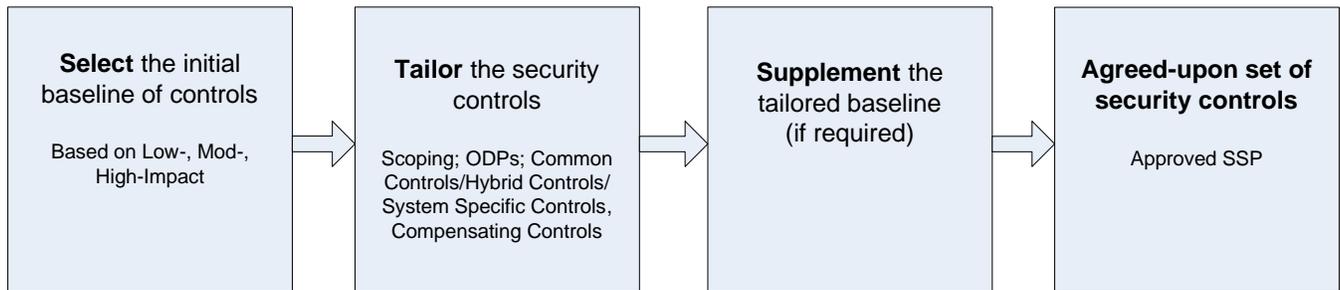
d. Document the security categorization in the SSP.

e. Describe the information system (including system boundary) and document the description in the SSP.

f. Register the information system in VA's Office for Information Security approved system database – currently called Security Management and Reporting Tool.

7. SELECTION OF SECURITY CONTROLS - RMF STEP 2

a. When system categorization has been performed by determining the impact level, VA's RMF continues with (1) selecting the initial baseline of security controls, (2) tailoring, and (3) supplementing the baseline controls, as outlined below in Figure 2: RMF 2 – Selection Chart, according to the current version of SP 800-53, and VA Handbook 6500, Appendix F:

Figure 2 - RMF 2 – Selection Chart

The Selection of Security Controls process, as illustrated in Figure 2 above, demonstrates the process and result of selecting security controls:

Step 1: Select the initial baseline of controls (Based on low-, moderate-, high-impact)

Step 2: Tailor the security controls (Scoping, Organizationally Defined Parameters (ODP), Common Controls/Hybrid Controls/System Specific Controls, and Compensating Controls)

Step 3: Supplement the tailored baseline (if required)

Step 4: The result will be an agreed-upon set of security controls (Approved SSP)

(1) **Selecting the Initial Baseline of Security Controls:** The selection of a set of baseline controls is based on the impact level of the information as determined by the security categorization process. System owners select one of three sets of baseline security controls from VA Handbook 6500, Appendix F, corresponding to the low-, moderate-, or high-impact rating of the information system. (For easy reference, NIST maintains an Annex of the controls required for each system categorization on their Web site). VA Handbook 6500, Appendix E, contains a table of NIST's Security Control Classes, Families and Identifiers that are used by VA to secure VA's information and information systems. The class identifiers of management, operational, and technical are also used by NIST and have the following definitions:

(a) Management controls – the security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.

(b) Operational controls – the security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems).

(c) Technical controls – the security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

(2) **Tailoring the Security Controls:** Prior to implementation of the selected set of baseline security controls the controls must be tailored to align with the specific operating conditions of the information system with the purpose of achieving a cost-effective and risk-based approach to providing information security. All tailoring decisions, including the specific rationale for the decisions, must be documented in the SSP for a VA system. The tailoring process consists of scoping, compensating controls, and ODPs.

(a) Scoping Guidance: Application of scoping considerations to the initial baseline of security controls helps VA to implement only those controls which are essential for protection of the specific mission requirements and operating environments of the information system.

1. *Common Control-related considerations:* Security controls designated as common controls within VA serve the protection needs of the entire VA, and must have management responsibility assigned at an organizational level by the appropriate group and officials instead of the System Owner. This centralized management is instrumental in creating cost-effective security protection. Common controls are designed to be "inherited" by information systems and can be designated as a combination of common and system specific controls, known as a hybrid control.

2. *Security Objective-related considerations:* Security controls that uniquely support the confidentiality, integrity, or availability objectives may be downgraded (or modified or eliminated) if and only if, the downgrading action:

- a. Is consistent with the FIPS 199 security categorization for the corresponding security objectives of confidentiality, integrity, or availability before moving to the high water mark;
- b. Is supported by an assessment of risk; and
- c. Does not affect the security-relevant information within the information system.

(Further guidance is available in the current version of SP 800-53, including a list of recommended candidates for downgrading.)

3. *System Component Allocation-related considerations:* Security controls apply only to the components of the system that provide or support the security capability addressed by the control and are sources of potential risk being mitigated by the control. The VA inventory of components is assessed to determine which controls apply to various components and make decisions regarding where to allocate controls in order to satisfy VA security requirements.

4. *Technology-related considerations:* Security controls that refer to specific technologies (e.g., wireless, cryptography, public key infrastructure (PKI)) apply only where the technology is used or required to be used. Security control support by automated mechanism is only required where they are available and feasible.

5. *Physical Infrastructure-related considerations:* Security controls that refer to facilities (e.g., physical controls such as locks and guards, environmental controls for temperature, humidity, lighting, fire, and power) are applicable only to those parts of the facilities that are directly related to the system and its assets.

6. *Policy/Regulatory-related considerations:* Security controls related to laws, policies, standards, or regulations (e.g., threshold analysis, PIAs) are required only if they are consistent with the types of information and information systems covered by the applicable laws, policies, standards, or regulations.

7. *Operational/Environmental-related considerations:* Controls that depend upon the nature of the operational environment only apply if the system is operating in such an environment.

8. *Scalability-related considerations:* Controls are scalable with regard to the extent and rigor of the implementation. Scalability is guided by impact level. Scaling controls helps control costs while achieving sufficient risk mitigation and adequate security.

9. *Public Access-related considerations:* Some controls (e.g., identification and authentication, personnel security controls) may not apply to users accessing systems through public interfaces.

(b) Compensating Security Controls: After applying the scoping considerations, if the System Owner is unable to implement a security control or the control is not a cost-effective means of risk mitigation, a compensating control(s) or control enhancement(s) may be employed in lieu of the normal baseline control described in SP 800-53. The compensating control must be designed to provide an equivalent or comparable level of protection to the information and information system to that of the original control. Compensating controls may be employed only under the following conditions:

1. It is selected from SP 800-53 or a suitable control is adopted (priority is always given to existing SP 800-53 controls); and

2. A rationale is supplied and documented in the SSP that explains why the baseline control could not be used and how the compensating control provides equivalent protection. The System Owner accepts any residual risk from the use of selected compensating controls.

(c) Organizationally-Defined Security Control Parameters: ODPs are portions of security controls containing VA management-defined parameters. ODP values are generally determined after applying scoping guidance and selecting compensating controls and allow the System Owner the flexibility to support specific operating environment requirements or objectives. VA's ODPs are specified in VA Handbook 6500, Appendix F. Suggested minimum control values are specified for system specific and hybrid controls; however, System Owners should tailor the ODPs to align with the specific operating conditions of the information system as described above and document the ODPs and the rationale for determining the ODP values in the SSP. Values for ODPs may be superseded by more restrictive values prescribed by applicable Federal laws, Executive Orders, policies, standards, guidelines, or regulations.

(3) **Supplementing the Tailored Baseline:**

a. Using the tailored baseline as a foundation, additional controls or enhancements may be needed to address specific threats and vulnerabilities. The determination of a set of controls that provide adequate security is a function of assessment of risk and what is required to mitigate the risk. If the sufficiency of the tailored security controls is not adequate, additional security controls or control enhancements will be needed and can be added to the baseline under the following conditions:

(1) Use existing baseline controls and enhancements first (note that some controls and enhancements are found only in higher-impact baselines or are not included in any baseline);

(2) Restrictions can provide an alternate method to reduce or mitigate risk; and

(3) Documenting these decisions and the rationale involved in the SSP is essential and imperative for the authorization process.

b. SP 800-53 security controls are contained in VA Handbook 6500, Appendix F. System Owners must use VA Handbook 6500, Appendix F for selecting the security controls for their systems.

c. Additional security control enhancements, if required, can be found in the current version of SP 800-53.

d. Control enhancements or security functionality specific to the information system may also be governed by additional regulations, requirements, standards, and policies not adequately addressed by SP 800-53 or Appendix F of this Handbook.

e. The SSP containing the security controls that have been tailored, compensated, and supplemented, as required, is reviewed and approved by the VA AO (CIO) or designee.

f. Any subsequent changes, modifications, and updating controls to the approved security plan will be reviewed and approved by the VA AO (CIO) or designee.

8. IMPLEMENT SECURITY CONTROLS - RMF STEP 3

a. System Owners will implement and test the security controls specified in the approved SSP.

b. System Owners will implement the VA approved US Government Configuration Baseline (USGCB) controls formerly known as the Federal Desktop Core Configuration.

9. ASSESS SECURITY CONTROLS – RMF STEP 4

a. OIT will develop, review, and approve a plan to assess the security controls.

b. The security assessment plan provides a detailed roadmap of how to conduct an assessment and associated procedures.

c. The assessment plan reflects the type of assessment OIT is conducting (e.g., developmental testing and evaluation, independent verification and validation, assessments supporting security authorizations or reauthorizations, audits, continuous monitoring, assessments subsequent to remediation actions).

d. OIT will assess the security controls in accordance with the assessment procedures defined in the security assessment plan.

e. System Owners will ensure that assessors have access to the information system and environment of operation where the security controls are employed and the appropriate documentation, records, artifacts, test results, and other materials needed to assess the security controls.

f. The security assessment report documents the issues, findings, and recommendations.

g. System Owners will conduct initial remediation actions on security controls based on the findings and recommendations of the security assessment report and reassess remediated controls, as appropriate.

10. AUTHORIZE INFORMATION SYSTEM – RMF STEP 5

a. The System Owner or designee will prepare the POA&M based on the findings and recommendations of various security assessment reports excluding any remediation actions taken.

b. The POA&M is a key document/process in the security authorization package. A POA&M describes the specific tasks that are planned to correct any weaknesses or deficiencies in the security controls noted during the assessment and address the residual vulnerabilities in the information system.

c. The System Owner assembles the security authorization package and submits the package to the AO for adjudication.

d. The AO or designee will determine the risk to VA operations (including mission, functions, image, or reputation) and assets, individuals, and other organizations.

e. The AO or designee will determine if the risk to VA's operations and assets, individuals, and other organizations is acceptable.

f. If the risks are acceptable, the AO will authorize the system for use in VA.

11. MONITOR SECURITY CONTROLS – RMF STEP 6

a. The information System Owner determines the security impact of proposed or actual changes to the information system and its environment of operation.

b. The information System Owner will adhere to VA Directive 6004, *Configuration, Change, and Release Management Programs*.

c. OIT will develop a process to assess a select subset of the technical, management, and operational security controls employed within and inherited by the information system in accordance with a VA's defined monitoring strategy.

d. Security control assessments (SCA) in support of initial and subsequent security authorizations are conducted by independent assessors. Assessor independence during continuous monitoring, although not mandated, introduces efficiencies into the process and allows for reuse of assessment results when reauthorization is required.

e. The information System Owner conducts remediation actions based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in the POA&M.

f. The information System Owner updates the SSP, security assessment report, and POA&M based on the results of the continuous monitoring process.

- g. The information System Owner reports the security status of the information system (including the effectiveness of security controls employed within and inherited by the system) to the AO and other appropriate VA officials on an ongoing basis, in accordance with VA's monitoring strategy.
- h. The AO reviews the reported security status of VA's information systems on an ongoing basis in accordance with the monitoring strategy to determine whether the risk to VA's operations and assets, individuals, and other organizations remains acceptable.
- i. The information System Owner follows VA Handbook 6500.1, *Electronic Media Sanitization*, requirements when a system is removed from service.

TERMS AND DEFINITIONS

- 1. Application:** A software program hosted by an information system. SOURCE: SP 800-137
 - 2. Assessment and Authorization (A&A):** The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. SOURCE: SP 800-37 [VA Adapted]
 - 3. Authentication:** Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. SOURCE: SP 800-53; SP 800-53A; SP 800-27A; FIPS 200
 - 4. Authorizing Official (AO):** Senior (Federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. SOURCE: SP 800-53; SP 800-53A; SP 800-37. In VA, this is the VA CIO.
 - 5. Availability:** Ensuring timely and reliable access to and use of information. SOURCE: 38 U.S.C. § 5727
 - 6. Business Associate:** For the purposes of this Handbook, a Business Associate is defined as an entity, including any individual, company, or organization that, on behalf of VHA, performs or assists in the performance of functions or activities involving the use or disclosure of protected health information (PHI), or that provides certain services to or for VHA involving the disclosure of PHI by VHA. SOURCE: 45 C.F.R. § 160.103 VHA Handbook 1600.01
 - 7. Common Security Control:** Security control that is inherited by one or more organizational information systems. SOURCE: SP 800-53
- These controls affect all VA facilities and systems with operations at the local site(s).
- 8. Compensating Security Controls:** The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the baselines described in SP 800-53 and the Committee on National Security Systems (CNSS) Instruction 1253, that provide equivalent or comparable protection for an information system. SOURCE: SP 800-53.
 - 9. Confidentiality:** Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. SOURCE: 38 U.S.C. § 5727

10. Continuity of Operations Plan (COOP): A COOP provides guidance on the system restoration for emergencies, disasters, mobilization, and for maintaining a state of readiness to provide the necessary level of information processing support commensurate with the mission requirements/priorities identified by the respective functional proponent. The Federal government and its supporting agencies traditionally use this term to describe activities otherwise known as disaster recovery, business continuity, business resumption, or contingency planning. SOURCE: VA Handbook 6500.8

11. Covered Entity: A covered entity is an organization or individual that is covered by the compliance requirements of HIPAA and is: (a) a health care provider who transmits any health information in electronic form; (b) a health care clearinghouse; or (c) a health insurance plan. SOURCE: 45 Code of Federal Regulations (CFR) §160.103

12. Data Breach: The loss, theft, or other unauthorized access, other than those incidental to the scope of employment, to data containing SPI, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. SOURCE: 38 U.S.C. § 5727.

May or may not be a breach under the HITECH Act, which defines “breach” as “the unauthorized acquisition, access, use, or disclosure of PHI in violation of the HIPAA Privacy Rule which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.” Under HITECH, breach of PHI excludes:

a. Any unintentional acquisition, access, or use of PHI by an employee or individual acting under the authority of a covered entity or business associate if such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship with the covered entity or business associate and does not result in further use or disclosure.

b. Any inadvertent disclosure from an individual who is otherwise authorized to access PHI at a facility operated by a covered entity or business associate to another similarly situated individual at same facility.

c. Any such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person. SOURCE: 45 C.F.R. § 164.402.

13. Denial of Service (DoS): An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources. SOURCE: SP 800-61

For example, an attacker sends specially crafted packets to a Web server, causing it to crash; an attacker directs hundreds of external compromised workstations to send as many Internet Control Message Protocol requests as possible to the organization’s network.

14. Encryption: The process of changing plaintext into ciphertext for the purpose of security or privacy. SOURCE: SP 800-57

15. External Information Systems (formerly known as Other Equipment): An information system or component of an information system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness. SOURCE: SP 800-53

16. Firewall: A device or program that controls the flow of network traffic between networks or hosts that employ differing security postures. SOURCE: SP 800-41

17. High-Impact System: An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high. SOURCE: SP 800-37; SP 800-53; SP 800-60; FIPS 200

18. Hybrid Security Control: A security control that is implemented in an information system in part as a common control and in part as a system-specific control. SOURCE: SP 800-37; SP 800-53; SP 800-53A; CNSSI-4009

19. Incident: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. SOURCE: FIPS 200; SP 800-53

The term incident means security incident as defined in 38 U.S.C. § 5727.

20. Individually Identifiable Health Information: “Individually identifiable health information” is information, including demographic data, that (a) relates to an individual’s past, present or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual, and (b) identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number). SOURCE: 45 C.F.R. § 160.103.

21. Information Owner: An agency official with statutory or operational authority for specified information and responsibility for establishing the control criteria for its creation, collection, processing, dissemination, and disposal which responsibilities may extend to interconnected systems or groups of interconnected systems. SOURCE: 38 U.S.C. § 5727

22. Information Resources: Information in any medium or form and its related resources, such as personnel, equipment, funds, and IT. SOURCE: 38 U.S.C. § 5727

23. Information Security: A means for protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability. SOURCE: 38 U.S.C. § 5727

24. Information Security Program Plan: Formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements. SOURCE: SP 800-37; SP 800-53; SP 800-53A

25. Information Security Officer (ISO): Individual working with the senior agency ISO, AO, or information system owner to help ensure the appropriate operational security posture is maintained for an information system or program. SOURCE: CNSSI-4009 [VA Adapted]

26. Information Security Requirements: Information security requirements promulgated in accordance with law, or directed by the Secretary of Commerce, NIST, and OMB, and, as to national security systems, the President. SOURCE: 38 U.S.C. § 5727

27. Information System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, whether automated or manual. SOURCE: 38 U.S.C. § 5727

28. Information System Owner: Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. SOURCE: FIPS 200

29. Information Technology (IT): Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. Includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. SOURCE: SP 800-53; SP 800-53A

30. Information Type: A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management), defined by an organization or in some instances, by a specific law, Executive Orders, directive, policy or regulation. SOURCE: SP 800-53; SP 800-53A; SP 800-37; SP 800-18; SP 800-60; FIPS 200; FIPS 199; CNSSI-4009; 40 U.S.C. § 11101 and § 1401

31. Integrity: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. SOURCE: 38 U.S.C. § 5727

32. Interconnection Security Agreement (ISA): An agreement established between the organizations that own and operate connected IT systems to document the technical requirements of the interconnection. The ISA also supports a Memorandum of Understanding or Agreement (MOU/A) between the organizations. SOURCE: SP 800-47

33. Local Area Network (LAN): A datacomm system allowing a number of independent devices to communicate directly with each other, within a moderately sized geographic area over a physical communications channel of moderate rates. SOURCE: FIPS 191

34. Low-Impact System: An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low. SOURCE: SP 800-37; SP 800-53; SP 800-60; FIPS 200

35. Malicious Code: A virus, worm, Trojan horse, or other code-based malicious entity that infects a host, also called “malware.” SOURCE: SP 800-61

36. Management Controls: The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security. SOURCE: SP 800-37; SP 800-53; SP 800-53A; FIPS 200

37. Media: Physical devices or writing surfaces including, but not limited to magnetic tapes, optical disks; magnetic disks; Large-Scale Integration memory chips; and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system. SOURCE: FIPS 200; SP 800-53; CNSSI-4009

38. Memorandum of Understanding/Agreement (MOU/A): A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. In this Handbook, an MOU/A defines the responsibilities of two or more organizations in establishing, operating, and securing a system interconnection. SOURCE: SP 800-47

39. Mobile Device: Portable cartridge/disk-based, removable storage media (e.g., floppy disks, compact discs (CD), universal serial bus (USB) flash drives, external hard drives, and other flash memory cards/drives that contain non-volatile memory). Portable computing and communications device with information storage capability (e.g., notebook/laptop computers, personal digital assistants (PDA), cellular telephones, digital cameras, and audio recording devices). SOURCE: SP 800-53

40. Moderate-Impact System: An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate and no security objective is assigned a FIPS 199 potential impact value of high. SOURCE: SP 800-53; SP 800-60; SP 800-37; FIPS 200

41. Operating Unit: An Operating Unit consists of any and all individuals responsible for the management, operation, maintenance, and security of VA’s information and information systems within their area of responsibility. Examples of individuals who are part of the

Operating Unit include, but are not limited to, Directors, Program Managers, Information and Technology staff (system managers, system administrators, and ISOs). SOURCE: VA Handbook 6500, Information Security Program (September 18, 2007)

42. Operational Controls: The security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems). SOURCE: SP 800-53; SP 800-37; FIPS 200

43. Personally Identifiable Information (PII): Any information which can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, biometric records, etc., alone, or when combined with other personal or identifying information that is linked to a specific individual, such as date and place of birth, mother's maiden name, etc. (See Sensitive Personal Information, below) SOURCE: VA Handbook 6500.2/1

44. Plan of Action and Milestones (POA&M): A plan used as a basis for the quarterly reporting requirements of OMB that includes the following information: (i) A description of the security weakness; (ii) the identity of the office or organization responsible for resolving the weakness; (iii) an estimate of resources required to resolve the weakness by fiscal year; (iv) the scheduled completion date; (v) key milestones with estimated completion dates; (vi) any changes to the original key milestone date; (vii) the source that identified the weakness; (viii) the status of efforts to correct the weakness. SOURCE: 38 U.S.C. § 5727

POA&M is a key document in the security authorization package and is subject to Federal reporting requirements established by OMB.

45. Potential Impact: The loss of confidentiality, integrity, or availability could be expected to have: (i) a limited adverse effect (FIPS 199 low); (ii) a serious adverse effect (FIPS 199 moderate); or (iii) a severe or catastrophic adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals. SOURCE: SP 800-53; SP 800-60; SP 800-37; FIPS 199

46. Privacy Event: A Privacy Event is a confirmed instance in which information protected by HIPAA; the Privacy Act of 1974; or other confidentiality statutes such as 38 U.S.C. §§ 5701, 5705, or 7332 may have been improperly disclosed, and includes the loss, theft, or any other unauthorized access, or any other access than that which is incidental to the scope of employment, to data containing SPI in electronic, printed, or any other format, and results in the potential compromise of the confidentiality or integrity of the data regardless of the manner in which the breach might have occurred. SOURCE: VA Directive 6509

47. Privacy Impact Assessment (PIA): An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. SOURCE: 44 U.S.C. § 3541-3549; SP 800-53; SP 800-18; SP 800-122; CNSSI-4009; OMB Memorandum 03-22

48. Privacy Officer (PO): The PO is responsible for taking proactive measures to help ensure that PII collected by VA is limited to that which is legally authorized and necessary; and is maintained in a manner that precludes unwarranted intrusions upon individual privacy; thereby minimizing privacy events. Additionally, it is the defensive duty of a PO to assist in mitigating damage when PII is compromised. SOURCE: VA Directive 6509

49. Privileged Account: An information system account with authorizations of a privileged user. SOURCE: SP 800-53

50. Privileged Command: A human-initiated command executed on an information system involving the control, monitoring, or administration of the system including security functions and associated security-relevant information. SOURCE: SP 8000-53

51. Privileged User: A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. SOURCE: SP 800-53; CNSSI-4009

This is synonymous with VA's "Users with elevated privileges" terminology used in the handbook.

52. Protected Health Information (PHI): Individually identifiable health information held by a covered entity or by a business associate acting on its behalf. PHI excludes education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. § 1232g, records described at 20 U.S.C. §§ 1232g(a)(4)(B)(iv), and employment records held by a covered entity in its role as employer. Within VA, VHA is the only covered entity. Certain other VA components, such as OIT, are business associates of VHA. SOURCE: 45 CFR § 160.103

53. Public Key Infrastructure (PKI): An architecture which is used to bind public keys to entities, enable other entities to verify public key bindings, revoke such bindings, and provide other services critical to managing public keys. SOURCE: FIPS 196

54. Remote Access: Access by users (or information systems) communicating externally to an information system security perimeter. SOURCE: SP 800-18

Remote access uses telecommunications to enable authorized access to non-public VA computing services that would otherwise be inaccessible from work locations outside a VA LAN or VA-controlled wide area network (WAN) computing environment. Remote Access includes access to non-public VA Information Systems and data that are exposed to the public Internet (e.g., web access to electronic mail (e-mail) by the home user or business traveler) as well as modem-dial-up and/or Virtual Private Network (VPN) access to internal VA IT servers and desktop workstations.

55. Risk: The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. SOURCE: SP 800-60

56. Risk Assessment: Process of identifying risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other operations, and the Nation, arising through the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place. SOURCE: SP 800-53; SP 800-53A; SP 800-37

57. Risk Management: The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment techniques and procedures for the continuous monitoring of the security state of the information system. SOURCE: SP 800-53; SP 800-53A; SP 800-37

58. Sanitization: Process to remove information from media so that information recovery is not possible. It includes removing all labels, markings and activity logs. SOURCE: FIPS 200

59. Security Categorization: The process of determining the security category for information or information system. SOURCE: SP 800-53

60. Security Control Assessment (SCA): The testing and/or evaluation of the management, operational, and technical security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system and/or enterprise. SOURCE: CNSSI-4009

61. Security Controls: The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. SOURCE: SP 800-53; SP 800-37; SP 800-53A; SP 800-60; FIPS 200; FIPS 199; CNSSI-4009

62. Security Controls Baseline: The set of minimum security controls defined for a low-, moderate-, or high-impact information system. SOURCE: CNSSI-4009

63. Sensitive Personal Information (SPI): The term, with respect to an individual, means any information about the individual maintained by VA, including the following: (i) education, financial transactions, medical history, and criminal or employment history; (ii) information that can be used to distinguish or trace the individual's identity, including name, social security number, date and place of birth, mother's maiden name, or biometric records. SOURCE: 38 U.S.C. § 5727

64. System Development Life Cycle (SDLC): The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal. SOURCE: CNSSI-4009

65. System Security Plan (SSP): Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. SOURCE: SP 800-37; SP 800-53; SP 800-53A; SP 800-18; FIPS 200

66. System Specific Security Control: A security control for an information system that has not been designated as a common security control or the portion of a hybrid control that is to be implemented within an information system. SOURCE: SP 800-37; SP 800-53; SP 800-53A; CNSSI-4009

67. Tailoring: The process by which a security controls baseline is modified based on: (i) the application of scoping guidance; (ii) the specification of compensating security controls, if needed; and (iii) the specification of ODPs in the security controls via explicit assignment and selection statements. SOURCE: SP 800-37; SP 800-53; SP 800-53A; CNSSI-4009

68. Technical Controls: The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. SOURCE: SP 800-53; SP 800-53A; SP 800-37; FIPS 200

69. Threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or DoS. SOURCE: SP 800-53; SP 800-53A; SP 800-27; SP 800-60; SP 800-37; CNSSI-4009

70. Training: A learning experience in which an individual is taught to execute a specific information security procedure or understand the information security common body of knowledge. SOURCE: 38 U.S.C. § 5727

71. User: Individual or (system) process acting on behalf of an individual, authorized to access an information system. SOURCE: SP 800-53; SP 800-18; CNSSI-4009

At VA, users are Department personnel, employees, contractors working under an approved contract, business associates working under approved business associate agreements, and any other individuals providing services or performing functions for, to, or on behalf of VA who have been authorized by VA to access VA information or information systems. To access VA sensitive information or VA information systems, these individuals must complete VA-approved security/privacy training, sign the VA National ROB or Contractor ROB, and complete appropriate background screening before such access may be granted.

72. Unauthorized Access: Gaining logical or physical access to VA information or information systems either without authorization or in excess of previously authorized access. SOURCE: SP 800-61

73. VA Contractor Rules of Behavior: A set of Department rules that describes the responsibilities and expected behavior of contractors using VA information systems or VA sensitive information. 38 U.S.C. § 5727

74. VA Information/Data: Information collected or maintained by VA or any entity acting for or on the behalf of VA in support of VA operations and assets. Generally includes information collected or maintained by a VA contractor in the performance of services under a VA contract but excludes information received from VA by entities over which VA has no statutory or operational authority, such as other Federal agencies. SOURCE: FISMA

75. VA National Rules of Behavior: A set of Department rules that describes the responsibilities and expected behavior of users of VA information systems or VA sensitive information. SOURCE: 38 U.S.C. § 5727

76. VA Sensitive Information/Data: All Department Information and/or data on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, and records about individuals requiring protection under applicable confidentiality provisions. SOURCE: 38. USC § 5727

77. Non-Sensitive Information/Data: Information for which the potential impact from the loss of confidentiality, integrity, and availability is low or non-existent, such as information that is routine and administrative, is not protected by any confidentiality provision, is publicly available, and/or is not exempt from release under the Freedom of Information Act. SOURCE: FIPS 199

78. Virtual Private Network (VPN): A virtual network built on top of existing networks that can provide a secure communications mechanism for data and internet protocol (IP) information transmitted between networks. SOURCE: SP 800-113

79. Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. SOURCE: SP 800-53; SP 800-53A; SP 800-37; SP 800-60; SP 800-115; FIPS 200

80. Wide Area Network (WAN): VA's WAN is a telecommunication network that covers a broad area (i.e., any network that links across metropolitan, regional, or national boundaries) and may be comprised of one or more LANs connected to each other.

ACRONYMS AND ABBREVIATIONS USED IN HANDBOOK AND APPENDICES

Acronym/Abbreviation	Definition
A&A	Assessment and Authorization (formerly C&A)
AC	Access Control
AO	Authorizing Official
AT	Awareness and Training
ATO	Authorization to Operate
AU	Audit and Accountability
BI	Background Investigation
C&A	Certification and Accreditation (currently A&A)
CA	Security Assessment and Authorization
CBOC	Community Based Outpatient Clinic
CCB	Change Control Board
CD	Compact Disc
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CM	Configuration Management
CNSS	Committee on National Security Systems
CO	Contracting Officer
COOP	Continuity of Operations Plan
COR	Contracting Officer Representative
COTS	Commercial Off-The-Shelf
CP	Contingency Planning
DAS	Deputy Assistant Secretary
DoS	Denial of Service
DVD	Digital Video Disc
E-mail	Electronic Mail
EA	Enterprise Architecture
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GFE	Government Furnished Equipment
HIPAA	Health Insurance Portability and Accountability Act
HISD	Health Information Security Division
HITECH	Health Information Technology for Economic and Clinical Health
HR	Human Resources
HSPD	Homeland Security Presidential Directive
HTM	Healthcare Technical Management

HTTP	Hyper Text Transfer Protocol
IA	Identification and Authentication
IDS	Intrusion Detection System
IP	Internet Protocol
IR	Incident Response
ISA	Interconnection Security Agreement
ISO	Information Security Officer
IT	Information Technology
LAN	Local Area Network
MA	Maintenance
MAC	Media Access Control
MOU/A	Memorandum of Understanding or Agreement
MP	Media Protection
NARA	National Archives and Records Administration
NCA	National Cemetery Administration
NIST	National Institute of Standards and Technology
NSOC	Network and Security Operations Center
OCS	Office of Cyber Security
ODP	Organizationally Defined Parameters
OIG	Office of Inspector General
OIT	Office of Information and Technology
OMB	Office of Management and Budget
P1	Priority Code 1
P2	Priority Code 2
P3	Priority Code 3
PACS	Physical Access Control Systems
PBX	Private Branch Exchange
PDA	Personal Digital Assistant
PE	Physical and Environmental Protection
PHI	Protected Health Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PL	Planning
PM	Program Management
PO	Privacy Officer
POA&M	Plan of Action and Milestones
PS	Personnel Security

PVT	Patch and Vulnerability Team
RA	Risk Assessment
RMF	Risk Management Framework
ROB	Rules of Behavior
SA	System and Services Acquisition
SC	System and Communications Protection
SCA	Security Control Assessment
SDLC	System Development Life Cycle
SI	System and Information Integrity
SOP	Standard Operating Procedures
SOW	Statement(s) of Work
SP	Special Publication(s)
SPI	Sensitive Personal Information
SSP	System Security Plan
TCP	Transmission Control Protocol
TMS	Talent Management System
U.S.	United States
USB	Universal Serial Bus
U.S.C.	United States Code
US-CERT	United States Computer Emergency Readiness Team
USGCB	United States Government Configuration Baseline
VA	Veterans Affairs
VBA	Veterans Benefits Administration
VHA	Veterans Health Administration
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network

REFERENCES

1. Statutes and Regulations

- a. 20 U.S.C. § 1232g, *Family Educational and Privacy Rights*
- b. 38 CFR § 1.201, *Employee's Duty to Report*
- c. 38 CFR § 1.204, *Information to be Reported to the Office of Inspector General*
- d. 38 CFR §§ 1.460-1.496, *Release of information from Department of Veterans Affairs Records Relating to Drug Abuse, Alcoholism or Alcohol Abuse, Infection with the Human Immunodeficiency Virus (HIV), or Sickle Cell Anemia*
- e. 38 CFR §§ 1.500-1.527, *Release of Information from Department of Veterans Affairs Claimant Records*
- f. 38 CFR §§ 1.575-1.582, *Safeguarding Personal Information in Department of Veterans Affairs Records*
- g. 38 CFR §§ 17.500-17.511, *Confidentiality of Healthcare Quality Assurance Review Records*
- h. 38 C.F.R. §§ 75.111-75.119, *Data Breaches*
- i. 38 U.S.C. § 5701, *Confidential Nature of Claims*
- j. 38 U.S.C. § 5705, *Confidentiality of Medical Quality-Assurance Records*
- k. 38 U.S.C. §§ 5721-5728, *Veteran's Benefits, Information Security*
- l. 38 U.S.C. § 7332, *Confidentiality of Certain Medical Records*
- m. 40 U.S.C. § 11101, *Definitions*
- n. 40 U.S.C. § 1401, *The Clinger Cohen Act of 1996*
- o. 44 U.S.C. §§ 3541-3549, *Coordination of Federal Information Policy, Information Security*
- p. 44 U.S.C. § 3541, *Federal Information Security Management Act of 2002 (FISMA)*
- q. 45 CFR Parts 160 and 164, *HIPAA Privacy and Security Rules*
- r. 45 CFR § 160.103, *Definitions*

- s. 45 CFR §§ 164.400-164.414, *HITECH Breach Notification Rule*
- t. 5 U.S.C., *Government Organization and Employees*
- u. 5 U.S.C. § 552, *Freedom of Information Act*
- v. 5 U.S.C. § 552a, *Privacy Act of 1974*
- w. Pub. L. 104-191 § 264, 110 Stat. 1936, *Health Insurance Portability and Accountability Act*
- x. Pub. L. 107-347 § 208, 116 Stat. 2899, 2921, *E-Government Act of 2002*
- y. Pub. L. 111-5 §§ 13400-13411, 123 Stat. 226, *Health Information Technology for Economic and Clinical Health (HITECH) Act*

2. Federal Information Processing Standards (FIPS) Publications

- a. FIPS Pub. 140-2, *Security Requirements for Cryptographic Modules*
- b. FIPS Pub. 191, *Guideline for the Analysis of Local Area Network Security*
- c. FIPS Pub. 196, *Entity Authentication Using Public Key Cryptography*
- d. FIPS Pub 199, *Standards for Security Categorization of Federal Information and Information Systems*
- e. FIPS Pub 200, *Minimum Security Requirements for Federal Information and Information Systems*
- f. FIPS Pub 201, *Personal Identity Verification of Federal Employees and Contractors*

3. National Institute of Standards and Technology (NIST) Special Publications (SP)

- a. NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*
- b. NIST SP 800-19, *Mobile Agent Security*
- c. NIST SP 800-27A, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*
- d. NIST SP 800-28, *Guidelines on Active Content and Mobile Code*
- e. NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*

- f. NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*
- g. NIST SP 800-40, *Creating a Patch and Vulnerability Management Program*
- h. NIST SP 800-41, *Guidelines on Firewalls and Firewall Policy*
- i. NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*
- j. NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*
- k. NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans*
- l. NIST SP 800-57, *Recommendation for Key Management*
- m. NIST SP 800-58, *Security Considerations for Voice Over IP Systems*
- n. NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) - Volume 1: Guide Volume 2: Appendices*
- o. NIST SP 800-61, *Computer Security Incident Handling Guide*
- p. NIST SP 800-63, *Electronic Authentication Guideline*
- q. NIST SP 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*
- r. NIST SP 800-73, *Interfaces for Personal Identity Verification (4 parts): Pt. 1 - End Point PIV Card Application Namespace, Data Model and Representation, Pt. 2 - PIV Card Application Card Command Interface, Pt. 3 - PIV Client Application Programming Interface, and Pt. 4 - The PIV Transitional Interfaces and Data Model Specification*
- s. NIST SP 800-76, *Biometric Data Specification for Personal Identity Verification*
- t. NIST SP 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification (PIV)*
- u. NIST SP 800-79-1, *Guidelines for the Accreditation of Personal Identity Verification Card Issuers*
- v. NIST SP 800-88, *Guidelines for Media Sanitization*

- w. NIST SP 800-113, *Guide to SSL VPNs*
- x. NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*
- y. NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*
- z. NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*

4. Office of Management and Budget (OMB) Publications

- a. OMB Circular A-11, *Preparation, Submission, and Execution of the Budget*
- b. OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*
- c. OMB Memorandum M-00-07, *Incorporating and Funding Security in Information Systems Investments*
- d. OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*
- e. OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*
- f. OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*
- g. OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*
- h. OMB Memorandum M-08-23, *Securing the Federal Government's Domain Name System Infrastructure*

5. VA Directives and Handbooks

- a. VA Directive 0735, *Homeland Security Presidential Directive 12 (HSPD-12) Program*
- b. VA Directive 5011, *Hours of Duty and Leave*
- c. VA Directive 6001, *Limited Personal Use of Government Office Equipment Including Information Technology*
- d. VA Directive 6004, *Configuration, Change, and Release Management Programs*
- e. VA Directive 6066, *Protected Health Information (PHI)*

- f. VA Directive 6330, *Directives Management*
- g. VA Directive 6371, *Destruction of Temporary Paper Records*
- h. VA Directive 6500, *Managing Information Security Risk: VA Information Security Program*
- i. VA Directive 6502, *VA Enterprise Privacy Program*
- j. VA Directive 6508, *Privacy Impact Assessments*
- k. VA Directive 6509, *Duties of Privacy Officers*
- l. VA Directive 6511, *Presentations Displaying Personally-Identifiable Information*
- m. VA Directive 6512, *Secure Wireless Technology*
- n. VA Directive 6513, *Secure External Connections*
- o. VA Directive 6550, *Pre-Procurement Assessment for Medical Devices*
- p. VA Directive 6609, *Mailing of Sensitive Personal Information*
- q. VA Directive and Handbook 0710, *Personnel Security and Suitability Program*
- r. VA Directive and Handbook 0730, *Security and Law Enforcement*
- s. VA Handbook 5011/5, *Hours of Duty and Leave*
- t. VA Handbook 6300.6, *Procedures for Releasing Lists of Veterans' and Dependents' Names and Addresses*
- u. VA Handbook 6330, *Directives Management Procedures*
- v. VA Handbook 6500.1, *Electronic Media Sanitization*
- w. VA Handbook 6500.2/1, *Management of Data Breaches Involving Sensitive Personal Information (SPI)*
- x. VA Handbook 6500.3, *Certification and Accreditation of VA Information Systems*
- y. VA Handbook 6500.5, *Incorporating Security and Privacy into the System Development Life Cycle*
- z. VA Handbook 6500.6, *Contract Security*

- aa. VA Handbook 6500.8, *Information Technology Contingency Planning*
- bb. VA Handbook 6502.1, *Privacy Event Tracking*
- cc. VA Handbook 6508.1, *Privacy Impact Assessment (PIA)*
- dd. VA Handbook 7002, *Logistics Management*

6. VHA Directives and Handbooks

- a. VHA Directive 2007-040, *Appointment of Facility Information Security Office (ISO) and Privacy Officer to the Institutional Review Board (IRB) or the Research and Development (R&D) Committee*
- b. VHA Handbook 1200.05, *Requirements for the Protection of Human Subjects in Research*
- c. VHA Handbook 1600.01, *Business Associate Agreements*

7. Other References

- a. CNSSI-4009, *National Information Assurance Glossary*
- b. Homeland Security Presidential Directive (HSPD) 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*

**DEPARTMENT OF VETERANS AFFAIRS NATIONAL RULES OF BEHAVIOR
INTRODUCTION****1. BACKGROUND.**

a. Section 5723(b)(12) of title 38, U.S.C., requires the Assistant Secretary for Information and Technology to establish “VA National Rules of Behavior for appropriate use and protection of the information which is used to support Department’s missions and functions.” OMB Circular A-130, Appendix III, paragraph 3a(2)(a) requires that all Federal agencies promulgate rules of behavior (ROB) that “clearly delineate responsibilities and expected behavior of all individuals with access” to the agencies’ information and information systems, as well as to state clearly the “consequences of behavior not consistent” with the ROB. **The Department of Veterans Affairs (VA) National ROB that begins on page D-4 is required to be used throughout VA.**

b. Congress and OMB require the promulgation of ROB for two reasons. First, Congress and OMB recognize that knowledgeable users are the foundation of a successful security program. Users must understand that taking personal responsibility for the security of their computer and the VA data that it contains or that may be accessed through it, as well as the security and protection of VA information in any form (e.g., digital, paper), are essential aspects of their job. Second, individuals must be held accountable for their use of VA information and information systems.

c. VA must achieve the Gold Standard in data security which requires that VA information and information system users protect VA information and information systems, especially the personal data of Veterans, their family members, and employees. Users must maintain a heightened and constant awareness of their responsibilities regarding the protection of VA information. The Golden Rule with respect to this aspect of VA employees’ responsibilities is to treat the personal information of others the same as they would their own.

d. Since written guidance cannot cover every contingency, authorized users are asked to go beyond the stated rules, using “due diligence” and highest ethical standards to guide their actions. Users must understand that these rules are based on Federal laws, regulations, and VA directives.

2. COVERAGE

a. The attached VA National ROB must be signed annually by all VA employees who are authorized to use VA information systems or VA sensitive information. The term VA employees includes all individuals who are employees under title 5 or title 38, U.S.C., as well as individuals whom the Department considers employees such as volunteers non-compensated employees, students, and other trainees. The VA Contractor ROB must be signed by contractors/sub-contractors that have been authorized to use VA information systems or VA sensitive information and is addressed in VA Handbook 6500.6. The Contractor ROB can be found as an Appendix to VA Handbook 6500.6. Contractors sign the VA Contractor ROB; they do not sign the VA National ROB. All users of VA information systems or VA sensitive information must sign the appropriate ROB to indicate that they have read, understood, and agree to abide by the ROB before access is provided to the VA information system or the VA sensitive information.

b. The VA National ROB and the Contractor ROB address notice and consent issues identified by the Department of Justice and other sources. It also serves to clarify the roles of management and system administrators, as well as to provide notice of what is considered acceptable use of all VA information and information systems, VA sensitive information, and behavior of VA users.

c. The VA National ROB uses the phrase "VA sensitive information". This phrase is defined in VA Handbook 6500,, Appendix F. This definition covers all information as defined in 38 U.S.C. 5727(19), and in 38 U.S.C. 5727(23). The phrase "VA sensitive information" as used in the attached VA National ROB means:

All Department data, on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, records about individuals requiring protection under various confidentiality provisions such as the Privacy Act of 1974 and the HIPAA Privacy Rule, and information that can be withheld under the Freedom of Information Act.

Examples of information that could be considered VA sensitive information, depending on the specific circumstances, include the following: individually-identifiable medical, benefits, and personnel information; financial; budgetary; research; quality assurance; confidential commercial; critical infrastructure; investigatory and law enforcement information; information that is confidential and privileged in litigation such as information protected by the deliberative process privilege, attorney work-product privilege, and the attorney-client privilege; and other information which, if released, could result in violation of law or harm or unfairness to any individual or group, or could adversely affect the national interest or the conduct of Federal programs.

d. The phrase "VA sensitive information" includes information entrusted to the Department.

e. The VA National ROB and the Contractor ROB are included in VA's OIT Security and Privacy Training module located in the VA Talent Management System (TMS). Users are advised to complete their ROB electronically within the TMS system, if possible.

f. The VA National ROB and the Contractor ROB can be signed in hard copy or electronically. If signed using the hard copy method the user should initial and date each page and provide the information requested on the last page.

3. RULES OF BEHAVIOR

Immediately following this section is the VA approved National ROB that all employees as outlined above, who are users of VA information systems or VA sensitive information, are required to sign in order to obtain access to VA sensitive information or VA information systems.

DEPARTMENT OF VETERANS AFFAIRS NATIONAL RULES OF BEHAVIOR

I understand, accept, and agree to the following terms and conditions that apply to my access to, and use of, information, including VA sensitive information, or information systems of the U.S. Department of Veterans Affairs.

1. GENERAL RULES OF BEHAVIOR

a. I understand that an essential aspect of my job is to take personal responsibility for the secure use of VA systems and the VA data that it contains or that may be accessed through it, as well as the security and protection of VA information in any form (e.g., digital, paper).

b. I understand that when I use any government information system, I have NO expectation of privacy in any records that I create or in my activities while accessing or using such information system.

c. I understand that authorized VA personnel may review my conduct or actions concerning VA information and information systems, and take appropriate action. Authorized VA personnel include my supervisory chain of command as well as VA system administrators and ISOs. Appropriate action may include monitoring, recording, copying, inspecting, restricting access, blocking, tracking, and disclosing information to authorized OIG, VA, and law enforcement personnel.

d. I understand that the following actions are prohibited: unauthorized access, unauthorized uploading, unauthorized downloading, unauthorized changing, unauthorized circumventing, or unauthorized deleting of information on VA systems, modifying VA systems, unauthorized denying or granting access to VA systems, using VA resources for unauthorized use on VA systems, or otherwise misusing VA systems or resources. I also understand that attempting to engage in any of these unauthorized actions is also prohibited.

e. I understand that such unauthorized attempts or acts may result in disciplinary or other adverse action, as well as criminal or civil penalties. Depending on the severity of the violation, disciplinary or adverse action consequences may include: suspension of access privileges, reprimand, suspension from work, demotion, or removal. Theft, conversion, or unauthorized disposal or destruction of Federal property or information may also result in criminal sanctions.

f. I understand that I have a responsibility to report suspected or identified information security incidents (security and privacy) to my VA supervisor, ISO and PO, immediately upon suspicion.

g. I understand that I have a duty to report information about actual or possible criminal violations involving VA programs, operations, facilities, contracts or information systems to my VA supervisor, local CIO and ISO, any management official or directly to the OIG, including reporting to the OIG Hotline. I also understand that I have a duty to immediately report to the OIG any possible criminal matters involving felonies, including crimes involving information systems.

h. I understand that the VA National ROB do not and should not be relied upon to create any other right or benefit, substantive or procedural, enforceable by law, by a party to litigation with the U.S. Government.

i. I understand that the VA National ROB do not supersede any policies of VA facilities and other agency components that provide higher levels of protection to VA's information or information systems. The VA National ROB provide the minimal rules with which individual users must comply.

j. I understand that if I refuse to sign this VA National ROB as required by VA policy, I will be denied access to VA information systems or VA sensitive information. Any refusal to sign the VA National ROB may have an adverse impact on my employment with the Department.

2. SPECIFIC RULES OF BEHAVIOR

a. Basic

(1) I will follow established VA information security and privacy policies and procedures.

(2) I will comply with any directions from my supervisors, VA system administrators, and ISOs concerning my access to, and use of, VA information and information systems or matters covered by these ROB.

(3) I understand that I may need to sign a non-VA entity's ROB to obtain access to their system in order to conduct VA business. While using their system, I must comply with their ROB. However, I must also comply with VA's National ROB whenever I am accessing VA information systems or VA sensitive information.

(4) I may be required to acknowledge or sign additional specific or unique ROB in order to access or use specific VA systems. I understand that those specific ROB may include, but are not limited to, restrictions or prohibitions on limited personal use, special requirements for access or use of the data in that system, special requirements for the devices used to access that specific system, or special restrictions on interconnections between that system and other IT resources or systems.

b. Data Protection

(1) I will safeguard electronic VA sensitive information at work and remotely. I understand that all VA owned mobile devices must be encrypted using FIPS 140-2, *Security Requirements for Cryptographic Modules*, validated encryption (or its successor) unless encryption is not technically possible, as determined and approved by my local ISO, CIO and the DAS for OIS. This includes laptops, thumb drives, and other removable storage devices and storage media (e.g., CDs, Digital Video Discs (DVD)).

(2) I understand that per VA Directive 6609, *Mailing of Sensitive Personal Information*, the following types of information are excluded from the encryption requirement when mailed

according to the requirements outlined in the directive:

(a) Information containing the SPI of a single individual to:

1. That person (e.g., the Veteran's, beneficiary's, dependent's, or employee's own information) or to that person's legal representative (e.g., guardian, attorney-in-fact, attorney, or Veteran Service Organization). Such information may be mailed to an entity, not otherwise the subject of an exception, with the express written consent of the individual. Such information may be mailed via U.S. Postal Service regular mail unless tracked delivery service is requested and paid for by the recipient;

2. A business partner such as a health plan or insurance company, after reviewing potential risk;

3. A court, adjudicative body, parties in litigation, or to persons or entities in the course of a judicial or administrative proceeding; and

4. Congress, law enforcement agencies, and other governmental entities.

(b) Information containing SPI of one or more individuals to a person or entity that does not have the capability to decrypt information that is encrypted by VA, when sent according to VA Directive 6609.

(3) I understand that I must have approval from my supervisor to use, process, store, or transmit electronic VA sensitive information remotely (outside of VA owned or managed facilities (e.g., medical centers, community based outpatient clinics (CBOC), regional offices)).

(4) If approved to use, process, store, or transmit electronic VA sensitive information remotely, I must ensure any device I utilize is encrypted using FIPS 140-2 (or its successor) validated encryption. Information systems must use VA's approved configuration and security control requirements. The local CIO and ISO must review and approve (in writing) the mechanisms used to transport and store the VA sensitive data before it can be removed from the VA facility.

(5) I will ensure that all printouts of VA sensitive information that I work with, as part of my official duties, are physically secured when not in use (e.g., locked cabinet, locked door).

(6) I acknowledge that particular care should be taken to protect SPI aggregated in lists, databases, or logbooks, and will include only the minimum necessary SPI to perform a legitimate business function.

(7) I recognize that access to certain databases, regional-, or national-level data such as data warehouses or registries containing patient or benefit information, and data from other Federal agencies such as the Centers for Medicare and Medicaid or the Social Security Administration, has the potential to cause great risk to VA, its customers and employees due to the number and/or sensitivity of the records being accessed. I will act accordingly to ensure the confidentiality and security of these data commensurate with this increased potential risk.

(8) If I have been approved by my supervisor to take printouts of VA sensitive information home or to another remote location outside of a VA facility, or if I have been provided the ability to print VA sensitive information from a remote location to a location outside of a VA facility, I must ensure that the printouts are destroyed to meet VA disposal requirements when they are no longer needed and in accordance with all relevant records retention requirements. Two secure options that can be used are to utilize a shredder that meets VA and NIST's requirements or return the printouts to a VA facility for appropriate destruction.

(9) When in an uncontrolled environment (e.g., public access work area, airport, or hotel), I will protect against disclosure of VA sensitive information which could occur by eavesdropping, overhearing, or overlooking (shoulder surfing) from unauthorized persons. I will also follow a clear desk policy that requires me to remove VA sensitive information from view when not in use (e.g., on desks, printers, fax machines, etc.). I will also secure mobile and portable computing devices (e.g., laptops, USB thumb drives, PDA).

(10) I will use VA approved encryption to encrypt any e-mail, including attachments to the e-mail that contains VA sensitive information before sending the e-mail. I will not send any e-mail that contains VA sensitive information in an unencrypted form. I will not encrypt e-mail that does not include VA sensitive information or any e-mail excluded from the encryption requirement under para. b(2).

(11) I will not auto-forward e-mail messages to addresses outside the VA network.

(12) I will take reasonable steps to ensure fax transmissions are sent to the appropriate destination, including double checking the fax number, confirming delivery of the fax, using a fax cover sheet with the required notification message included and only transmitting individually identifiable-information via fax when no other reasonable means exist and when someone is at the machine to receive the transmission or the receiving machine is in a secured location.

(13) I will protect VA sensitive information from unauthorized disclosure, use, modification, or destruction, including using encryption products approved and provided by VA to protect sensitive data. I will only provide access to sensitive information to those who have a need-to-know for their professional duties, including only posting sensitive information to web-based collaboration tools restricted to those who have a need-to-know and when proper safeguards are in place for sensitive information. For questions regarding need-to-know and safeguards, I will obtain guidance from my VA supervisor, local CIO, and/or ISO before providing any access.

(14) When using wireless connections for VA business I will only use VA authorized wireless connections and will not transmit VA sensitive information via wireless technologies unless the connection uses FIPS 140-2 (or its successor) validated encryption.

(15) I will properly dispose of VA sensitive information, either in hardcopy, softcopy, or electronic format, in accordance with VA policy and procedures.

(16) I will never swap or surrender VA hard drives or other storage devices to anyone other than an authorized OIT employee.

c. Logical Access Controls

(1) I will follow established procedures for requesting access to any VA computer system and for notification to the VA supervisor, local CIO, and/or ISO when the access is no longer needed.

(2) I will only utilize passwords that meet the VA minimum requirements defined in control **IA-5: Authenticator Management** in VA Handbook 6500, Appendix F, including using compliant passwords for authorized web-based collaboration tools that may not enforce such requirements.

(3) I will protect my verify codes and passwords from unauthorized use and disclosure. I will not divulge a personal username, password, access code, verify code, or other access requirement to anyone.

(4) I will not store my passwords or verify codes in any file on any IT system, unless that file has been encrypted using FIPS 140-2 (or its successor) validated encryption and I am the only person who can decrypt the file. I will not hardcode credentials into scripts or programs.

(5) I will use elevated privileges (e.g., Administrator accounts), if provided for the performance of my official duties, only when such privileges are needed to carry out specifically assigned tasks which require elevated access. When performing general user responsibilities, I will use my individual user account.

d. Remote Access/Teleworking

(1) I understand that remote access is allowed from other Federal Government computers and systems to VA information systems, subject to the terms of VA and the host Federal agency's policies.

(2) I agree that I will directly connect to the VA network whenever possible. If a direct connection to the VA network is not possible, then I will use VA-approved remote access software and services. I will use VA-provided IT equipment for remote access when possible.

(3) I agree that I will not have both a VA network connection and any non-VA network connection (including a modem or phone line or wireless network card, etc.) physically connected to any computer at the same time unless the dual connection is explicitly authorized in writing by my VA supervisor, local CIO, and ISO.

(4) I am responsible for the security of VA property and information, regardless of my work location. VA security policies are the same and will be enforced at the same rigorous level when I telework as when I am in the office. I will keep government furnished equipment (GFE) and VA information safe, secure, and separated from my personal property and information.

(5) I will ensure that VA sensitive information, in any format, and devices, systems and/or software that contain such information or that I use to access VA sensitive information or information systems are adequately secured in remote locations (e.g., at home and during travel) and agree to periodic VA inspections of the devices, systems or software from which I conduct access from remote locations. I agree that if I work from a remote location, pursuant to an approved telework agreement with VA sensitive information, authorized OIT personnel may periodically inspect the remote location for compliance with required security requirements.

(6) I will protect information about remote access mechanisms from unauthorized use and disclosure.

(7) I will notify my VA supervisor, local CIO and ISO prior to any international travel with a mobile device (laptop, PDA) so that appropriate actions can be taken prior to my departure and upon my return, including potentially issuing a specifically configured device for international travel and/or inspecting the device or reimaging the hard drive upon return.

(8) I will exercise a higher level of awareness in protecting mobile devices when traveling internationally as laws and individual rights vary by country and threats against Federal employee devices may be heightened.

e. Non-VA Owned Systems

(1) I agree that I will not allow VA sensitive information to reside on non-VA systems or devices unless specifically designated and approved in writing in advance by my VA supervisor, local CIO, and ISO. I agree that I will not access, transmit, or store remotely any VA sensitive information that is not encrypted using VA approved encryption.

(2) I will only use VA approved solutions for connecting non-VA owned systems to VA's network.

(3) I will obtain my local CIO's approval prior to connecting any non-VA equipment to VA's network at a VA facility. This includes directly connecting to a network port or utilizing remote access capabilities within the VA facility.

f. System Security Controls

(1) I will not attempt to override, circumvent, or disable operational, technical, or management security controls unless expressly directed to do so in writing by authorized VA staff. I will not attempt to alter the security configuration of government equipment unless authorized.

(2) I will only use virus protection software, anti-spyware, and firewall/intrusion detection software authorized by VA on VA equipment.

(3) I will not disable or degrade software programs used by VA that install security software updates to VA computer equipment, to computer equipment used to connect to VA information systems, or to create, store or use VA information.

(4) I agree to have issued GFE scanned and serviced by VA authorized personnel. This may require me to return it promptly to a VA facility upon demand.

(5) I will permit only those authorized by OIT to perform maintenance on IT components, including installation or removal of hardware or software.

g. System Access

(1) I will use only VA approved devices, systems, software, services, and data which I am authorized to use, including complying with any software licensing or copyright restrictions.

(2) I will only use VA approved collaboration technologies for conducting VA business.

(3) I will not download software from the Internet, or other public available sources, offered as free trials, shareware, or other unlicensed software to a VA owned system.

(4) I will not host, set up, administer, or operate any type of Internet server or wireless access point on any VA network unless explicitly authorized in writing by my local CIO and approved by my ISO. I will ensure that all such activity is in compliance with Federal and VA policies.

(5) I will not attempt to probe computer systems to exploit system controls or to obtain unauthorized access to VA sensitive data.

(6) I will only use my access to VA computer systems and/or records for officially authorized and assigned duties. The use must not violate any VA policy regarding jurisdiction, restrictions, limitations or areas of responsibility.

(7) I will use my access under VA Directive 6001, *Limited Personal Use of Government Office Equipment Including Information Technology*, understanding that this Directive does not pertain to accessing VA applications or records. I will not engage in any activity that is prohibited by the Directive.

(8) I will prevent unauthorized access by another user by ensuring that I log off or lock any VA computer or console before walking away or initiate a comparable application feature that will keep others from accessing the information and resources available in my computing session.

h. Miscellaneous

(1) I will complete mandatory periodic security and privacy awareness training within designated timeframes, and complete any additional role-based security training required, based on my roles and responsibilities.

(2) I will take precautions as directed by communications from my ISO and local OIT staff to protect my computer from emerging threats.

(3) I understand that while logged into authorized Web-based collaboration tools I am a representative of VA and I will abide by the ROB and all other policies and procedures related to these tools.

(4) I will protect government property from theft, loss, destruction, or misuse. I will follow VA policies and procedures for handling Federal Government IT equipment and will sign for items provided to me for my exclusive use and return them when no longer required for VA activities.

3. ACKNOWLEDGEMENT AND ACCEPTANCE

a. I acknowledge that I have received a copy of these Rules of Behavior.

b. I understand, accept and agree to comply with all terms and conditions of these Rules of Behavior.

Print or type your full name

Signature

Date

Office Phone

Position Title

SECURITY CONTROL CLASSES, FAMILIES, AND IDENTIFIERS

IDENTIFIER	FAMILY	CLASS
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PM	Program Management	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational

VA SYSTEM SECURITY CONTROLS

1. BACKGROUND/OVERVIEW

a. The Assistant Secretary for Information and Technology is VA's CIO. VA's CIO is responsible for the implementation of security controls on all VA OIT systems and other designated systems when appropriate and technically possible. The VA CIO has delegated the implementation of appropriate security controls to the System Owner. This Appendix has been prepared to assist the System Owners in selecting the appropriate security controls to secure their systems. The controls outlined in this Appendix are a combination of the current version of SP 800-53 controls for Federal systems as well as VA specific requirements. VA Directive and Handbook 6500 should be read and understood prior to using this Appendix as they provide the rationale and background for this Appendix. Once the controls have been determined by the System Owner, they are documented in the SSP and approved by the VA AO (CIO) or designee. Once approved, these controls will be implemented, monitored, and revised as required. Auditing personnel will use the approved security plan and the controls outlined within the plan to determine compliance. The approved security plan will also be used in the A&A of all new systems.

b. System Owners may supplement the minimum requirements of this Appendix with more stringent requirements based on the need for additional controls within the operating unit's unique computing environment within the constraints of a formal risk assessment. See **Selection of Security Controls – RMF Step 2** in the core document for information regarding the scoping, tailoring and supplementing of security controls for a system. System Owners should use the current version of SP 800-53 for supplemental controls required for their systems.

c. FIPS 200 and the current version of SP 800-53 notes that the security controls applied to a particular information system should be commensurate with the overall impact on VA operations and assets, or individuals should there be a breach in security due to the loss of confidentiality, integrity, and availability. This is a natural outgrowth of the formal risk assessment process. FIPS 199 requires VA to categorize their information systems as low-, moderate-, or high-impact for the security objectives of confidentiality, integrity, and availability. The overall impact value assigned to the entire information system is the highest value (i.e., high water mark, aka "System High" concept) from among the security categories that have been determined for each type of information resident on those information systems. The current version of SP 800-60 provides guidance on the assignment of security categories to information systems. The generalized format for expressing the security category of an information system is:

d. **Security Category** information system= {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)}, where the acceptable values for potential impact are low, moderate, or high.

e. Since the potential impact values for confidentiality, integrity, and availability may not always be the same for a particular information system, the high water mark concept is used to

determine the impact level of the information system for the express purpose of selecting an initial set of security controls from one of the three security controls baselines defined in the current version of SP 800-53. Thus, a low-impact system is defined as an information system in which all three of the security objectives are low. A moderate-impact system is an information system in which at least one of the security objectives is moderate and no security objective is greater than moderate. A high-impact system is an information system in which at least one security objective is high. Once the overall impact level of the information system is determined, an initial set of security controls can be selected from the minimum controls recommended by NIST for low, moderate, or high baselines, which are contained in this Appendix.

f. VA requires that Operating Units comply with all FIPS mandates and recommendations of the current version of SP 800-53 and this Appendix, to develop an acceptable control baseline for each information system appropriate to the impact level of the system. This Appendix contains both the NIST controls as outlined in the current version of SP 800-53 and VA's organizational controls based on VA's specific environment.

g. To uniquely identify each control within the families, a numeric identifier is appended to the family identifier to indicate the number of the control within the family. Table 1: Security Controls Baselines summarizes the numeric identifiers for each security control family.

h. Each of the controls outlined in this Appendix has been designated with a type of security control. The types of security controls are:

(1) Common Controls

(a) Common controls are security controls that are inheritable by one or more VA information system. Common security controls can apply to: (i) all agency information systems; (ii) a group of information systems at a specific site (may be associated with the terms site A&A); or (iii) common information systems, subsystems, or applications (i.e., common hardware, software, and/or firmware) deployed at multiple operational sites (may be associated with the terms type authorization). Common security controls, typically identified during a collaborative agency-wide process with the involvement of the VA AO (CIO), Director for Cyber Security, Information System Owners, and ISOs (and by developmental program managers in the case of common security controls for common hardware, software, and/or firmware), have the following properties:

1. The development, implementation, and assessment of common security controls can be assigned to responsible agency officials or organizational elements (other than the information System Owners whose systems will implement or use those common security controls); and

2. The results from the assessment of the common security controls can be used to support the security authorization processes of agency information systems where those controls have been applied.

(b) The objective of common controls is to reduce security costs by centrally managing the development, implementation, and assessment of the common security controls designated by the agency and subsequently, sharing assessment results with the owners of information systems where those common security controls are applied. The list of VA's common controls and the responsible office are located in **Attachment 1** of this Appendix.

(2) Hybrid Controls – Controls for which one part of the control is deemed to be common, while another part of the control is deemed to be system-specific are considered *hybrid controls*. For example, **CA-5: Plan of Action and Milestones** security control is a hybrid control with the policy portion of the control deemed to be common and the procedures/SOPs portion of the control deemed to be system-specific. Hybrid security controls may also serve as templates for further control refinement. For example, the **CP-2: Contingency Plan** security control may be implemented as a master template for a generalized contingency plan for all agency information systems with individual information System Owners tailoring the plan, where appropriate, for system-specific issues. The list of hybrid controls is located in **Attachment 2** of this Appendix.

(3) System Specific Controls - Controls not designated as common controls are considered *system specific controls* and are the responsibility of the information System Owner. SSPs should clearly identify which security controls have been designated as common security controls and which controls have been designated as system-specific controls. The list of system specific controls and recommended parameters is located in **Attachment 3** of this Appendix.

i. System Owners can use the recommended *priority code* designation associated with each security control in the baselines to assist in making sequencing decisions for control implementation (i.e., a Priority Code 1 (P1) control has a higher priority for implementation than a Priority Code 2 (P2) control; a P2 control has a higher priority for implementation than a Priority Code 3 (P3) control). This recommended sequencing prioritization helps ensure that foundational security controls upon which other controls depend are implemented first, thus enabling VA to deploy controls in a more structured and timely manner in accordance with available resources. The implementation of security controls by sequence priority code does not imply the achievement of any defined level of risk mitigation until *all* of the security controls in the security plan have been implemented. The priority codes are used only for implementation sequencing, not for making security control selection decisions. Table 1: Security Controls Baselines summarizes sequence priority codes for the baseline security controls.

j. The following figure, Figure:3: Security Control Selection Process, is a flowchart that contains the security control selection process.

FIGURE 3: SECURITY CONTROL SELECTION PROCESS

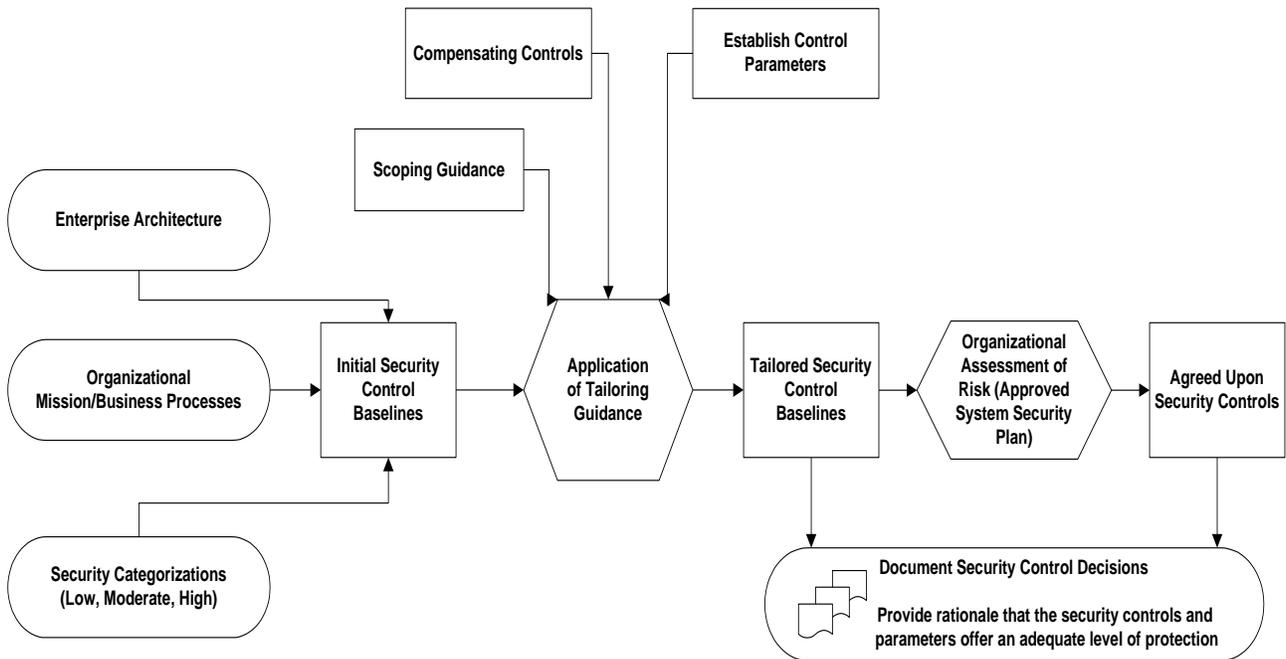


Figure 3 is a flowchart that contains the security control selection process that has been defined in VA Handbook 6500.

TABLE 1: SECURITY CONTROLS BASELINES

The initial security controls baselines for systems designated as low-, moderate-, and high-impact are provided in Table 1 below:

Priority Code	Sequencing	Action
Priority Code 1 (P1)	FIRST	Implement P1 security controls first
Priority Code 2 (P2)	NEXT	Implement P2 security controls after implementation of P1 controls
Priority Code 3 (P3)	LAST	Implement P3 security controls after implementation of P1 and P2 controls
Unspecified Priority Code (P4)	NONE	Security control not selected for baseline

Control Number	Control Name	Priority	Control Baselines		
			Low	Moderate	High
Access Controls					
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1)(2)(3)(4)	AC-2 (1)(2)(3)(4)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5
AC-6	Least Privilege	P1	Not Selected	AC-6 (1)(2)	AC-6 (1)(2)
AC-7	Unsuccessful Logon Attempts	P2	AC-7	AC-7	AC-7
AC-8	System Use Notification	P1	AC-8	AC-8	AC-8
AC-9	Previous Logon (Access) Notification	P4	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	P2	Not Selected	Not Selected	AC-10
AC-11	Session Lock	P3	Not Selected	AC-11	AC-11
AC-12	Session Termination (Withdrawn)	---	---	---	---
AC-13	Supervision and Review—Access Control (Withdrawn)	---	---	---	---
AC-14	Permitted Actions without Identification or Authentication	P1	AC-14	AC-14 (1)	AC-14 (1)
AC-15	Automated Marking (Withdrawn)	---	---	---	---
AC-16	Security Attributes	P4	Not Selected	Not Selected	Not Selected
AC-17	Remote Access	P1	AC-17	AC-17 (1)(2)(3)(4)(5)(7)(8)	AC-17 (1)(2)(3)(4)(5)(7)(8)

Control Number	Control Name	Priority	Control Baselines		
			Low	Moderate	High
Access Controls					
AC-18	Wireless Access	P1	AC-18	AC-18 (1)	AC-18 (1)(2)(4)(5)
AC-19	Access Control for Mobile Devices	P1	AC-19	AC-19 (1)(2)(3)	AC-19 (1)(2)(3)
AC-20	Use of External Information Systems	P1	AC-20	AC-20 (1)(2)	AC-20 (1)(2)
AC-21	User-Based Collaboration and Information Sharing	P4	Not Selected	Not Selected	Not Selected
AC-22	Publicly Accessible Content	P2	AC-22	AC-22	AC-22
Awareness and Training					
AT-1	Security Awareness and Training Policy and Procedures	P1	AT-1	AT-1	AT-1
AT-2	Security Awareness	P1	AT-2	AT-2	AT-2
AT-3	Security Training	P1	AT-3	AT-3	AT-3
AT-4	Security Training Records	P3	AT-4	AT-4	AT-4
AT-5	Contacts with Security Groups and Associations	P4	Not Selected	Not Selected	Not Selected
Audit and Accountability					
AU-1	Audit and Accountability Policy and Procedures	P1	AU-1	AU-1	AU-1
AU-2	Auditable Events	P1	AU-2	AU-2 (3)(4)	AU-2 (3)(4)
AU-3	Content of Audit Records	P1	AU-3	AU-3 (1)	AU-3 (1)(2)
AU-4	Audit Storage Capacity	P1	AU-4	AU-4	AU-4
AU-5	Response to Audit Processing Failures	P1	AU-5	AU-5	AU-5 (1)(2)
AU-6	Audit Review, Analysis, and Reporting	P1	AU-6	AU-6	AU-6 (1)
AU-7	Audit Reduction and Report Generation	P2	Not Selected	AU-7 (1)	AU-7 (1)
AU-8	Time Stamps	P1	AU-8	AU-8 (1)	AU-8 (1)
AU-9	Protection of Audit Information	P1	AU-9	AU-9	AU-9
AU-10	Non-repudiation	P1	Not Selected	Not Selected	AU-10
AU-11	Audit Record Retention	P3	AU-11	AU-11	AU-11
AU-12	Audit Generation	P1	AU-12	AU-12	AU-12 (1)
AU-13	Monitoring for Information Disclosure	P4	Not Selected	Not Selected	Not Selected
AU-14	Session Audit	P4	Not Selected	Not Selected	Not Selected

Control Number	Control Name	Priority	Control Baselines		
			Low	Moderate	High
Security Assessment and Authorization					
CA-1	Security Assessment and Authorization Policies and Procedures	P1	CA-1	CA-1	CA-1
CA-2	Security Assessments	P2	CA-2	CA-2 (1)	CA-2 (1)(2)
CA-3	Information System Connections	P1	CA-3	CA-3	CA-3
CA-4	Security Certification (Withdrawn)	---	---	---	---
CA-5	Plan of Action and Milestones	P3	CA-5	CA-5	CA-5
CA-6	Security Authorization	P3	CA-6	CA-6	CA-6
CA-7	Continuous Monitoring	P3	CA-7	CA-7	CA-7
Configuration Management					
CM-1	Configuration Management Policy and Procedures	P1	CM-1	CM-1	CM-1
CM-2	Baseline Configuration	P1	CM-2	CM-2 (1)(3)(4)	CM-2 (1)(2)(3)(5)(6)
CM-3	Configuration Change Control	P1	Not Selected	CM-3 (2)	CM-3 (1)(2)
CM-4	Security Impact Analysis	P2	CM-4	CM-4	CM-4 (1)
CM-5	Access Restrictions for Change	P1	Not Selected	CM-5	CM-5 (1)(2)(3)
CM-6	Configuration Settings	P1	CM-6	CM-6 (3)	CM-6 (1)(2)(3)
CM-7	Least Functionality	P1	CM-7	CM-7 (1)	CM-7 (1)(2)
CM-8	Information System Component Inventory	P1	CM-8	CM-8 (1)(5)	CM-8 (1)(2)(3)(4)(5)
CM-9	Configuration Management Plan	P1	Not Selected	CM-9	CM-9

Control Number	Control Name	Priority	Control Baselines		
			Low	Moderate	High
Contingency Planning					
CP-1	Contingency Planning Policy and Procedures	P1	CP-1	CP-1	CP-1
CP-2	Contingency Plan	P1	CP-2	CP-2 (1)	CP-2 (1)(2)(3)
CP-3	Contingency Training	P2	CP-3	CP-3	CP-3 (1)
CP-4	Contingency Plan Testing and Exercises	P2	CP-4	CP-4 (1)	CP-4 (1)(2)(4)
CP-5	Contingency Plan Update (Withdrawn)	---	---	---	---
CP-6	Alternate Storage Site	P1	Not Selected	CP-6 (1)(3)	CP-6 (1)(2)(3)
CP-7	Alternate Processing Site	P1	Not Selected	CP-7 (1)(2)(3)(5)	CP-7 (1)(2)(3)(4)(5)
CP-8	Telecommunications Services	P1	Not Selected	CP-8 (1)(2)	CP-8 (1)(2)(3)(4)
CP-9	Information System Backup	P1	CP-9	CP-9 (1)	CP-9 (1)(2)(3)
CP-10	Information System Recovery and Reconstitution	P1	CP-10	CP-10 (2)(3)	CP-10 (2)(3)(4)
Identification and Authentication					
IA-1	Identification and Authentication Policy and Procedures	P1	IA-1	IA-1	IA-1
IA-2	Identification and Authentication (Organizational Users)	P1	IA-2 (1)	IA-2 (1)(2)(3)(8)	IA-2 (1)(2)(3)(4)(8)(9)
IA-3	Device Identification and Authentication	P1	Not Selected	IA-3	IA-3
IA-4	Identifier Management	P1	IA-4	IA-4	IA-4
IA-5	Authenticator Management	P1	IA-5 (1)	IA-5 (1)(2)(3)	IA-5 (1)(2)(3)
IA-6	Authenticator Feedback	P1	IA-6	IA-6	IA-6
IA-7	Cryptographic Module Authentication	P1	IA-7	IA-7	IA-7
IA-8	Identification and Authentication (Non-Organizational Users)	P1	IA-8	IA-8	IA-8

Control Number	Control Name	Priority	Control Baselines		
			Low	Moderate	High
Incident Response					
IR-1	Incident Response Policy and Procedures	P1	IR-1	IR-1	IR-1
IR-2	Incident Response Training	P2	IR-2	IR-2	IR-2 (1)(2)
IR-3	Incident Response Testing and Exercises	P2	Not Selected	IR-3	IR-3 (1)
IR-4	Incident Handling	P1	IR-4	IR-4 (1)	IR-4 (1)
IR-5	Incident Monitoring	P1	IR-5	IR-5	IR-5 (1)
IR-6	Incident Reporting	P1	IR-6	IR-6 (1)	IR-6 (1)
IR-7	Incident Response Assistance	P3	IR-7	IR-7 (1)	IR-7 (1)
IR-8	Incident Response Plan	P1	IR-8	IR-8	IR-8
Maintenance					
MA-1	System Maintenance Policy and Procedures	P1	MA-1	MA-1	MA-1
MA-2	Controlled Maintenance	P2	MA-2	MA-2 (1)	MA-2 (1)(2)
MA-3	Maintenance Tools	P2	Not Selected	MA-3 (1)(2)	MA-3 (1)(2)(3)
MA-4	Non-Local Maintenance	P1	MA-4	MA-4 (1)(2)	MA-4 (1)(2)(3)
MA-5	Maintenance Personnel	P1	MA-5	MA-5	MA-5
MA-6	Timely Maintenance	P1	Not Selected	MA-6	MA-6
Media Protection					
MP-1	Media Protection Policy and Procedures	P1	MP-1	MP-1	MP-1
MP-2	Media Access	P1	MP-2	MP-2 (1)	MP-2 (1)
MP-3	Media Marking	P1	Not Selected	MP-3	MP-3
MP-4	Media Storage	P1	Not Selected	MP-4	MP-4
MP-5	Media Transport	P1	Not Selected	MP-5 (2)(4)	MP-5 (2)(3)(4)
MP-6	Media Sanitization	P1	MP-6	MP-6	MP-6 (1)(2)(3)

Control Number	Control Name	Priority	Control Baselines		
			Low	Moderate	High
Physical and Environmental Protection					
PE-1	Physical and Environmental Protection Policy and Procedures	P1	PE-1	PE-1	PE-1
PE-2	Physical Access Authorizations	P1	PE-2	PE-2	PE-2
PE-3	Physical Access Control	P1	PE-3	PE-3	PE-3 (1)
PE-4	Access Control for Transmission Medium	P1	Not Selected	PE-4	PE-4
PE-5	Access Control for Output Devices	P1	Not Selected	PE-5	PE-5
PE-6	Monitoring Physical Access	P1	PE-6	PE-6 (1)	PE-6 (1)(2)
PE-7	Visitor Control	P1	PE-7	PE-7 (1)	PE-7 (1)
PE-8	Access Records	P3	PE-8	PE-8	PE-8 (1)(2)
PE-9	Power Equipment and Power Cabling	P1	Not Selected	PE-9	PE-9
PE-10	Emergency Shutoff	P1	Not Selected	PE-10	PE-10
PE-11	Emergency Power	P1	Not Selected	PE-11	PE-11 (1)
PE-12	Emergency Lighting	P1	PE-12	PE-12	PE-12
PE-13	Fire Protection	P1	PE-13	PE-13 (1)(2)(3)	PE-13 (1)(2)(3)
PE-14	Temperature and Humidity Controls	P1	PE-14	PE-14	PE-14
PE-15	Water Damage Protection	P1	PE-15	PE-15	PE-15 (1)
PE-16	Delivery and Removal	P1	PE-16	PE-16	PE-16
PE-17	Alternate Work Site	P1	Not Selected	PE-17	PE-17
PE-18	Location of Information System Components	P2	Not Selected	PE-18	PE-18 (1)
PE-19	Information Leakage	P4	Not Selected	Not Selected	Not Selected
Planning					
PL-1	Security Planning Policy and Procedures	P1	PL-1	PL-1	PL-1
PL-2	System Security Plan	P1	PL-2	PL-2	PL-2
PL-3	System Security Plan Update (Withdrawn)	---	---	---	---
PL-4	Rules of Behavior	P1	PL-4	PL-4	PL-4
PL-5	Privacy Impact Assessment	P1	PL-5	PL-5	PL-5
PL-6	Security-Related Activity Planning	P3	Not Selected	PL-6	PL-6

Control Number	Control Name	Priority	Control Baselines		
			Low	Moderate	High
Program Management					
PM-1	Information Security Program Plan	P1	Deployed VA-wide supporting all baselines		
PM-2	Senior Information Security Officer	P1			
PM-3	Information Security Resources	P1			
PM-4	Plan of Action and Milestones Process	P1			
PM-5	Information System Inventory	P1			
PM-6	Information Security Measures of Performance	P1			
PM-7	Enterprise Architecture	P1			
PM-8	Critical Infrastructure Plan	P1			
PM-9	Risk Management Strategy	P1			
PM-10	Security Authorization Process	P1			
PM-11	Mission/Business Process Definition	P1			
Personnel Security					
PS-1	Personnel Security Policy and Procedures	P1	PS-1	PS-1	PS-1
PS-2	Position Categorization	P1	PS-2	PS-2	PS-2
PS-3	Personnel Screening	P1	PS-3	PS-3	PS-3
PS-4	Personnel Termination	P2	PS-4	PS-4	PS-4
PS-5	Personnel Transfer	P2	PS-5	PS-5	PS-5
PS-6	Access Agreements	P3	PS-6	PS-6	PS-6
PS-7	Third-Party Personnel Security	P1	PS-7	PS-7	PS-7
PS-8	Personnel Sanctions	P3	PS-8	PS-8	PS-8
Risk Assessment					
RA-1	Risk Assessment Policy and Procedures	P1	RA-1	RA-1	RA-1
RA-2	Security Categorization	P1	RA-2	RA-2	RA-2
RA-3	Risk Assessment	P1	RA-3	RA-3	RA-3
RA-4	Risk Assessment Update (Withdrawn)	---	---	---	---
RA-5	Vulnerability Scanning	P1	RA-5	RA-5 (1)	RA-5 (1)(2)(3)(4)(5)(7)

Control Number	Control Name	Priority	Control Baselines		
			Low	Moderate	High
System and Services Acquisition					
SA-1	System and Services Acquisition Policy and Procedures	P1	SA-1	SA-1	SA-1
SA-2	Allocation of Resources	P1	SA-2	SA-2	SA-2
SA-3	Life Cycle Support	P1	SA-3	SA-3	SA-3
SA-4	Acquisitions	P1	SA-4	SA-4 (1)(4)	SA-4 (1)(2)(4)
SA-5	Information System Documentation	P2	SA-5	SA-5 (1)(3)	SA-5 (1)(2)(3)
SA-6	Software Usage Restrictions	P1	SA-6	SA-6	SA-6
SA-7	User-Installed Software	P1	SA-7	SA-7	SA-7
SA-8	Security Design Principles	P1	Not Selected	SA-8	SA-8
SA-9	External Information System Services	P1	SA-9	SA-9	SA-9
SA-10	Developer Configuration Management	P1	Not Selected	SA-10	SA-10
SA-11	Developer Security Testing	P2	Not Selected	SA-11	SA-11
SA-12	Supply Chain Protection	P1	Not Selected	Not Selected	SA-12
SA-13	Trustworthiness	P1	Not Selected	Not Selected	SA-13
SA-14	Critical Information System Components	P4	Not Selected	Not Selected	Not Selected
System and Communications Protection					
SC-1	System and Communications Protection Policy and Procedures	P1	SC-1	SC-1	SC-1
SC-2	Application Partitioning	P1	Not Selected	SC-2	SC-2
SC-3	Security Function Isolation	P1	Not Selected	Not Selected	SC-3
SC-4	Information in Shared Resources	P1	Not Selected	SC-4	SC-4
SC-5	Denial of Service Protection	P1	SC-5	SC-5	SC-5
SC-6	Resource Priority	P4	Not Selected	Not Selected	Not Selected
SC-7	Boundary Protection	P1	SC-7	SC-7 (1)(2)(3)(4)(5)(7)	SC-7 (1)(2)(3)(4)(5)(6)(7)(8)
SC-8	Transmission Integrity	P1	Not Selected	SC-8 (1)	SC-8 (1)
SC-9	Transmission Confidentiality	P1	Not Selected	SC-9 (1)	SC-9 (1)
SC-10	Network Disconnect	P2	Not Selected	SC-10	SC-10
SC-11	Trusted Path	P4	Not Selected	Not Selected	Not Selected
SC-12	Cryptographic Key Establishment and Management	P1	SC-12	SC-12	SC-12 (1)
SC-13	Use of Cryptography	P1	SC-13	SC-13	SC-13
SC-14	Public Access Protections	P1	SC-14	SC-14	SC-14

Control Number	Control Name	Priority	Control Baselines		
			Low	Moderate	High
System and Communications Protection					
SC-15	Collaborative Computing Devices	P1	SC-15	SC-15	SC-15
SC-16	Transmission of Security Attributes	P4	Not Selected	Not Selected	Not Selected
SC-17	Public Key Infrastructure Certificates	P1	Not Selected	SC-17	SC-17
SC-18	Mobile Code	P1	Not Selected	SC-18	SC-18
SC-19	Voice Over Internet Protocol	P1	Not Selected	SC-19	SC-19
SC-20	Secure Name/Address Resolution Service (Authoritative Source)	P1	SC-20 (1)	SC-20 (1)	SC-20 (1)
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	P1	Not Selected	Not Selected	SC-21
SC-22	Architecture and Provisioning for Name/Address Service	P1	Not Selected	SC-22	SC-22
SC-23	Session Authenticity	P1	Not Selected	SC-23	SC-23
SC-24	Fail in Known State	P1	Not Selected	Not Selected	SC-24
SC-25	Thin Nodes	P4	Not Selected	Not Selected	Not Selected
SC-26	Honeypots	P4	Not Selected	Not Selected	Not Selected
SC-27	Operating System-Independent Applications	P4	Not Selected	Not Selected	Not Selected
SC-28	Protection of Information at Rest	P1	Not Selected	SC-28	SC-28
SC-29	Heterogeneity	P4	Not Selected	Not Selected	Not Selected
SC-30	Virtualization Techniques	P4	Not Selected	Not Selected	Not Selected
SC-31	Covert Channel Analysis	P4	Not Selected	Not Selected	Not Selected
SC-32	Information System Partitioning	P1	Not Selected	SC-32	SC-32
SC-33	Transmission Preparation Integrity	P4	Not Selected	Not Selected	Not Selected
SC-34	Non-Modifiable Executable Programs	P4	Not Selected	Not Selected	Not Selected

Control Number	Control Name	Priority	Control Baselines		
			Low	Moderate	High
System and Information Integrity					
SI-1	System and Information Integrity Policy and Procedures	P1	SI-1	SI-1	SI-1
SI-2	Flaw Remediation	P1	SI-2	SI-2 (2)	SI-2 (1) (2)
SI-3	Malicious Code Protection	P1	SI-3	SI-3 (1)(2)(3)	SI-3 (1)(2)(3)
SI-4	Information System Monitoring	P1	Not Selected	SI-4 (2)(4)(5)(6)	SI-4 (2)(4)(5)(6)
SI-5	Security Alerts, Advisories, and Directives	P1	SI-5	SI-5	SI-5 (1)
SI-6	Security Functionality Verification	P1	Not Selected	Not Selected	SI-6
SI-7	Software and Information Integrity	P1	Not Selected	SI-7 (1)	SI-7 (1)(2)
SI-8	Spam Protection	P1	Not Selected	SI-8	SI-8 (1)
SI-9	Information Input Restrictions	P2	Not Selected	SI-9	SI-9
SI-10	Information Input Validation	P1	Not Selected	SI-10	SI-10
SI-11	Error Handling	P2	Not Selected	SI-11	SI-11
SI-12	Output Handling and Retention	P2	SI-12	SI-12	SI-12
SI-13	Predictable Failure Prevention	P4	Not Selected	Not Selected	Not Selected

2. SECURITY CONTROLS

The control tables located within each family in this next section are based on the current version of SP 800-53 and provide specific controls outlined in Table 1: Security Controls Baselines of this Appendix. Subsequent paragraphs following each control table provide supplemental information/details for meeting NIST controls in addition to VA specific requirements for that particular control family.

a. Access Control (AC)

(1) AC-1: Access Control Policy and Procedures

VA OIT in this Appendix has outlined VA’s system security controls based on the current version of SP 800-53 that are required for the effective implementation of the Access Control family. Local SOPs should be developed to facilitate the implementation and management of

these controls at the local level, as needed. The Access controls and procedures in this Appendix are consistent with applicable laws: Executive Orders, policies, regulations, standards, and guidance, and will be periodically reviewed, and, updated when necessary ([See Attachment 2](#)).

(2) **AC-2: Account Management (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
Operating Units manage information system accounts, including: <ul style="list-style-type: none"> • Identifying account types (i.e., individual, group, system, application, and temporary); • Establishing conditions for group membership; • Identifying authorized users of the information system and specifying access privileges; • Requiring appropriate approvals for requests to establish accounts; • Establishing, activating, modifying, disabling, and removing accounts; • Prohibiting the use of shared and guest/generic/anonymous accounts on VA systems and specifically authorizing and monitoring the use of temporary accounts; • Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes; • Terminating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users immediately; • Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by VA or associated missions/business functions; and • Reviewing accounts (See Attachment 2). 	X	X	X
(1) OIT employs automated mechanisms to support the management of information system accounts.	Not Selected	X	X
(2) OIT ensures information systems automatically terminate temporary and emergency accounts (See Attachment 3).	Not Selected	X	X
(3) OIT ensures information systems automatically disable inactive accounts (See Attachment 2).	Not Selected	X	X
(4) OIT employs automated mechanisms to audit account creation, modification, disabling, and termination actions and notify, as required, appropriate individuals.	Not Selected	X	X
Baseline allocation summary	AC-2	AC-2 (1)(2)(3)(4)	AC-2 (1)(2)(3) (4)

For all system impact levels (low, moderate, and high), OIT will manage information system accounts by ensuring the following:

- (a) The local CIO or designee will be able to provide, when required, a current list of approved and authorized system users and their access.
- (b) Operating Units must grant access to information systems based on a valid need-to-know that is determined by assigned official duties that satisfy all personnel security criteria and intended system usage.
- (c) The supervisor and application coordinator responsible for the user will determine the appropriate menus, when applicable. The supervisor will also determine any other programs or access required by the user and coordinate with OIT. Responsibility and authorization for the creation or modification of application menus and system access within the systems will be under the control of the local CIO or designee.
- (d) The ISO will review/concur/non-concur with requests for VA systems access by users based on whether the approval of a higher level official within the requestor's facility or Operating Unit is in place and that the individuals have met the requirements to access VA's systems (security awareness training, signed ROB, and background screening requirements). The decision to provide access to the system remains with the system owner. The Operating Unit will implement a process for secure distribution of security codes. Options include but are not limited to providing the user his/her code in person or through FIPS 140-2 (or its successor) validated encrypted e-mail.
- (e) Requests for access to remote systems must be approved by the user's supervisor and submitted to the ISO for processing.
- (f) Requests for access by contractors will be submitted in writing to the ISO from the CO or the COR to include the user's name, service, phone number, mail code, and purpose for access.
- (g) In the event that temporary access is required (i.e., OIG, Joint Commission on Accreditation of Healthcare Organizations) access will be provided and an automatic termination date established to ensure the account is terminated appropriately.
- (h) The local CIO and the ISO must approve specific user actions that can be performed on the information systems without appropriate identification and authentication (i.e., service accounts, site-to-site VPN accounts, training accounts in test system).
- (i) In the event of an emergency, emergency access to VA sensitive information will be granted in accordance with contingency procedures. These accounts will be terminated immediately upon conclusion of the emergency situation.
- (j) Account management is a process whereby VA Operating Units manage and maintain system accounts throughout their life cycle. VA Operating Units must ensure that their local account management SOP(s) includes:

1. Identification of account types (i.e., individual, group, and system) and establishment of conditions for group membership, and assignment of associated authorizations;

2. Identification of authorized users of the information system and specified access rights/privileges;

3. Identification of access granted to the user based on:

a. A valid need-to-know that is determined by assigned official duties and satisfying all personnel security criteria; and

b. Intended system usage.

4. Account creation and distribution procedures, including procedures for supervisor account request and approval;

5. Procedures and timeframes to notify account managers when information system users are terminated or transferred. Account managers should also be notified when users' information system usage or need-to-know changes;

6. Procedures to terminate, disable, or otherwise secure accounts to occur within 24 hours of notification of a change in user status such as:

a. Departs the agency voluntarily or involuntarily;

b. Transfers to another office within VA;

c. Is suspended;

d. Goes on long term detail; or

e. Information system usage or need-to-know changes.

7. Procedures and timeframe for the review and auditing of accounts (i.e., Federal employee, contractor).

(3) AC-3: Access Enforcement (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
Information system enforces approved authorizations for logical access to the system in accordance with applicable VA policy.	X	X	X
Baseline allocation summary	AC-3	AC-3	AC-3

OIT will ensure information systems enforce assigned authorizations for controlling access to the system. This control can be accomplished by employing access control policies (e.g., identity based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. In addition to controlling access at the information system level, access enforcement mechanisms will be applied at the application level, when necessary, to provide increased information security for VA. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used will be FIPS 140-2 (or its successor) validated. Additional guidance is available in the current version of SP 800-53.

(4) AC-4: Information Flow Enforcement (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
Information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.	Not Selected	X	X
Baseline allocation summary	Not Selected	AC-4	AC-4

Information flow control regulates where information is allowed to travel within or between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. A few examples of flow control restrictions include: keeping export controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within VA, and not passing any web requests to the Internet that are not from the internal web proxy. Information flow control policies and enforcement mechanisms are commonly employed to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that use rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or provide message-filtering capability based on content (e.g., using key word searches or document characteristics).

(5) **AC-5: Separation of Duties (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT separates duties of individuals as necessary, to prevent malevolent activity without collusion; documents separation of duties; and implements separation of duties through assigned information system access authorizations.	Not Selected	X	X
Baseline allocation summary	Not Selected	AC-5	AC-5

(a) Examples of separation of duties include: (i) mission functions and distinct information system support functions for division among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, programming, configuration management, quality assurance and testing, network security); (iii) personnel who approve accounts but do not administer audit functions; and (iv) different administrator accounts for different roles.

(b) Users requiring elevated privileges to VA systems (privileged users) will follow OIT’s approved process. The requirements and approved process document is available on OIS’s portal or from the local ISO or CIO.

(c) Privileged users may include, but are not limited to, system managers, network administrators, and others which allow elevated or unrestricted access, access not normally provided to the general end user of a system. For example, users with access rights or permissions that allows a user to access system control, monitoring, or administration functions on the IT system. This includes functions such as installing, upgrading, or removing system software.

(d) Privileged users must not misuse their authority by viewing or modifying anyone else’s files and/or mail messages.

(e) Privileged users are prohibited from reviewing or accessing individual accounts or devices for investigations or reviews requested by local management unless authorized in writing or e-mail by appropriate senior management officials and the ISO. OIT continuous monitoring reviews/activities of the system and OIG audits/reviews are examples of activities that do not require this additional management approval.

(f) Privileged users should not use their elevated privilege accounts to conduct routine activities. A separate account must be established and used for actions requiring elevated privileges.

(g) Access control software should be in place to limit individual authority and information access, whereby the collusion of two or more individuals is required to commit fraudulent activity.

(h) Job descriptions should reflect accurately the assigned duties and responsibilities that support separation of duties.

(i) Supervisors must analyze the duties performed by their employees to ensure separation of duties and verify that users only have the system privileges that are needed to perform their assigned duties (least privilege). The ISO will monitor compliance with separation of duties and confirm appropriate actions taken to correct any conflicts. This type of control must ensure that a single individual cannot subvert a critical process. Supervisors should ensure that a single individual does not perform combinations of functions including, but not limited to:

1. Data entry and verification of data;
2. Data entry and its reconciliation to output;
3. Input of transactions that may result in a conflict of interest, fraud, or abuse (e.g., input of vendor invoices and purchasing and receiving information); and
4. Data entry and approval functions.

(j) Some examples of this principle include: The same individual should not enter and authorize a purchase order; the same individual should not request a user account or create the account in the system; the system administrator should not be the one to conduct the audits/reviews of the system he/she is administering; and the ISO should not be a system administrator.

(6) **AC-6: Least Privilege (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT employs the concept of least privilege, allowing only authorized access for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with VA missions and business functions.	Not Selected	X	X
(1) OIT explicitly authorizes access to <u>security functions and security-relevant information</u> (See Attachment 3).	Not Selected	X	X
(2) OIT requires that users of information system accounts, or roles, with access to <u>security functions and security-relevant information</u> use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions (See Attachment 3).	Not Selected	X	X
Baseline allocation summary	Not Selected	AC-6 (1)(2)	AC-6 (1)(2)

(a) OIT employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to VA operations and assets, individuals, and other organizations.

(b) Each user or process will be assigned the most restrictive set of privileges needed for the performance of authorized tasks. See **AC-5: Separation of Duties**.

(7) **AC-7: Unsuccessful Login Attempts (P2)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system: <ul style="list-style-type: none"> Enforces a limit of consecutive invalid login attempts by a user during a time period (See Attachment 3); and Automatically takes action when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection (See Attachment 3). 	X	X	X
Baseline allocation summary	AC-7	AC-7	AC-7

(a) Due to the potential for DoS attacks, automatic lockouts by information systems should be temporary and automatically release after the specified predetermined time period.

(b) This control applies to all IT resources owned or used by VA with capabilities for account lockout (including those that may require supplementary software to add this

capability). The control applies to all accesses other than those accesses explicitly identified and documented by VA in **AC-14: Permitted Actions Without Identification or Authentication**.

(c) Locked accounts with privileged access (i.e., root or administrator access) will remain locked until unlocked by the Help Desk or other authorized account management personnel.

(8) **AC-8: System Use Notification (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
<p>The information system:</p> <ul style="list-style-type: none"> • Displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable Federal laws, Executive Orders, policies, regulations, standards, and guidance and states that: (i) users are accessing a U.S. Government information system; (ii) system usage may be monitored, recorded, and subject to audit; (iii) unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) use of the system indicates consent to monitoring and recording; • Retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and • For publicly accessible systems: (i) displays the system use information when appropriate, before granting further access; (ii) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) includes in the notice given to public users of the information system, a description of the authorized uses of the system. 	X	X	X
Baseline allocation summary	AC-8	AC-8	AC-8

(a) The local CIO will coordinate with the system managers, and other OIT personnel to ensure that VA approved logon warning banners are deployed on VA computer systems, including servers, workstations, routers, switches, and other devices that can accommodate VA approved banner within their area of responsibility. As part of the annual FISMA review, the ISO will ensure all capable equipment displays the warning banner.

(b) System use notification is intended only for information system access that includes an interactive log in interface with a human user and is not intended to require notification when an interactive interface does not exist.

(c) The System Owner or local CIO must select and configure the operating system to display a warning banner screen (or close approximation) at log in, and require users to electronically acknowledge the warning (such as clicking an “OK” or “I agree” button to proceed).

(d) The following banner has been approved by VA and should be used when technically possible:

“This U.S government system is intended to be used by [authorized VA network users] for viewing and retrieving information only, except as otherwise explicitly authorized. VA information resides on and transmits through computer systems and networks funded by VA. All use is considered to be with an understanding and acceptance that there is no reasonable expectation of privacy for any data or transmissions on Government Intranet or Extranet (non-public) networks or systems. All transactions that occur on this system and all data transmitted through this system are subject to review and action including (but not limited to) monitoring, recording, retrieving, copying, auditing, inspecting, investigating, restricting access, blocking, tracking, disclosing to authorized personnel, or any other authorized actions by all authorized VA and law enforcement personnel. All use of this system constitutes understanding and unconditional acceptance of these terms.

Unauthorized attempts or acts to either (1) access, upload, change, or delete information on this system, (2) modify this system, (3) deny access to this system, or (4) accrue resources for unauthorized use on this system are strictly prohibited. Such attempts or acts are subject to action that may result in criminal, civil, or administrative penalties.”

(9) AC-9: Previous Logon (Access) Notification (P4)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system notifies the user, upon successful logon (access), of the date and time of the last logon (access).	Not Selected	Not Selected	Not Selected
Baseline allocation summary	Not Selected	Not Selected	Not Selected

(a) This control is intended to cover both traditional logons to information systems and general access to information systems that occur in other types of architectural configurations (e.g., service oriented architectures).

(b) VA does not require, at this time, application of **AC-9: Previous Logon (Access) Notification**. OIT may, at their discretion and the system's capability, elect to ensure that information systems notify the user, upon successful logon, of the date and time of the last logon, and the number of unsuccessful logon attempts since the last successful logon.

(10) **AC-10: Concurrent Session Control (P2)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system limits the number of concurrent sessions for each system account to a maximum number of sessions (See Attachment 3).	Not Selected	Not Selected	X
Baseline allocation summary	Not Selected	Not Selected	AC-10

Certain roles and situations may require multiple concurrent sessions. These are handled on a case-by-case basis, and should include justification and concurrence by designated ISO and the local CIO with the exception of users that require multiple concurrent sessions to use the graphical user interface and other software packages simultaneously. Exceptions should be documented in the SSP.

(11) **AC-11: Session Lock (P3)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system: <ul style="list-style-type: none"> Prevents further access to the system by initiating a session lock after a specified number of minutes of inactivity or upon receiving a request from a user (See Attachment 3). Retains the session lock until the user reestablishes access using established identification and authentication procedures. 	Not Selected	X	X
Baseline allocation summary	Not Selected	AC-11	AC-11

A session lock is not a substitute for logging out of the information system when OIT requires users to logout at the end of the workday.

(12) **AC-12: Session Termination**

Withdrawn from SP 800-53, Rev. 3, and incorporated into **SC-10: Network Disconnect** control.

(13) **AC-13: Supervision and Review – Access Control**

Withdrawn from SP 800-53, Rev. 3, and incorporated into **AC-2: Account Management** and **AU-6: Audit Review, Analysis, And Reporting**.

(14) **AC-14: Permitted Actions Without Identification or Authentication (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The System Owner: <ul style="list-style-type: none"> Identifies specific user actions that can be performed on the information system without identification or authentication. Documents and provides supporting rationale in the security plan for the information system, including user actions not requiring identification and authentication. 	X	X	X
(1) The System Owner permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission/business objectives.	Not Selected	X	X
Baseline allocation summary	AC-14	AC-14 (1)	AC-14 (1)

(a) This control is intended for those specific instances where a System Owner determines that no identification and authentication is required. It is not, however, mandating that such instances exist in given information systems.

(b) System Owners may allow a limited number of user actions without identification and authentication (e.g., when individuals access public Web sites or other publicly accessible Federal information systems).

(c) In the event of non-routine circumstances (emergency) in which the employee possesses VA sensitive information and is not available, management officials may review an account or device as part of their supervisory responsibilities with local senior management approval. The following procedures have been established for obtaining such access:

1. Submit a request for access to a user’s account or device to the ISO and include, at a minimum, the following information: first and last name of user; username (account name); justification for access; location of files; location to save the files (i.e., supervisor’s drive or CD); and duration of review.

2. Upon approval from the designated supervisor/manager, the ISO will coordinate requested access with the local CIO. The ISO will not be the recipient of user’s individual files from a facility storage device.

3. Audit logging for all activities related to this emergency access request is required and must be protected and saved.

4. Emergency access must specify the person authorized to access the account. Under no circumstance will the unavailable individual's logon identifier or password be used or compromised during emergency access.

5. The system administrator will rewrite the access rules to give the manager or designee access to the information (files).

6. Upon completion of the emergency access, all access to the information will be returned to the original state.

7. It is the responsibility of the user's supervisor/manager or designee to notify the unavailable individual of the emergency access as soon as the user becomes available.

(15) **AC-15: Automated Marking**

Withdrawn from SP 800-53, Rev. 3 and incorporated into **MP-3: Media Marking** control.

(16) **AC-16: Security Attributes**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system supports and maintains the binding of (organizationally defined security attributes) to information in storage, in process, and in transmission.	Not Selected	Not Selected	Not Selected
Baseline allocation summary	Not Selected	Not Selected	Not Selected

VA does not require, at this time, application of control **AC-16: Security Attributes**. OIT, may, at their discretion, elect to ensure that information systems appropriately support and maintain the binding of security attributes and settings.

(17) **AC-17: Remote Access (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT documents allowed methods of remote access to the information system; establishes usage restrictions and implementation guidance for each allowed remote access method; monitors for unauthorized remote access to the information system; authorizes remote access to the information system prior to connection; and enforces requirements for remote connections to the information system.	X	X	X
(1) OIT employs automated mechanisms to facilitate the monitoring and control of remote access methods.	Not Selected	X	X
(2) OIT uses encryption to protect the confidentiality and integrity of remote access sessions.	Not Selected	X	X
(3) OIT ensures the information system routes all remote accesses through a limited number of managed access control points.	Not Selected	X	X
(4) OIT authorizes the executing of privileged commands and access to security-relevant information via remote access only for compelling operational needs and documents the rationale for such access in the security plan for the information system.	Not Selected	X	X
(5) OIT monitors for unauthorized remote connections to the information system and takes appropriate action if an unauthorized connection is discovered (See Attachment 2).	Not Selected	X	X
(7) OIT ensures that remote sessions for accessing specified security functions and security-relevant information automatically employ additional security measures and are audited (See Attachment 2).	Not Selected	X	X
(8) OIT disables networking protocols within the information system deemed to be non-secure except for explicitly identified components in support of specific operational requirements (See Attachment 2).	Not Selected	X	X
Baseline allocation summary	AC-17	AC-17 (1)(2)(3)(4)(5) (7)(8)	AC-17 (1)(2)(3)(4) (5)(7)(8)

(a) Remote access is any access to a VA information system by a user (or process acting on behalf of a user) communicating through an external network (e.g., the Internet). Examples of remote access include dial-up, broadband, and wireless (see **AC-18: Wireless Access**).

(b) Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access.

(c) Only VA authorized users may remotely access VA-owned equipment used to process VA information or access VA processing services.

(d) Users will utilize VA approved technologies for remote access.

(e) Users can access VA systems from their residence or while they are on travel status using approved VA GFE or external information systems (formerly known as Other Equipment) when using VA approved technology for both VA GFE and external information systems. Approved remote access users are governed under the same local policies, Federal laws, and regulations that apply to all local users of VA computer systems and the security and privacy of the data contained therein.

(f) Dial-up lines, other than those with FIPS 140-2 (or its successor) validated encryption, will not be used to gain access to a VA information system that processes VA sensitive information unless the local CIO provides specific written authorization. The written authorization must be attached to the SSP or the authorization must be uploaded into the VA approved FISMA database to ensure availability for oversight groups. If modems are approved for systems connected to VA's network, security controls and procedures must be documented and readily available for oversight inspections. If stand-alone system modems are approved, a procedure for remote diagnostics and maintenance of equipment is required and must be tightly controlled. In both cases, event logging functions are to be enabled to provide the review of any suspicious activity. Only remote control software configured and approved by OIT may be used to control VA systems via the LAN, WAN, or remote access. Periodic monitoring will be implemented to ensure that installed equipment does not include unanticipated dial-up capabilities.

(g) Users may transport, transmit, download, or store VA sensitive information on VA owned and approved storage devices/media that are taken outside of VA facilities only when their VA supervisor, and local ISO and CIO approves it or it is documented and approved within a VA contract or agreement. The ISO and local CIO will review the security mechanisms that will be used to ensure that the sensitive data (thumb drive, hard drive, etc.) is encrypted during transit and storage using FIPS 140-2 (or its successor) validated encryption. The approval from the supervisor, ISO, and CIO should be in writing. Use of or access to sensitive information may be revoked, modified, or limited at any time by an employee's VA supervisor or superior to the supervisor. Supervisors should limit the amount of information to be removed to the least amount required.

(h) All relevant MOUs/As, contracts, SOWs, and data use agreements should include assertions that all parties will conform to these remote use policies and procedures as appropriate.

(i) Users will not simultaneously connect to VA and one or more non-VA networks.

(j) Users may not share instructions or information regarding establishing connections to VA private networks and computers with unauthorized personnel. Users may not share remote access log on identifiers, passwords, and other authentication means used specifically to protect VA information or access techniques to VA private networks.

(k) In recognition of users' responsibility to secure and safeguard information from misuse or improper disclosure, all remote access service computer users must provide proper justification of the need for access, and sign the VA National ROB or Contractor ROB prior to remote access being granted.

(l) Responsibility for access to, or training on, systems not covered by this policy lies solely with the individual or service/section requiring this access. Remote access to VA computer systems does not constitute approval for overtime pay or compensatory time if the individual uses the systems outside of normal working hours.

(m) OIT staff is responsible for ensuring that the approved requestor receives instructions on how to setup the device for the required access and for providing any needed assistance. If the remote access user needs assistance with configuration or to determine hardware compatibility, the user should follow local Help Desk procedures.

(n) Requests for remote access from VA personnel will be submitted (using the current VA approved process) to the ISO, and include the user's name, service, phone number, mail code, and purpose for access, and will have the concurrence of a higher level official within the user's facility. When remote access is requested to another facility (other than the one at which the individual normally works), the appropriate documentation will be sent to and coordinated with the remote facility ISO. Codes for authorized remote users will be delivered either electronically using VA approved encryption, or in a sealed envelope, to the remote facility's ISO. The outside of the envelope will be annotated with the user's name and the statement, 'TO BE OPENED BY ADDRESSEE ONLY'. Users should contact their ISO if the envelope is not sealed when delivered.

(o) New users (those who do not have a current VA network account) who request remote access must complete VA approved privacy and information security awareness training, sign the appropriate ROB (employee/contractor), complete the authorization for information system access, and meet the appropriate background screening requirements before access can be granted.

(p) Requests for remote access by contractors will be submitted in writing to the ISO by the CO or the COR or supervisor and will include the user's name, service, phone number, mail code, and purpose for access. The appropriate documentation will be coordinated with the contractor by the CO or COR and ISO. Codes for authorized remote users will be delivered either electronically using encryption or in a sealed envelope, to the ISO or to the CO or COR for distribution to the contractor. Vendors may have a site-to-site VPN connection to VA's network. Requirements for access for a site-to-site VPN connection can be found on VA's Office of Information Security Portal.

(q) Transferring, Retiring, Resigning, Removed, or Discharged Employee: Supervisors will contact the ISO to ensure that remote access privileges are terminated as soon as they are no longer needed; when the account owner transfers out of the supervisor’s office or leaves VA; or when an authorized official determines that remote access privileges should be revoked. Upon termination of required access privileges, supervisors will confirm and notify the ISO and the individual responsible for the equipment inventory listing that the employee has returned all VA GFE related to remote access.

(r) ISOs are responsible for auditing remote access authorizations.

(18) **AC-18: Wireless Access (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT: <ul style="list-style-type: none"> Establishes usage restrictions and implementation guidance for wireless access; Monitors for unauthorized wireless access to the information system; Authorizes wireless access to the information system prior to connection; and Enforces requirements for wireless connections to the information system. 	X	X	X
(1) The information system protects wireless access to the system using authentication and FIPS 140-2 (or its successor) validated encryption. (Authentication applies to user, device, or both as necessary).	Not Selected	X	X
(2) OIT monitors for unauthorized wireless connections to the information system, including scanning for unauthorized wireless access points, and takes appropriate action if an unauthorized connection is discovered (See Attachment 3).	Not Selected	Not Selected	X
(4) OIT does not allow users to independently configure wireless network capabilities.	Not Selected	Not Selected	X
(5) OIT confines wireless communications to VA controlled boundaries.	Not Selected	Not Selected	X
Baseline allocation summary	AC-18	AC-18 (1)	AC-18 (1)(2)(4) (5)

(a) Wireless technologies include, but are not limited to, microwave, satellite, packet radio (UHF/VHF), 802.11x, and Bluetooth.

(b) Wireless scanning is not necessarily limited to only those areas within the facility containing the information systems. It is conducted outside of those areas only as needed to verify that unauthorized wireless access points are not connected to the system.

(c) Actions that may be taken by Operating Units to confine wireless communications to VA-controlled boundaries include:

1. Reducing the power of the wireless transmission such that it cannot transit the physical perimeter of the facility;
2. Employing measures such as TEMPEST to control wireless emanations; and
3. Configuring the wireless access such that it is point-to-point in nature.

(d) Wireless devices must meet and be kept up-to-date on the latest anti-viral and software/security patch remediation, as applicable.

(e) Operating Units must follow VA Directive 6512, *Secure Wireless Technology*, and other wireless configuration and guidance documents as created and posted by OIT.

(19) AC-19: Access Control for Mobile Devices (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT: <ul style="list-style-type: none"> • Establishes usage restrictions and implementation guidance for VA-controlled mobile devices; • Authorizes connection of mobile devices meeting VA usage restrictions and implementation guidance to VA information systems; • Monitors for unauthorized connections of mobile devices to VA information systems. • Enforces requirements for the connection of mobile devices to VA information systems; • Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction; • Issues specially configured mobile devices to individuals traveling to locations that VA deems to be of significant risk; and • Applies inspection and preventative measures to mobile devices returning from locations that VA deems to be of significant risk in accordance with VA policies and procedures (See Attachment 3). 	X	X	X
(1) OIT restricts the use of writable, removable media in VA information systems.	Not Selected	X	X
(2) OIT prohibits the use of personally owned, removable media in VA information systems.	Not Selected	X	X
(3) OIT prohibits the use of removable media in VA information systems when the media has no identifiable owner.	Not Selected	X	X
Baseline allocation summary	AC-19	AC-19 (1)(2)(3)	AC-19 (1)(2)(3)

(a) Mobile devices include portable cartridge/disk-based, removable storage media (e.g., floppy disks, CDs, USB flash drives, external hard drives, and other flash memory cards/drives that contain non-volatile memory). Mobile devices also include portable computing and communications devices with information storage capability (e.g., notebook/laptop computers, PDAs, cellular telephones, digital cameras, and audio recording devices).

(b) The local CIO and supervisors must authorize the use of portable, mobile, and wireless devices within their Operating Unit prior to their implementation.

(c) All VA employees must have documented permission from their supervisor to store VA sensitive information on a mobile device. The ISO and local CIO must approve and document that the mobile device to be used meets VA's security requirements.

(d) In order to ensure the protection of VA information, VA mobile devices will be encrypted using FIPS 140-2 (or its successor) validated encryption, if technically possible. If not technically possible, the documented justification and review/approval by the local ISO and CIO is required. The DAS for OIS or designee must also review/approve VA mobile devices that cannot be encrypted using FIPS 140-2 (or its successor) validated encryption. The local ISO will maintain the original and a copy of the document will be provided to the CIO. If the mobile device is a laptop used as a medical device (see paragraph (f) below).

(e) Similarly storage media such as CDs/DVDs that contain VA sensitive information must be adequately protected using FIPS 140-2 (or its successor) validated encryption, when possible. The CIO should consult OIT management for applicable VA approved tools for encrypting CDs. The same documented justification and review/approval by the local ISO and CIO and the DAS for OIS is required if CDs/DVDs cannot be encrypted, unless the CDs/DVDs are covered by the mailing exceptions that are outlined in the VA ROB and are mailed according to the policy outlined in VA Directive 6609. Per VA Directive 6609, the following types of information are excluded from the encryption requirement when mailed according to the requirements outlined in the directive:

1. Information containing the SPI of a single individual to:

a. That person (e.g., the Veteran's, beneficiary's, dependent's, or employee's own information) or to that person's legal representative (e.g., guardian, attorney-in-fact, attorney, or Veteran Service Organization). Such information may be mailed to an entity, not otherwise the subject of an exception, with the express written consent of the individual. Such information may be mailed via U.S. Postal Service regular mail unless tracked delivery service is requested and paid for by the recipient;

b. A business partner such as a health plan or insurance company, after considering potential risk;

c. A court, adjudicative body, parties in litigation, or to persons or entities in the course of a judicial or administrative proceeding; and

d. Congress, law enforcement agencies, and other governmental entities.

2. Information containing SPI of one or more individuals to a person or entity that does not have the capability to decrypt information that is encrypted by VA, when sent according to VA Directive 6609.

(f) All VA owned laptops, regardless of location, must have VA approved FIPS 140-2 (or its successor) validated encryption, if technically possible. If encryption does not allow a laptop used as a medical device to function as required the justification and review/approval by the VISN Biomedical Engineer (or VISN Biomedical Engineering Point of Contact), the local Healthcare Technical Management (HTM), Health Information Security Division (HISD), the Deputy Under Secretary for Health for Operations and Management and the DAS for OIS should be documented and maintained by HTM with a copy provided to HISD and the local ISO. Any laptops other than medical devices that cannot be encrypted must have documented local ISO and CIO approval as well as the DAS for OIS. The local ISO will maintain the original and a copy of the document will be provided to the CIO.

(g) Utilization of non-VA approved USB thumb drives on VA systems is prohibited. FIPS 140-2 (or its successor) validated USB thumb drives are required.

(h) Non- VA personnel (i.e., contractors, business partners) must furnish their own FIPS 140-2 (or its successor) validated USB thumb drives that conform to the published listing of VA approved USB thumb drives. Further, permission must be obtained from a designated VA supervisor before they can be utilized within the Department.

(i) Portable and mobile devices are not allowed access to any VA network without first meeting VA and the facility's security policies, procedures, and configuration standards. These include (when technically possible) scanning the devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless).

(j) Mobile, portable, and wireless devices will follow VA policy regarding system hardware and electronic media sanitization and disposal.

(k) For VA staff required to travel outside the US for VA business, OIT must provide them the necessary mobile devices that:

1. Have been sanitized to remove any existing VA information;
2. Have limited applications installed;
3. Have the most stringent configuration settings possible that still allow the user to perform their required duties; and
4. Are encrypted with FIPS 140-2 (or its successor) validated encryption.

(20) **AC-20: Use of External Information Systems (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: <ul style="list-style-type: none"> • Access the information system from the external information systems; and • Process, store, and transmit VA information using the external information systems. 	X	X	X
(1) OIT permits authorized individuals to use an external information system to access VA's information systems or to process, store, or transmit VA sensitive information only when OIT: <ul style="list-style-type: none"> • Can verify the implementation of required security controls on the external system as specified in the VA information security policy and the security plan; or • Has approved information system connection or processing agreements with the organization hosting the external information system. 	Not Selected	X	X
(2) OIT limits the use of VA portable storage media by authorized individuals on external information systems.	Not Selected	X	X
Baseline allocation summary	AC-20	AC-20 (1)(2)	AC-20 (1)(2)

(a) Authorized individuals in this control include VA employees, contractors working under an approved contract, business associates working under approved business associate agreements and others that have been authorized by VA to access VA information systems or VA sensitive information. These individuals have completed the security requirements for access to VA systems or VA sensitive information.

(b) External information systems are information systems or components of information systems that are outside of the authorization boundary established by VA and for which VA typically has no direct supervision and authority over the application of required security controls or the assessment of security control effectiveness. External information systems include, but are not limited to:

1. Personally owned information systems (e.g., computers, cellular telephones, or PDA);
2. Privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports);
3. Information systems owned or controlled by non-Federal Government organizations (such as VA affiliate's information systems); and

4. Federal information systems that are not owned, operated, or under the direct supervision and authority of VA.

(c) Per 1, first bullet in the NIST box above, verification of the implementation of required security controls on some external systems can be accomplished by reviewing the external system's A&A (formerly C&A) documents (e.g., other Federal agency) or by using other VA developed and approved processes to ensure appropriate security controls are implemented on the external system. The DAS for Information Security or designee will review these documents. Other VA approved processes for verification will be developed/utilized as appropriate, such as VA oversight reviews or self-assessments.

(d) Per 1, second bullet in the NIST box above, security controls/requirements for external information systems that process, store, or transmit VA sensitive information should be documented in a VA approved MOU/ISA, VA contract or other VA approved agreement (e.g., Data Use Agreement). See VA Directive 6513, *Secure External Connections*, and VA Handbook 6500.6. Remote access for individuals is covered under **AC-17: Remote Access**.

(e) For contractors and business partners, the use of external systems including removable storage devices to store VA sensitive information must be included in the appropriate contracts or agreements. The appropriate security requirements required for these systems will be covered in the contract or other approved agreement.

(f) ISOs and local CIOs should monitor the approved agreements within their facility on a yearly basis to ensure the agreements are still valid and the need still exists.

(g) Local CIOs should approve (through their formal management chain, as required) and maintain a list of all authorized external information systems connected to VA's network (both internally and remotely) and those approved through the agreements outlined in (d) above for their area of responsibility.

(h) Other systems (systems maintained by contractors or others) must meet the security requirements as outlined in the contract and/or other VA approved agreements.

(i) This control does not apply to the use of external information systems to access public interfaces to VA information systems and information (e.g., individuals accessing Federal information through www.usa.gov etc.).

(j) Personally owned information systems (capable of storing data) used on-site at a VA facility to connect to VA's network or to perform assigned official duties must be approved by the local CIO.

(21) **AC-21: User-Based Collaboration and Information Sharing (P4)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
VA: <ul style="list-style-type: none"> 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 (VA defined circumstances); and Employs (VA list of sharing circumstances and automated mechanisms or manual processes required) to assist users in making information sharing/collaboration decisions. 	Not Selected	Not Selected	Not Selected
Baseline allocation summary	Not Selected	Not Selected	Not Selected

VA does not require, at this time, application of **Control AC-21: User-Based Collaboration and Information Sharing**. OIT, may, at their discretion, elect to implement this control.

(22) **AC-22: Publicly Accessible Content (P2)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
VA: <ul style="list-style-type: none"> Designates individuals authorized to post information onto a VA information system that is publicly accessible; Trains authorized individuals to ensure that publicly accessible information does not contain non-public information; Reviews the proposed content of publicly accessible information for non-public information prior to posting onto VA information system; Reviews the content on the publicly accessible VA information system for non-public information (See Attachment 3); and Removes non-public information from the publicly accessible VA information system, if discovered. 	X	X	X
Baseline allocation summary	AC-22	AC-22	AC-22

Non-public information is any information for which the general public is not authorized access in accordance with Federal laws, Executive Orders, policies, regulations, standards, or guidance. Information protected under the Privacy Act of 1974 and vendor proprietary information are examples of non-public information. This control addresses posting information on a VA information system that is accessible to the general public, typically without identification or authentication.

b. Awareness and Training (AT)

(1) AT-1: Security Awareness and Training Policy and Procedures

VA OIT in this Appendix has outlined VA’s system security controls based on SP 800-53 that are required for the effective implementation of the Awareness and Training family. Local SOPs should be developed to facilitate the implementation and management of these controls at the local level, as needed. The Awareness and Training controls and procedures in this Appendix are consistent with applicable laws: Executive Orders, policies, regulations, standards, and guidance, and will be periodically reviewed, and, when necessary, updated ([See Attachment 2](#)).

(2) AT-2: Security Awareness (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes and annually thereafter. (See Attachment 2).	X	X	X
Baseline allocation summary	AT-2	AT-2	AT-2

VA requires that in addition to users of VA information systems outlined above, users of “VA sensitive information” are also responsible for completing VA approved security awareness training on at least an annual basis. Users of VA information systems or VA sensitive information will receive VA approved training as part of initial training for new users, when required by system changes, and annually thereafter.

(3) AT-3: Security Training (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; (iii) and thereafter. (See Attachment 2).	X	X	X
Baseline allocation summary	AT-3	AT-3	AT-3

Information Technology Workforce Development has developed IT competency modeling for the workforce. Information Assurance is a core competency across the Department (includes annual awareness training and on-going training through such modalities as the Information Security Focus Campaign, Information Protection Week, etc.). Through competency modeling, higher proficiencies (higher level of training) are identified for the Information Assurance competency. These higher levels of required knowledge/skill are added to the identified staff’s (e.g., System Administrators, Network Administrators, Database Administrators) competency profiles and role-based training for “those with significant responsibilities” are incorporated.

(4) **AT-4: Security Training Records**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
VA and OIT: <ul style="list-style-type: none"> Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and Retains individual training records for (See Attachment 2). 	X	X	X
Baseline allocation summary	AT-4	AT-4	AT-4

(5) **AT-5: Contacts with Security Groups and Associations**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
VA establishes and institutionalizes contact with selected groups and associations within the security community: <ul style="list-style-type: none"> To facilitate ongoing security education and training for organizational personnel; To stay up-to-date with the latest recommended security practices, techniques, and technologies; and To share current security-related information including threats, vulnerabilities, and incidents. 	Not Selected	Not Selected	Not Selected
Baseline allocation summary	Not Selected	Not Selected	Not Selected

VA does not require, at this time, application of control **AT-5: Contacts with Security Groups and Associations**. Operating Units may, at their discretion, establish and institutionalize contact with groups and associations within the security community.

c. **Audit and Accountability (AU)**

(1) **AU-1: Audit and Accountability Policy and Procedures**

VA OIT in this Appendix has outlined VA’s system security controls based on the current version of SP 800-53 that are required for the effective implementation of the Audit and Accountability family. Local SOPs should be developed to facilitate the implementation and management of these controls at the local level, as needed. The Audit and Accountability controls and procedures in this Appendix are consistent with applicable laws: Executive Orders, policies, regulations, standards, and guidance, and will be periodically reviewed, and, when necessary, updated [\(See Attachment 2\)](#).

(2) **AU-2: Auditable Events (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT: <ul style="list-style-type: none"> • Determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing events as defined by the System Owner (See Attachment 3); • Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; • Provides a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and • Determines, based on current threat information and ongoing assessment of risk, which events are to be audited within the information system including the frequency of auditing for each event (See Attachment 3). 	X	X	X
(3) OIT reviews and updates the list of auditable events (See Attachment 3).	Not Selected	X	X
(4) OIT includes execution of privileged functions in the list of events to be audited by the information system.	Not Selected	X	X
Baseline allocation summary	AU-2	AU-2 (3)(4)	AU-2 (3)(4)

OIT should, at a minimum, generate audit records for the following events when technically possible: Actions of system administrators and operators; production of printed output; new objects and deletion of objects in user address space; security relevant events; system configuration activities and events; events relating to use of privileges; all events relating to user identification and authentication; and the setting of user identifiers.

(3) **AU-3: CONTENT OF AUDIT RECORDS (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.	X	X	X
(1) The information system includes detailed information in audit records for audit events identified by type, location, or subject (See Attachment 3).	Not Selected	X	X
(2) OIT centrally manages the content of audit records generated by information system components (See Attachment 3).	Not Selected	Not Selected	X
Baseline allocation summary	AU-3	AU-3 (1)	AU-3 (1)(2)

(a) Audit record content that may satisfy the requirement of this control includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

(b) Audit logs will be maintained as follows:

1. Must be sufficient in detail to facilitate reconstruction of events if a compromise or malfunction is suspected or has occurred.

2. Must be treated as restricted information/limited access and protected from unauthorized access, modification, or destruction and reviewed periodically for action. Access to logs must be granted based upon need-to-know and least privilege.

3. Audit logs must be backed up and stored securely.

4. Must be retired according to approved Records Schedule.

(4) **AU-4: Audit Storage Capacity (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The system administrator allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.	X	X	X
Baseline allocation summary	AU-4	AU-4	AU-4

The System Owner considers the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity.

(5) AU-5: Response to Audit Processing Failures (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system: <ul style="list-style-type: none"> Alerts designated OIT officials in the event of an audit processing failure; and Takes one or more of the following actions (See Attachment 3): Either overwrites the oldest audit records, shuts down the system, or stops generating audit records, based on a local risk based decision and documented in the SSP. 	X	X	X
(1) The information system provides a warning when allocated audit record storage volume reaches Operating Unit identified capacity for maximum audit record storage capacity (See Attachment 3).	Not Selected	Not Selected	X
(2) The information system provides a real-time alert when the system administrator defined audit failure events occur. (See Attachment 3).	Not Selected	Not Selected	X
Baseline allocation summary	AU-5	AU-5	AU-5 (1)(2)

Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

(6) AU-6: Audit Review, Analysis, and Reporting (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT: <ul style="list-style-type: none"> Reviews and analyzes information system audit records for indications of inappropriate or unusual activity, and reports findings to designated OIT officials (See Attachment 3); and Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to VA's operations, assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information. 	X	X	X
(1) The information system integrates audit review, analysis, and reporting processes to support VA's processes for investigation and response to suspicious activities.	Not Selected	Not Selected	X
Baseline allocation summary	AU-6	AU-6	AU-6 (1)

(7) **AU-7: Audit Reduction and Report Generation (P2)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system provides an audit reduction and report generation capability.	Not Selected	X	X
(1) The information system provides the capability to automatically process audit records for events of interest based on selectable event criteria.	Not Selected	X	X
Baseline allocation summary	Not Selected	AU-7 (1)	AU-7 (1)

(a) The audit reduction and report generation capability provides support for near real-time audit review, analysis, and reporting requirements described in **AU-6: Audit Review, Analysis, and Reporting** and after-the-fact investigations of security incidents.

(b) Audit reduction and reporting tools do not alter original audit records.

(8) **AU-8: Time Stamps (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system uses internal system clocks to generate time stamps for audit records.	X	X	X
(1) The information system synchronizes internal information system clocks (See Attachment 3).	Not Selected	X	X
Baseline allocation summary	AU-8	AU-8 (1)	AU-8 (1)

Time stamps generated by the information system include both date and time. The time may be expressed in Coordinated Universal Time, a modern continuation of Greenwich Mean Time, or local time with an offset from Coordinated Universal Time.

(9) **AU-9: Protection of Audit Information (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	X	X	X
Baseline allocation summary	AU-9	AU-9	AU-9

Audit information constitutes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity.

(10) **AU-10: Non-Repudiation (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system protects against an individual falsely denying having performed a particular action.	Not Selected	Not Selected	X
Baseline allocation summary	Not Selected	Not Selected	AU-10

Examples of particular actions taken by individuals include creating information, sending a message, approving information (e.g., indicating concurrence or signing a contract), and receiving a message. Non-repudiation protects individuals against later claims by an author of a document as not having authored the document, a sender of not having transmitted a message, a receiver of not having received a message, or a signatory of not having signed a document. Non-repudiation services can be used to determine if information originated from an individual, or if an individual took specific actions (e.g., sending an e-mail, signing a contract, approving a procurement request) or received specific information. Non-repudiation services are obtained by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts).

(11) **AU-11: Audit Record Retention (P3)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT retains audit records to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements (See Attachment 2).	X	X	X
Baseline allocation summary	AU-11	AU-11	AU-11

This includes, for example, retention and availability of audit records relative to Freedom of Information Act requests, subpoena, and law enforcement actions. Standard categorizations of audit records relative to such types of actions and standard response processes for each type of action are developed and disseminated. The National Archives and Records Administration (NARA) General Records Schedules provide Federal policy on record retention.

(12) **AU-12: Audit Generation (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system: <ul style="list-style-type: none"> Provides audit record generation capability for the list of auditable events defined in AU-2: Auditable Events at information system components (See Attachment 3); Allows designated OIT personnel to select which auditable events are to be audited by specific components of the system; and Generates audit records for the list of audited events defined in AU-2: Auditable Events with the content as defined in AU-3: Content of Audit Records. 	X	X	X
(1) The information system compiles audit records from <u>information system components</u> into a system-wide (logical or physical) audit trail that is time correlated to within the <u>level of tolerance for relationship between time stamps of individual records in the audit trail</u> (See Attachment 3).	Not Selected	Not Selected	X
Baseline allocation summary	AU-12	AU-12	AU-12 (1)

(a) Audit records can be generated from various components within the information system. The list of audited events is the set of events for which audits are to be generated. This set of events is typically a subset of the list of all events for which the system is capable of generating audit records (i.e., auditable events).

(b) The audit trail will be time-correlated when the time stamp in the individual audit records can be reliably related to the time stamp in other audit records to achieve a time ordering of the records within VA’s defined tolerance.

(13) **AU-13: Monitoring For Information Disclosure (P4)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT monitors open source information for evidence of unauthorized exfiltration or disclosure of VA information.	Not Selected	Not Selected	Not Selected
Baseline allocation summary	Not Selected	Not Selected	Not Selected

VA does not require, at this time, application of control **AU-13: Monitoring for Information Disclosure**. OIT may, at their discretion, elect to monitor for information disclosure.

(14) **AU-14: Session Audit (P4)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system provides the capability to: <ul style="list-style-type: none"> • Capture/record and log all content related to a user session; and • Remotely view/hear all content related to an established user session in real time. 	Not Selected	Not Selected	Not Selected
Baseline allocation summary	Not Selected	Not Selected	Not Selected

VA does not require, at this time, application of control **AU-14: Session Audit**. OIT may, at their discretion, elect to conduct session audits.

d. **Security Assessment and Authorization (CA)**

(1) **CA-1: Security Assessment and Authorization Policies and Procedures**

VA OIT in this Appendix has outlined VA’s system security controls based on the current version of SP 800-53 that are required for the effective implementation of the Security Assessment and Authorization family. Local SOPs should be developed to facilitate the implementation and management of these controls at the local level, as needed. The Security Assessment and Authorization controls and procedures in this Appendix are consistent with applicable laws: Executive Orders, policies, regulations, standards, and guidance, and will be periodically reviewed, and, when necessary, updated ([See Attachment 2](#)).

(2) **CA-2: Security Assessments (P2)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT: <ul style="list-style-type: none"> • Develops a security assessment plan that describes the scope of the assessment including: <ol style="list-style-type: none"> i. Security controls and control enhancements under assessment; ii. Assessment procedures to be used to determine security control effectiveness; and iii. Assessment environment, assessment team, assessment roles and responsibilities. • Assesses the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system (See Attachment 2); • Produces a security assessment report that documents the results of the assessment; and • Provides the results of the SCA, in writing, to the AO or designee. 	X	X	X
(1) OIT employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system.	Not Selected	X	X
(2) OIT includes, as part of SCAs, other types of testing (See Attachment 2).	Not Selected	Not Selected	X
Baseline allocation summary	CA-2	CA-2 (1)	CA-2 (1)(2)

(3) **CA-3: Information System Connections (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT: <ul style="list-style-type: none"> • Authorizes connections from the information system to other information systems outside of the authorization boundary through the use of ISAs; • Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and • Monitors the information system connections on an ongoing basis verifying enforcement of security requirements. 	X	X	X
Baseline allocation summary	CA-3	CA-3	CA-3

(a) This control applies to dedicated connections between information systems and does not apply to transitory, user-controlled connections such as e-mail and Web site browsing.

(b) The System Owner carefully considers the risks that may be introduced when VA information systems are connected to other systems with different security requirements and security controls, both within VA and external to VA.

(c) If the interconnecting systems have the same AO, an ISA is not required. Rather, the interface characteristics between the interconnecting information systems are described in the security plans for the respective systems.

(d) System Owners determine the risk associated with each connection and the appropriate controls employed. The Department requires that System Owners utilize the methodology for documenting system support and interconnectivity agreements as developed in accordance with the current version of SP 800-47, *Security Guide for Interconnecting Information Technology Systems*.

(e) An MOU, stating the terms and conditions for sharing data and information resources, and an ISA, specifying the technical and security requirements for the connection must be completed for each external connection. The MOU and ISA will be obtained prior to connection with other systems and/or sharing of sensitive data/information. The local CIO and the ISO, in coordination and agreement with the Enterprise Security Change Control Board (CCB), approve ISAs. An MOU/ISA template is available on the Information Security portal.

(f) For contractor systems, the MOU-ISA, if required, is used in addition to inclusion of any additional appropriate security and privacy language in the contract as required by VA Handbook 6500.6.

(g) If a system interconnection exists where VA controls information from other entities (e.g., Social Security Administration, Department of Defense, Federal Aviation Administration) VA must protect the information at the same level as similar VA information. Any additional requirements should be outlined in the MOU-ISA.

(4) **CA-4: Security Certification**

Withdrawn from SP 800-53, Rev. 3, and incorporated into **CA-2: Security Assessments** control.

(5) **CA-5: Plan of Action and Milestones (POA&M) (P3)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT: <ul style="list-style-type: none"> • Develops a POA&M for the information system to document the Operating Unit’s planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and • Updates existing POA&Ms based on the findings from SCAs, security impact analyses, and continuous monitoring activities (See Attachment 2). 	X	X	X
Baseline allocation summary	CA-5	CA-5	CA-5

(a) The ISO coordinates with other VA officials with significant information and information system responsibilities to address cited deficiencies in preparing the program-level POA&M to implement corrective actions. The ISO and System Owner must track all POA&M activity within a VA approved FISMA database and coordinate completion with appropriate VA parties.

(b) The Operating Unit ISO must ensure the development and management of a process to track actions to correct weaknesses in critical elements of VA Operating Unit’s Information Security Program and system security controls. In the case of Department-level deficiencies, OIT’s Certification Program Office will document a POA&M for all IT security control deficiencies warranting corrective action that were identified by:

1. The Secretary of VA, and resulting in a material weakness in the Department’s Annual Performance and Accountability Report;
2. An external audit or evaluation (e.g., the Government Accountability Office or OIG);
3. Internal Operating Unit evaluations (e.g., SSPs documenting “planned” controls, self-assessments, periodic SCAs, contingency plan testing, or through the A&A).

(c) The POA&M is a key document in the security authorization package and is subject to Federal reporting requirements established by OMB.

(6) **CA-6: Security Authorization (P3)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT: <ul style="list-style-type: none"> • Assigns a senior-level executive or manager to the role of AO for the information system; • Ensures that the AO authorizes the information system for processing before commencing operations; and • Updates the security authorization (See Attachment 2). 	X	X	X
Baseline allocation summary	CA-6	CA-6	CA-6

(a) The role of AO has been assigned to the VA CIO.

(b) The security authorization is the official management decision given by the AO to authorize operation of an information system and explicitly accept the level of risk to VA operations, its assets, individuals, possible impact on other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

(c) The A&A process employed by VA is consistent with the current version of SP 800-37.

(d) Through the employment of a comprehensive continuous monitoring process, the authorization package is updated on an ongoing basis, and provides the AO and the Information System Owner with an up-to-date status of the security state of the information system. To reduce the administrative cost of security reauthorization, the AO uses the results of the continuous monitoring process to the maximum extent possible as the basis for rendering a reauthorization decision.

(7) **CA-7: Continuous Monitoring (P3)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT establishes a continuous monitoring strategy and implements a continuous monitoring program that includes: <ul style="list-style-type: none"> • A configuration management process for the information system and its constituent components; • A determination of the security impact of changes to the information system and environment of operation; • Ongoing SCAs in accordance with VA's continuous monitoring strategy; and • Reporting the security state of the information system to appropriate OIT officials (See Attachment 2). 	X	X	X
Baseline allocation summary	CA-7	CA-7	CA-7

(a) The implementation of a continuous monitoring program results in ongoing updates to the security plan, the security assessment report, and the POA&M, which are the three principal documents in the security authorization package.

(b) A rigorous and well-executed continuous monitoring program significantly reduces the level of effort required for the reauthorization of the information system.

(c) Continuous monitoring activities are scaled in accordance with the security categorization of the information system.

(d) Continuous monitoring of security controls using automated support tools facilitates near real-time risk management and promotes VA's situational awareness with regard to the security state of the information system.

(e) VA utilizes a VA approved FISMA database to collect, store, and report the information on the Department's assessments.

e. Configuration Management (CM)

(1) CM-1: Configuration Management Policy and Procedures

VA OIT in this Appendix has outlined VA's system security controls based on the current version of SP 800-53 that are required for the effective implementation of the Configuration Management family. Local SOPs should be developed to facilitate the implementation and management of these controls at the local level, as needed. The Configuration Management controls and procedures in this Appendix are consistent with applicable laws: Executive Orders, policies, regulations, standards, and guidance, and will be periodically reviewed, and, when necessary, updated ([See Attachment 2](#)).

(2) **CM-2: Baseline Configuration (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	X	X	X
(1) The System Owner reviews and updates the baseline configuration of the information system periodically, upon a system change, and as an integral part of information system component installations and upgrades (See Attachment 3).	Not Selected	X	X
(2) OIT employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.	Not Selected	Not Selected	X
(3) OIT retains older versions of baseline configurations as deemed necessary to support rollback.	Not Selected	X	X
(4) OIT: <ul style="list-style-type: none"> Develops and maintains a <u>list of software programs not authorized to execute on the information system</u> (See Attachment 3); and Employs an allow-all, deny-by-exception authorization policy to identify software allowed to execute on the information system. 	Not Selected	X	Not Selected
(5) OIT: <ul style="list-style-type: none"> Develops and maintains a <u>list of software programs authorized to execute on the information system</u> (See Attachment 3); and Employs a deny-all, permit-by-exception authorization policy to identify software allowed to execute on the information system. 	Not Selected	Not Selected	X
(6) OIT maintains a baseline configuration for development and test environments that is managed separately from the operational baseline configuration.	Not Selected	Not Selected	X
Baseline allocation summary	CM-2	CM-2 (1)(3)(4)	CM-2 (1)(2)(3) (5)(6)

(a) The baseline configuration is a documented, up-to-date specification to which the information system is built. The baseline configuration provides information about the components of an information system (e.g., the standard software load for a workstation, server, network component, or mobile device including operating system/installed applications with current version numbers and patch information), network topology, and the logical placement of the component within the system architecture.

(b) Maintaining the baseline configuration involves creating new baselines as the information system changes over time.

(c) The configuration of the information system must be consistent with the Federal EA and VA's information system architecture.

(d) OIT will monitor VA's approved USGCB configuration on applicable VA systems regularly using a NIST validated Security Content Automation Protocol tool.

(e) Automated mechanisms employed for maintaining baseline configurations may include software inventory tools which can be deployed for each operating system in use within the Operating Unit (e.g., on workstations, servers, network components, mobile devices) and can be used to track operating system version numbers, applications and types of software installed on the operating systems, and current patch levels. Software inventory tools can scan information systems for unauthorized software to validate lists of authorized and unauthorized software programs. See **CM-8: Information System Component Inventory** for information on requirements for information system component inventory.

(3) **CM-3: Configuration Change Control (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT: <ul style="list-style-type: none"> • Determines the types of changes to the information system that are configuration controlled; • Approves configuration-controlled changes to the system with explicit consideration for security impact analyses; • Documents approved configuration-controlled changes to the system; • Retains and reviews records of configuration-controlled changes to the system; • Audits activities associated with configuration-controlled changes to the system; and • Coordinates and provides oversight for configuration change control activities through the local CCB and the national Executive CCB, as required (See Attachment 3). 	Not Selected	X	X
(1) OIT employs automated mechanisms to: <ul style="list-style-type: none"> • Document proposed changes to the information system; • Notify designated approval authorities; • Highlight approvals that have not been received by deadline. (See Attachment 3); • Inhibit change until designated approvals are received; and • Document completed changes to the information system. 	Not Selected	Not Selected	X
(2) OIT tests, validates, and documents changes to the information system before implementing the changes on the operational system.	Not Selected	X	X
Baseline allocation summary	Not Selected	CM-3 (2)	CM-3 (1)(2)

(a) Configuration change control for the information system involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the system, including upgrades and modifications. Configuration change control includes changes to components of the information system, changes to the configuration settings for IT products (e.g., operating systems, applications, firewalls, and routers), emergency changes, and changes to remediate flaws. VA will follow VA Directive 6004.

(b) All changes to the configuration of a system will be documented in the SSP and COOP, if applicable. The System Owners, system managers, and the ISO will review all VA-NSOC security alerts and take appropriate remedial actions in a timely manner.

(c) Activities associated with configuration changes to the information system will be audited. Auditing of changes refers to changes in activity before and after a change is made to the information system and the auditing activities required to implement the change.

(d) Emergency changes for VA information systems must be documented and approved by appropriate VA officials, either prior to the change or immediately after the fact, and VA designated personnel must be notified for security analysis and follow-up.

(e) VA requires a process to be in place to identify, track, and report on security patch management that is consistent with the methodology described in the **SI-2, Flaw Remediation** of this handbook.

(f) Testing of changes prior to implementation must not interfere with information system operations. An operational system may need to be taken offline, or replicated to the extent feasible, before testing can be conducted. If an information system must be taken offline for testing, the tests are scheduled to occur during planned system outages whenever possible. When testing cannot be conducted on an operational system, compensating controls (e.g., providing a replicated system to conduct testing) are employed in accordance with the general tailoring guidance.

(4) **CM-4: Security Impact Analysis (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT analyzes changes to the information system to determine potential security impacts prior to change implementation.	X	X	X
(1) OIT analyzes new software in a separate test environment before installation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.	Not Selected	Not Selected	X
Baseline allocation summary	CM-4	CM-4	CM-4 (1)

(a) Security impact analyses are conducted by VA personnel with information security responsibilities, appropriate skills, and technical expertise to analyze the changes to information systems and the associated security ramifications. These personnel include, for example, Information System Administrators, ISOs, Information System Security Managers, and Information System Security Engineers.

(b) Security impact analysis may include, for example, reviewing information system documentation such as the security plan to understand how specific security controls are implemented within the system and how the changes might affect the controls. Security impact analysis may also include an assessment of risk to understand the impact of the changes and to determine if additional security controls are required. Security impact analysis is scaled in accordance with the security categorization of the information system.

(5) CM-5: Access Restrictions for Change (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.	Not Selected	X	X
(1) OIT employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.	Not Selected	Not Selected	X
(2) OIT conducts audits of information system changes and when indications so warrant determines whether unauthorized changes have occurred (See Attachment 3) .	Not Selected	Not Selected	X
(3) The information system prevents the installation of <u>list of critical software programs</u> that are not signed with a certificate that is recognized and approved by OIT. (See Attachment 3) .	Not Selected	Not Selected	X
Baseline allocation summary	Not Selected	CM-5	CM-5 (1)(2)(3)

Any changes to the hardware, software, and/or firmware components of the information system can potentially have significant effects on the overall security of the system. Accordingly, only qualified and authorized individuals are allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications. The approved OIT process will be used for obtaining elevated privileges to VA systems. Additionally, maintaining records of access is essential for ensuring that configuration change control is being implemented as intended and for supporting after-the-fact actions should the Operating Unit become aware of an unauthorized change to the information system. Access restrictions for change also include software libraries. Examples of access restrictions include, for example, physical and logical access controls (see **AC-3: Access Enforcement** and **PE-3: Physical Access Control**), workflow automation, media libraries, abstract layers (e.g., changes are implemented into a third-party interface rather than directly into the information system component), and change windows (e.g., changes occur only during specified times, making unauthorized changes outside the window easy to discover).

(6) **CM-6: Configuration Settings (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT: <ul style="list-style-type: none"> Establishes and documents mandatory configuration settings for IT products employed within the information system using the most restrictive mode consistent with operational requirements (See Attachment 3); OIT implements the configuration settings; The local CCB identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and The local CCB monitors and controls changes to the configuration settings in accordance with VA policies and procedures. 	X	X	X
(1) OIT employs automated mechanisms to centrally manage, apply, and verify configuration settings.	Not Selected	Not Selected	X
(2) OIT employs automated mechanisms to respond to unauthorized changes to VA's defined configuration settings (See Attachment 3).	Not Selected	Not Selected	X
(3) OIT incorporates detection of unauthorized, security-relevant configuration changes into the Operating Unit's incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes.	Not Selected	X	X
Baseline allocation summary	CM-6	CM-6 (3)	CM-6 (1)(2)(3)

Configuration settings are the configurable security-related parameters of IT products that are part of the information system. Security-related parameters are those parameters impacting the security state of the system including parameters related to meeting other security control requirements. Security-related parameters include, for example, registry settings; account, file, and directory settings (i.e., permissions); and settings for services, ports, protocols, and remote connections.

(7) **CM-7: Least Functionality (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The System Owner configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of a defined list of functions, ports, protocols, and/or services (See Attachment 3).	X	X	X
(1) The System Owner reviews the information system to identify and eliminate unnecessary functions, ports, protocols, and/or services (See Attachment 3).	Not Selected	X	X
(2) The System Owner employs automated mechanisms to prevent program execution (See Attachment 3).	Not Selected	Not Selected	X
Baseline allocation summary	CM-7	CM-7 (1)	CM-7 (1)(2)

Where feasible, OIT limits component functionality to a single function per device (e.g., e-mail server or web server, not both). The functions and services provided by information systems, or individual components of information systems, are carefully reviewed to determine which functions and services are candidates for elimination (e.g., Voice over Internet Protocol (VoIP), Instant Messaging, auto-execute, file sharing).

(8) **CM-8: Information System Component Inventory (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT develops, documents, and maintains an inventory of information system components that: <ul style="list-style-type: none"> • Accurately reflects the current information system; • Is consistent with the authorization boundary of the information system; • Is at the level of granularity deemed necessary for tracking and reporting; • Includes information necessary for effective property accountability (See Attachment 3); and • Is available for review and audit by designated VA officials. 	X	X	X
(1) OIT updates the inventory of information system components as an integral part of component installations, removals, and information system updates.	Not Selected	X	X
(2) OIT employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.	Not Selected	Not Selected	X
(3) The System Owner employs automated mechanisms to detect the addition of unauthorized components/devices into the information system and disables network access by such components/devices or notifies designated officials (See Attachment 3).	Not Selected	Not Selected	X
(4) OIT includes in property accountability information for information system components, and a means for identifying individuals responsible for administering those components (See Attachment 3).	Not Selected	Not Selected	X
(5) OIT verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system.	Not Selected	X	X
Baseline allocation summary	CM-8	CM-8 (1)(5)	CM-8 (1)(2)(3)(4)(5)

(9) **CM-9: Configuration Management Plan (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT develops, documents, and implements a configuration management plan for the information system that: <ul style="list-style-type: none"> • Addresses roles, responsibilities, and configuration management processes and procedures; • Defines the configuration items for the information system and when in the SDLC the configuration items are placed under configuration management; and • Establishes the means for identifying configuration items throughout the SDLC and a process for managing the configuration of the configuration items. 	Not Selected	X	X
Baseline allocation summary	Not Selected	CM-9	CM-9

(a) Configuration items include, but are not limited to, hardware, software, firmware, and documentation. The configuration management plan will describe how to move a change through the change management process, how configuration settings and configuration baselines are updated, how the information system component inventory is maintained, how development, test, and operational environments are controlled, and finally, how documents are developed, released, and updated.

(b) The configuration plan defines detailed processes and procedures for how configuration management is used to support SDLC activities at the information system level.

(c) The configuration management approval process includes designation of key management stakeholders that are responsible for reviewing and approving proposed changes to the information system, and security personnel that would conduct a security impact analysis prior to the implementation of any changes to the system.

f. **Contingency Planning (CP)**

(1) **CP-1: Contingency Planning Policy and Procedures**

VA OIT in this Appendix has outlined VA’s system security controls based on the current version of SP 800-53 that are required for the effective implementation of the Contingency Planning family. Local SOPs should be developed to facilitate the implementation and management of these controls at the local level, as needed. The Contingency Planning controls and procedures in this Appendix are consistent with applicable laws: Executive Orders, policies, regulations, standards, and guidance, and will be periodically reviewed, and, when necessary, updated ([See Attachment 2](#)).

(2) CP-2: Contingency Plan (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
<p>The System Owner:</p> <ul style="list-style-type: none"> • Develops a contingency plan for the information system that: <ul style="list-style-type: none"> i. Identifies essential missions and business functions and associated contingency requirements; ii. Provides recovery objectives, restoration priorities, and metrics; iii. Addresses contingency roles, responsibilities, assigned individuals with contact information; iv. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; v. Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and vi. Is reviewed and approved by designated officials within OIT; • Distributes copies of the contingency plan to <u>identified key personnel (by name and/or by role and organizational elements)</u> (See Attachment 3); • Coordinates contingency planning activities with incident handling activities; • Reviews the contingency plan for the information system (See Attachment 2); • Revises the contingency plan to address changes to VA, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; and • Communicates contingency plan changes to <u>identified key personnel and organizational elements</u> (See Attachment 3). 	X	X	X
(1) The System Owner coordinates contingency plan development with organizational elements responsible for related plans.	Not Selected	X	X
(2) The System Owner conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.	Not Selected	Not Selected	X
(3) The System Owner plans for the resumption of essential missions and business functions within <u>time period</u> of contingency plan activation (See Attachment 3).	Not Selected	Not Selected	X
Baseline allocation summary	CP-2	CP-2 (1)	CP-2 (1)(2)(3)

(a) Contingency planning for information systems is part of an overall Operating Unit program for achieving continuity of operations for mission/business operations. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. Information system recovery objectives are consistent with applicable laws, Executive Orders, policies, standards, or regulations. In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in mission/business effectiveness, such as malicious attacks compromising the confidentiality or integrity of the information system. Examples of actions to call out in contingency plans include, for example, graceful degradation, information system shutdown, fall back to a manual mode, alternate information flows, or operating in a mode that is reserved solely for when the system is under attack.

(b) System Owners will coordinate with business/service lines to identify essential missions and business functions; associated contingency requirements; and to provide recovery objectives and restoration priorities in preparing to create a system’s contingency plan.

(c) See VA Handbook 6500.8, *Information Technology Contingency Plan*, for more information and details.

(3) CP-3: Contingency Training (P2)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training (See Attachment 2).	X	X	X
(1) The Operating Unit incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.	Not Selected	Not Selected	X
Baseline allocation summary	CP-3	CP-3	CP-3 (1)

(4) **CP-4: Contingency Plan Testing and Exercises (P2)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT: <ul style="list-style-type: none"> • Tests and/or exercises the contingency plan for the information system using <u>OIT defined tests or exercises</u> to determine the plan's effectiveness and VA's readiness to execute the plan (See Attachment 3); and • Reviews the contingency plan test/exercise results and initiates corrective actions. 	X	X	X
(1) OIT coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.	Not Selected	X	X
(2) OIT tests/exercises the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.	Not Selected	Not Selected	X
(4) OIT includes a full recovery and reconstitution of the information system to a known state as part of contingency plan testing.	Not Selected	Not Selected	X
Baseline allocation summary	CP-4	CP-4 (1)	CP-4 (1)(2)(4)

There are several methods for testing and/or exercising contingency plans to identify potential weaknesses (e.g., checklist, walk-through/tabletop, simulation: parallel, full interrupt). Contingency plan testing and/or exercises include a determination of the effects on Operating Unit operations and assets (e.g., reduction in mission capability) and individuals arising due to contingency operations in accordance with the plan. See VA Handbook 6500.8 for more information.

(5) **CP-5: Contingency Plan Update**

Withdrawn from SP 800-53, Rev. 3, and incorporated into **CP-2: Contingency Plan** control.

(6) CP-6: Alternate Storage Site (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT establishes an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information.	Not Selected	X	X
(1) OIT identifies an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same hazards.	Not Selected	X	X
(2) OIT configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.	Not Selected	Not Selected	X
(3) OIT identifies potential accessibility problems to the alternate storage site in event of an area-wide disruption or disaster and outlines explicit mitigation actions.	Not Selected	X	X
Baseline allocation summary	Not Selected	CP-6 (1)(3)	CP-6 (1)(2)(3)

(a) Explicit mitigation actions include, for example, duplicating backup information at another alternate storage site if access to the first alternate site is hindered; or, if electronic accessibility to the alternate site is disrupted, planning for physical access to retrieve backup information.

(b) The alternate storage facility should have controlled access and proper environmental controls. Access controls to the VA information stored at this location will be stringently controlled and periodically tested. Locks and personnel will be used to control the off-site storage to prevent unauthorized access.

(c) System and application documentation and an up-to-date hard copy of the contingency plans are stored securely at the alternate storage location.

(7) CP-7: Alternate Processing Site (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT: <ul style="list-style-type: none"> Establishes an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions when the primary processing capabilities are unavailable (See Attachment 3); and Ensures that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the organization-defined time period for resumption. 	Not Selected	X	X
(1) OIT identifies an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same hazards.	Not Selected	X	X
(2) OIT identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	Not Selected	X	X
(3) OIT develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.	Not Selected	X	X
(4) OIT configures the alternate processing site so that it is ready to be used as the operational site supporting essential missions and business functions.	Not Selected	Not Selected	X
(5) OIT ensures that the alternate processing site provides information security measures equivalent to that of the primary site.	Not Selected	X	X
Baseline allocation summary	Not Selected	CP-7 (1)(2)(3)(5)	CP-7 (1)(2)(3)(4) (5)

Hazards that might affect the information system are typically defined in the risk analysis.

(8) CP-8: Telecommunications Services (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions when the primary telecommunications capabilities are unavailable (See Attachment 3).	Not Selected	X	X
(1) OIT: <ul style="list-style-type: none"> Develops primary and alternate telecommunications service agreements that contain priority-of- service provisions in accordance with the organization’s availability requirements; and Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier. 	Not Selected	X	X
(2) OIT obtains alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services.	Not Selected	X	X
(3) OIT obtains alternate telecommunications service providers that are separated from primary service providers so as not to be susceptible to the same hazards.	Not Selected	Not Selected	X
(4) OIT requires primary and alternate telecommunications service providers to have contingency plans.	Not Selected	Not Selected	X
Baseline allocation summary	Not Selected	CP-8 (1)(2)	CP-8 (1)(2)(3)(4)

(9) CP-9: Information System Backup (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT: <ul style="list-style-type: none"> • Conducts backups of user-level information contained in the information system (See Attachment 3); • Conducts backups of system-level information contained in the information system (See Attachment 3); • Conducts backups of information system documentation including security-related documentation (See Attachment 3); and • Protects the confidentiality and integrity of backup information at the storage location. 	X	X	X
(1) OIT tests backup information to verify media reliability and information integrity (See Attachment 3).	Not Selected	X	X
(2) OIT uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.	Not Selected	Not Selected	X
(3) OIT stores backup copies of the operating system and other critical information system software, as well as copies of the information system inventory (including hardware, software, and firmware components) in a separate facility or in a fire-rated container that is not co-located with the operational system.	Not Selected	Not Selected	X
Baseline allocation summary	CP-9	CP-9 (1)	CP-9 (1)(2)(3)

(a) System-level information includes, for example, system-state information, operating system and application software, and licenses. Digital signatures and cryptographic hashes are examples of mechanisms that can be employed by organizations to protect the integrity of information system backups. .

(b) VA system backups will be encrypted using FIPS 140-2 (or its successor) validated encryption.

(c) OIT will identify and initiate an MOU for storage of the site’s backup information when using another VA site. For commercial entities, a contract is required.

(d) The backup information will be labeled, packed, and transported to the off-site storage facility securely.

(e) Information system backups are required for all VA systems containing VA information, when technically possible.

(f) The Operating Unit ensures that a mobile device does not contain the only copy of sensitive information. A back-up of the device must be created at regular intervals and stored securely.

(10) **CP-10: Information System Recovery and Reconstitution (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The System Owner provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	X	X	X
(2) The information system implements transaction recovery for systems that are transaction-based.	Not Selected	X	X
(3) OIT provides compensating security controls for <u>organization-defined circumstances</u> (See Attachment 3).	Not Selected	X	X
(4) OIT provides the capability to reimage information system components from configuration-controlled and integrity-protected disk images representing a secure, operational state for the components (See Attachment 3).	Not Selected	Not Selected	X
Baseline allocation summary	CP-10	CP-10 (2)(3)	CP-10 (2)(3)(4)

Recovery is executing information system contingency plan activities to restore essential missions and business functions. Reconstitution takes place following recovery and includes activities for returning the information system to its original functional state before contingency plan activation. Recovery and reconstitution procedures are based on Operating Unit priorities, established recovery point/time and reconstitution objectives, and appropriate metrics. Reconstitution includes the deactivation of any interim information system capability that may have been needed during recovery operations. Reconstitution also includes an assessment of the fully restored information system capability, a potential system reauthorization and the necessary activities to prepare the system against another disruption, compromise, or failure. Recovery and reconstitution capabilities employed by the Operating Unit can be a combination of automated mechanisms and manual procedures.

g. Identification and Authentication (IA)

(1) IA-1: Identification and Authentication Policy and Procedures

(a) VA OIT in this Appendix has outlined VA’s system security controls based on the current version of SP 800-53 that are required for the effective implementation of the Identification and Authentication family. Local SOPs should be developed to facilitate the implementation and management of these controls at the local level, as needed. The Identification and Authentication controls and procedures in this Appendix are consistent with applicable laws: Executive Orders, policies, regulations, standards, and guidance, and will be periodically reviewed, and, when necessary, updated ([See Attachment 2](#)).

(b) User identification and authentication must be consistent with Homeland Security Presidential Directive (HSPD) 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, FIPS 140-2 (or its successor) validated encryption, FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, the current version of SP 800-63, *Electronic Authentication Guideline*, SP 800-73, *Interfaces for Personal Identity Verification (4 parts): Pt. 1 - End Point PIV Card Application Namespace, Data Model and Representation, Pt. 2 - PIV Card Application Interface, Pt. 3 - PIV Client Application Programming Interface, and Pt. 4 - The PIV Transitional Data Model and Interfaces*, SP 800-76, *Biometric Data Specification for Personal Identity Verification*, SP 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification* and current VA PIV procedures.

(2) **IA-2: Identification And Authentication (Organizational Users) (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	X	X	X
(1) The information system uses multifactor authentication for network access to privileged accounts.	Not Selected	X	X
(2) The information system uses multifactor authentication for network access to non-privileged accounts.	Not Selected	X	X
(3) The information system uses multifactor authentication for local access to privileged accounts.	Not Selected	X	X
(4) The information system uses multifactor authentication for local access to non-privileged accounts.	Not Selected	Not Selected	X
(8) The System Owner uses replay-resistant authentication mechanisms for network access to privileged accounts (See Attachment 3) .	Not Selected	X	X
(9) The System Owner uses replay-resistant authentication mechanisms for network access to non-privileged accounts (See Attachment 3) .	Not Selected	Not Selected	X
Baseline allocation summary	IA-2 (1)	IA-2 (1)(2)(3)(8)	IA-2 (1)(2)(3)(4)(8)(9)

(a) Authentication of users will be accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination therein, except for accesses explicitly identified in **AC-14: Permitted Actions Without Identification or Authentication**.

(b) Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in **AC-14: Permitted Actions Without Identification or Authentication**.

(c) VA users include VA employees, contractors, researchers, students, volunteers, representatives of Federal, state, local or tribal agencies. Access to VA information systems is

defined as either local or network. Local access is any access to a VA information system by a user (or process acting on behalf of a user) where such access is obtained by direct connection without the use of a network. Network access is any access to a VA information system by a user (or process acting on behalf of a user) where such access is obtained through a network connection. Remote access is a type of network access which involves communication through an external network (e.g., the Internet). Internal networks include LANs, WANs, and VPNs that are under the control of VA. The VPN is considered an internal network if the organization establishes the VPN connection between VA-controlled endpoints in a manner that does not require VA to depend on any external networks across which the VPN transits to protect the confidentiality and integrity of information transmitted. Identification and authentication requirements for information system access by other than VA users are described in **IA-8: Identification and Authentication (Non-Organizational Users)**.

(d) The identification and authentication requirements in this control are satisfied by complying with HSPD 12 consistent with VA-specific implementation plans provided to OMB. In addition to identifying and authenticating users at the information-system level (i.e., at logon), identification and authentication mechanisms are employed at the application level, when necessary, to provide increased information security for VA.

(3) IA-3: Device Identification and Authentication (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system uniquely identifies and authenticates a list of specific and/or types of devices before establishing a connection (See Attachment 3).	Not Selected	X	X
Baseline allocation summary	Not Selected	IA-3	IA-3

The devices requiring unique identification and authentication may be defined by type, by specific device, or by a combination of type and device as deemed appropriate by OIT. The information system typically uses either shared known information (e.g., Media Access Control (MAC) or Transmission Control Protocol (TCP)/IP addresses) for identification or an OIT approved authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol, Radius server with Extensible Authentication Protocol-Transport Layer Security authentication, Kerberos) to identify and authenticate devices on LAN and/or WAN. The required strength of the device authentication mechanism is determined by the security categorization of the information system.

(4) **IA-4: Identifier Management (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT manages information system identifiers for users and devices by: <ul style="list-style-type: none"> • Receiving authorization from a designated organizational official to assign a user or device identifier; • Selecting an identifier that uniquely identifies an individual or device; • Assigning the user identifier to the intended party or the device identifier to the intended device; • Preventing reuse of user or device identifiers (See Attachment 3); and • Disabling the user identifier (See Attachment 3). 	X	X	X
Baseline allocation summary	IA-4	IA-4	IA-4

Common device identifiers include MAC or IP addresses, or device-unique token identifiers. It is commonly the case that a user identifier is the name of an information system account associated with an individual. In such instances, identifier management is largely addressed by the account management activities of **AC-2: Account Management**. These requirements also cover user identifiers not necessarily associated with an information system account (e.g., the identifier used in a physical security control database accessed by a badge reader system for access to the information system).

(5) IA-5: Authenticator Management (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
<p>OIT manages information system authenticators for users and devices by:</p> <ul style="list-style-type: none"> • Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator; • Establishing initial authenticator content for authenticators defined by the organization; • Ensuring that authenticators have sufficient strength of mechanism for their intended use; • Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; • Changing default content of authenticators upon information system installation; • Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate); • Changing/refreshing authenticators (See Attachment 2); • Protecting authenticator content from unauthorized disclosure and modification; and • Requiring users to take, and having devices implement, specific measures to safeguard authenticators. 	X	X	X
<p>(1) The information system, for password-based authentication:</p> <ul style="list-style-type: none"> • Enforces VA minimum password complexity (See Attachment 2). • Enforces a number of characters to be changed when new passwords are created (See Attachment 2). • Encrypts passwords in storage and in transmission; • Enforces password minimum and maximum lifetime restrictions (See Attachment 2). • Prohibits reuse of a password (See Attachment 2). 	X	X	X
<p>(2) The information system, for PKI-based authentication:</p> <ul style="list-style-type: none"> • Validates certificates by constructing a certification path with status information to an accepted trust anchor; • Enforces authorized access to the corresponding private key; and • Maps the authenticated identity to the user account. 	Not Selected	X	X
<p>(3) The Operating Unit requires the registration process to receive defined types of authenticators to be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor) (See Attachment 2).</p>	Not Selected	X	X
Baseline allocation summary	IA-5 (1)	IA-5 (1)(2)(3)	IA-5 (1)(2)(3)

(a) User authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). Many information system components are shipped with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, present a significant security risk, and therefore, must be changed upon installation. The requirement to protect user authenticators may be implemented via control **PL-4: Rules of Behavior** or **PS-6: Access Agreements** for authenticators in the possession of users and by controls **AC-3: Access Enforcement**, **AC-6: Least Privilege**, and **SC-28: Protection Of Information At Rest** for authenticators stored within the information system (e.g., passwords stored in a hashed or encrypted format, files containing encrypted or hashed passwords accessible only with super user privileges). The information system supports user authenticator management by VA-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, password composition, validation time window for time synchronous one time tokens, and number of allowed rejections during verification stage of biometric authentication. Measures to safeguard user authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords.

(b) The minimum requirements for password-based authentication are intended primarily for environments where passwords are used as a single factor to authenticate users, or in a similar manner along with one or more additional authenticators. The enhancement generally does not apply to situations where passwords are used to unlock hardware authenticators.

(c) Status information for certification paths includes, for example, certificate revocation lists or online certificate status protocol responses.

(d) Authenticators (passwords) must be protected to prevent unauthorized used. Specifically:

1. Passwords must not be shared except in emergency circumstances or when there is an overriding operational necessity as documented in an operating unit SSP. Once shared, passwords must be changed as soon as possible.

2. Passwords that need to be shared because of an overriding operational necessity cannot be used to control access to other information systems or applications on information systems.

3. Passwords in readable form (e.g., written on paper) must be kept in a safe location and not stored in a location accessible to others.

4. Information systems and workstations must not display or print passwords as they are entered.

5. User applications must not be enabled to retain passwords for subsequent re-use, or be configured to bypass authentication mechanisms. For example, Internet browsers must not be enabled to save passwords for re-use. However, use of password retaining programs is allowed provided that the retaining program requires authentication and stores passwords in an encrypted manner.

6. Passwords must not be distributed through non-encrypted e-mail or left on answering machines.

7. Passwords must be changed as follows:

a. At least every 90 days;

b. Immediately if discovered to be compromised or one suspects a password has been compromised;

c. Immediately if discovered to be in non-compliance with VA requirements; or

d. On discretion from management.

8. Access to password files or password databases must be restricted to only those who are authorized to manage the information system and have appropriate clearance.

9. If a determination is made that a password has been compromised or is not in compliance with this standard, and if the password is not immediately changed, the account must be temporarily suspended until the password is changed.

10. Passwords for servers, mainframes, telecommunication devices (such as routers and switches) and devices used for information system security functions (such as firewalls, intrusion detection, and audit logging) must be encrypted when stored electronically.

11. Passwords, other than single-use (one-time) passwords, must be encrypted when transmitted across a WAN or the Internet.

12. Passwords for access to individual workstations, such as passwords for screen savers, should be encrypted when stored electronically.

(6) **IA-6: Authenticator Feedback (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	X	X	X
Baseline allocation summary	IA-6	IA-6	IA-6

The feedback from the information system does not provide information that would allow an unauthorized user to compromise the authentication mechanism. Displaying asterisks when a user types in a password, is an example of obscuring feedback of authentication information.

(7) **IA-7: Cryptographic Module Authentication (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system uses mechanisms for authentication to a cryptographic module that meet the requirements of applicable Federal laws, Executive Orders, policies, regulations, standards, and guidance for such authentication.	X	X	X
Baseline allocation summary	IA-7	IA-7	IA-7

(8) **IA-8: Identification And Authentication (Non-Organizational Users) (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).	X	X	X
Baseline allocation summary	IA-8	IA-8	IA-8

Non-VA users include all information system users other than VA users explicitly covered by **IA-2: Identification and Authentication (Organizational Users)**. Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by VA in accordance with **AC-14: Permitted Actions Without Identification or Authentication**. In accordance with the E-Authentication E-Government initiative, authentication of non-VA users accessing Federal information systems may be required to protect Federal, proprietary, or privacy-related information (with exceptions noted for national security systems). Accordingly, a risk assessment is used in determining the authentication needs of VA. Scalability, practicality, and security are simultaneously considered in balancing the need to ensure ease of use for access to Federal information and information systems with the need to protect and adequately mitigate risk to VA operations and assets, individuals, other organizations, and the Nation. Identification and authentication requirements for information system access by VA users are described in **IA-2: Identification and Authentication (Organizational Users)**.

h. Incident Response (IR)

(1) IR-1: Incident Response Policy and Procedures

(a) VA OIT in this Appendix has outlined VA’s system security controls based on the current version of SP 800-53 that are required for the effective implementation of the Incident Response family. Local SOPs should be developed to facilitate the implementation and management of these controls at the local level, as needed. The Incident Response controls and procedures in this Appendix are consistent with applicable laws: Executive Orders, policies, regulations, standards, and guidance, and will be periodically reviewed, and, when necessary, updated ([See Attachment 2](#)).

(b) For additional information regarding incident response see VA Handbook 6500.2/1, *Management of Data Breaches Involving Sensitive Personal Information (SPI)*.

(2) IR-2: Incident Response Training (P2)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT: <ul style="list-style-type: none"> • Trains personnel in their incident response roles and responsibilities with respect to the information system; and • Provides refresher training to personnel in their incident response roles and responsibilities with respect to the information system (See Attachment 2). 	X	X	X
(1) OIT incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.	Not Selected	Not Selected	X
(2) OIT employs automated mechanisms to provide a more thorough and realistic training environment.	Not Selected	Not Selected	X
Baseline allocation summary	IR-2	IR-2	IR-2 (1)(2)

Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources.

(3) IR-3: Incident Response Testing and Exercises (P2)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT tests and/or exercises the incident response capability for the information system to determine the incident response effectiveness and documents the results (See Attachment 2) .	Not Selected	X	X
(1) OIT employs automated mechanisms to more thoroughly and effectively test/exercise the incident response capability.	Not Selected	Not Selected	X
Baseline allocation summary	Not Selected	IR-3	IR-3 (1)

(a) All tests and/or exercises are documented in the SSP.

(b) The ISO and PO track and document information system security and privacy incidents on an ongoing basis.

(4) IR-4: Incident Handling (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT: <ul style="list-style-type: none"> • Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; • Coordinates incident handling activities with contingency planning activities; and • Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly. 	X	X	X
(1) OIT employs automated mechanisms to support the incident handling process.	Not Selected	X	X
Baseline allocation summary	IR-4	IR-4 (1)	IR-4 (1)

Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

(5) IR-5: Incident Monitoring (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT tracks and documents information system security incidents.	X	X	X
(1) OIT employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.	Not Selected	Not Selected	X
Baseline allocation summary	IR-5	IR-5	IR-5 (1)

OIT employs VA approved tools for tracking and documenting information systems security incidents on an ongoing basis. Documenting information system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

(6) IR-6: Incident Reporting (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit and OIT: <ul style="list-style-type: none"> Require personnel to report suspected security/privacy incidents immediately upon suspicion (See Attachment 2); and Report security/privacy incident information to immediate supervisor, ISO and PO after discovery or suspicion. Notify VA-NSOC after normal business hours. 	X	X	X
(1) OIT employs automated mechanisms to assist in the reporting of security incidents.	Not Selected	X	X
Baseline allocation summary	IR-6	IR-6 (1)	IR-6 (1)

(a) The intent of this control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for Federal agencies and their subordinate organizations. The types of security incidents reported, the content and timeliness of the reports, and the list of designated reporting authorities are consistent with applicable Federal laws, Executive Orders, policies, regulations, standards, and guidance. Current Federal policy requires that all Federal agencies (unless specifically exempted from such requirements) report security incidents to the US-CERT within specified time frames designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling.

(b) If any VA staff member witnesses a case of egregious waste of government resources or outright fraud, they must comply with 38 CFR 1.201, *Employee’s Duty to Report*, and 1.204, *Information to be Reported to the Office of Inspector General*, and directly contact the OIG Hotline.

(c) The ISO and PO will work with management and, if a compromise occurred, members of the appointed investigative team will examine the details surrounding the incident ensuring information and systems are not compromised. The ISO and/or PO will contact, either automatically via e-mail and/or via phone, VA-NSOC within an hour to coordinate a response to the incident and to limit the damage. If the incident is believed to involve criminal activity, the ISO and/or PO will contact the local VA Police and the OIG. VA-NSOC staff will file a report with VA OIG Hotline, as appropriate. VA-NSOC offers advice and assistance regarding handling and reporting of security incidents. This support resource is an integral part of VA’s incident response capability.

(d) For additional information and procedures see VA Handbook 6500.2/1.

(7) IR-7: Incident Response Assistance (P3)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit and OIT provide an incident response support resource, integral to the organizational incident response capability, which offers advice and assistance to users of the information system for the handling and reporting of security incidents.	X	X	X
(1) OIT employs automated mechanisms to increase the availability of incident response-related information and support.	Not Selected	X	X
Baseline allocation summary	IR-7	IR-7 (1)	IR-7 (1)

(a) VA-NSOC may also alert the Operating Unit of suspicious or malicious activity when such activity has been detected. The ISO will resolve the matter according to VA’s OIT policy and local procedures, as appropriate.

(b) VA-NSOC will provide technical guidance, advise vendors to address product/software related issues, and provide liaisons to legal and criminal investigative groups as needed. VA-NSOC will also ensure that, if appropriate, the related information will be shared with owners of interconnected systems, US-CERT, and other local law enforcement.

(c) VA-NSOC provides internal assistance to VA in handling incidents, technical queries, as well as alerts and advisories, and has a 24-hour incident response center at 1-866-407-1566 (via e-mail at VA-NSOC@va.gov).

(8) IR-8: Incident Response Plan (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
<p>The Operating Unit and OIT:</p> <ul style="list-style-type: none"> • Develop an incident response plan that: <ol style="list-style-type: none"> i. Provides OIT with a roadmap for implementing its incident response capability; ii. Describes the structure and organization of the incident response capability; iii. Provides a high-level approach for how the incident response capability fits into the overall organization; iv. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; v. Defines reportable incidents; vi. Provides metrics for measuring the incident response capability within the organization; vii. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and viii. Is reviewed and approved by designated officials within the organization. • Distribute copies of the incident response plan to a defined list of incident response personnel (identified by name and/or by role) and organizational elements (See Attachment 3); • Review the incident response plan (See Attachment 3) • Revise the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and • Communicate incident response plan changes to a defined list of incident response personnel (identified by name and/or by role) and organizational elements (See Attachment 3). 	X	X	X
Baseline allocation summary	IR-8	IR-8	IR-8

i. **Maintenance (MA)**

(1) **MA-1 System Maintenance Policy and Procedures**

VA OIT in this Appendix has outlined VA’s system security controls based on the current version of SP 800-53 that are required for the effective implementation of the Maintenance family. Local SOPs should be developed to facilitate the implementation and management of these controls at the local level, as needed. The Maintenance controls and procedures in this Appendix are consistent with applicable laws: Executive Orders, policies, regulations, standards, and guidance, and will be periodically reviewed, and, when necessary, updated ([See Attachment 2](#)).

(2) **MA-2: Controlled Maintenance (P2)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT: <ul style="list-style-type: none"> • Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or VA requirements; • Controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; • Requires that a designated official explicitly approve the removal of the information system or system components from VA facilities for off-site maintenance or repairs; • Sanitizes equipment to remove all information from associated media prior to removal from VA facilities for off-site maintenance or repairs; and • Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions. 	X	X	X
(1) OIT maintains maintenance records for the information system that include: <ul style="list-style-type: none"> • Date and time of maintenance; • Name of the individual performing the maintenance; • Name of escort, if necessary; • A description of the maintenance performed; and • A list of equipment removed or replaced (including identification numbers, if applicable). 	Not Selected	X	X
(2) OIT employs automated mechanisms to schedule, conduct, and document maintenance and repairs as required, producing up-to date, accurate, complete, and available records of all maintenance and repair actions, needed, in process, and completed.	Not Selected	Not Selected	X
Baseline allocation summary	MA-2	MA-2 (1)	MA-2 (1)(2)

(3) **MA-3: Maintenance Tools (P2)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT approves, controls, monitors the use of, and maintains on an ongoing basis, information system maintenance tools.	Not Selected	X	X
(1) OIT inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications.	Not Selected	X	X
(2) OIT checks all media containing diagnostic and test programs for malicious code before the media are used in the information system.	Not Selected	X	X
(3) OIT prevents the unauthorized removal of maintenance equipment by one of the following: (i) verifying that there is no VA information contained on the equipment; (ii) sanitizing or destroying the equipment; (iii) retaining the equipment within the facility; or (iv) obtaining an exemption from the local CIO explicitly authorizing removal of the equipment from the facility.	Not Selected	Not Selected	X
Baseline allocation summary	Not Selected	MA-3 (1)(2)	MA-3 (1)(2)(3)

(a) The intent of this control is to address the security-related issues arising from the hardware and software brought into the information system specifically for diagnostic and repair actions (e.g., a hardware or software packet sniffer that is introduced for the purpose of a particular maintenance activity). Hardware and/or software components that may support information system maintenance, yet are a part of the system (e.g., the software implementing “ping,” “ls,” “ipconfig,” or the hardware and software implementing the monitoring port of an Ethernet switch) are not covered by this control.

(b) Maintenance tools that may be brought into the facility by maintenance personnel include, for example, diagnostic and test equipment used to conduct maintenance on the information system.

(4) **MA-4: Non-Local Maintenance (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT: <ul style="list-style-type: none"> • Authorizes, monitors, and controls non-local maintenance and diagnostic activities; • Allows the use of non-local maintenance and diagnostic tools only as consistent with VA policy and documented in the security plan for the information system; • Employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions; • Maintains records for non-local maintenance and diagnostic activities; and • Terminates all sessions and network connections when non-local maintenance is completed. 	X	X	X
(1) OIT audits non-local maintenance and diagnostic sessions and designated VA personnel review the maintenance records of the sessions.	Not Selected	X	X
(2) OIT documents, in the security plan for the information system, the installation and use of non-local maintenance and diagnostic connections.	Not Selected	X	X
(3) OIT: <ul style="list-style-type: none"> • Requires that non-local maintenance and diagnostic services be performed from an information system that implements a level of security at least as high as that implemented on the system being serviced; or • Removes the component to be serviced from the information system and prior to non-local maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from VA facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software and surreptitious implants) before reconnecting the component to the information system. 	Not Selected	Not Selected	X
Baseline allocation summary	MA-4	MA-4 (1)(2)	MA-4 (1)(2)(3)

Non-local maintenance and diagnostic activities are those activities conducted by individuals communicating through a network; either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection. Identification and authentication techniques used in the establishment of non-local maintenance and diagnostic sessions are consistent with the network access requirements in **IA-2: Identification and Authentication (Organizational Users)**. Strong authenticators include, for example, PKI where certificates are stored on a token protected by a password, passphrase, or biometric.

Enforcing requirements in **MA-4: Non-Local Maintenance** is accomplished in part, by other controls. See **AC-17: Remote Access** for information regarding modems.

(5) **MA-5: Maintenance Personnel (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT: <ul style="list-style-type: none"> Establishes a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel; and Ensures that personnel performing maintenance on the information system have required access authorizations or designates VA personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations. 	X	X	X
Baseline allocation summary	MA-5	MA-5	MA-5

Based on a prior assessment of risk, OIT may issue temporary credentials to individuals not previously identified in the information systems, such as vendor personnel and consultants who have legitimate requirements for privileged access to the system when conducting maintenance activities. Temporary credentials must be issued for either one time use or for a very limited period of time.

(6) **MA-6: Timely Maintenance**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The System Owner obtains maintenance support and/or spare parts for security-critical information system components and/or key IT components within a time frame suitable to avoid failure (See Attachment 3).	Not Selected	X	X
Baseline allocation summary	Not Selected	MA-6	MA-6

OIT specifies those information system components that, when not operational, result in increased risk to organizations, individuals, or the Nation because the security functionality intended by that component is not being provided. Security-critical components include, for example, firewalls, guards, gateways, intrusion detection systems (IDS), audit repositories, authentication servers, and intrusion prevention systems.

j. **Media Protection (MP)**

(1) **MP-1: Media Protection Policy and Procedures**

VA OIT in this Appendix has outlined VA’s system security controls based on the current version of SP 800-53 that are required for the effective implementation of the Media Protection family. Local SOPs should be developed to facilitate the implementation and management of these controls at the local level, as needed. The Media Protection controls and procedures in this Appendix are consistent with applicable laws: Executive Orders, policies, regulations, standards, and guidance, and will be periodically reviewed, and, when necessary, updated ([See Attachment 2](#)).

(2) **MP-2: Media Access (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The System Owner restricts access to information in printed form or on digital media to authorized users (See below and refer to See Attachment 3).	X	X	X
(1) The System Owner employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.	Not Selected	X	X
Baseline allocation summary	MP-2	MP-2 (1)	MP-2 (1)

(a) The use of VA information system media within the Operating Unit must first be authorized by the local CIO. VA information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, USB flash/thumb drives, CDs, DVDs) and non-digital media (e.g., paper, microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, PDA, cellular telephones, digital cameras, and audio recording devices). VA telephone systems are also considered information systems and may have the capability to store information on internal media (e.g., on voicemail systems).

(b) See **AC-19: Access Control for Mobile Devices** regarding requirements for protecting mobile devices.

(c) Guard stations that control access to media storage areas may be used in lieu of automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted. Media storage areas are those areas where a significant volume of media is stored, locations where only some media is stored (e.g., in individual offices) are not considered media storage areas.

(3) **MP-3: Media Marking (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT: <ul style="list-style-type: none"> • Marks removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and • Exempts specific types of media or hardware, as documented in security plan, such as disk packs and backup tapes, from marking as long as the exempted items remain within the secured computer room (See Attachment 3). 	Not Selected	X	X
Baseline allocation summary	Not Selected	MP-3	MP-3

(a) The term marking is used when referring to the application or use of human-readable security attributes.

(b) Marking of removable media and information system output is consistent with applicable Federal laws, Executive Orders, policies, regulations, standards, and guidance.

(4) **MP-4: Media Storage (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT: <ul style="list-style-type: none"> • Physically controls and securely stores information systems media, both paper and electronic, within controlled areas based on the highest FIPS 199 security category of the information recorded on the media (See Attachment 3); and • Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures. 	Not Selected	X	X
Baseline allocation summary	Not Selected	MP-4	MP-4

(a) Mobile devices and hard copies of VA sensitive information will be stored securely when not in use. Examples of secure storage when not in use would include locking mobile devices and VA sensitive information in cabinets or drawers or keeping them in a locked room. Supervisors must ensure users understand their responsibility to securely store hard copies of VA sensitive information and all mobile and portable systems such as laptop computers, notebook computers, PDA, handheld devices, wireless telephones, and removable storage media devices when they are not in use and whenever they are in an unsecured environment.

(b) A controlled area is any area or space for which the Operating Unit has confidence that the physical and procedural protections are sufficient to meet the requirements established for protecting the information and/or information system (e.g., locked room with authorized access only).

(5) **MP-5: Media Transport (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit: <ul style="list-style-type: none"> Protects and controls information system media, paper and electronic, during transport outside of controlled areas using security measures that protect the items from disclosure, compromise, or breach (See Attachment 3); Maintains accountability for information system media during transport outside of controlled areas; and Restricts the activities associated with transport of such media to authorized personnel. 	Not Selected	X	X
(2) The Operating Unit documents activities associated with the transport of information system media.	Not Selected	X	X
(3) The Operating Unit employs an identified custodian throughout the transport of information system media.	Not Selected	Not Selected	X
(4) The Operating Unit employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	Not Selected	X	X
Baseline allocation summary	Not Selected	MP-5 (2)(4)	MP-5 (2)(3)(4)

(a) Physical and technical security measures for the protection of digital and non-digital media are commensurate with the classification or sensitivity of the information residing on the media, and consistent with applicable Federal laws, Executive Orders, policies, regulations, standards, and guidance.

(b) Authorized transport and courier personnel may include individuals from outside VA (e.g., U.S. Postal Service or a commercial transport or delivery service).

(c) See **AC-19: Access Control for Mobile Devices** regarding requirements for protecting mobile devices.

(6) **MP-6: Media Sanitization (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit and OIT: <ul style="list-style-type: none"> Sanitizes information system media, both digital and non-digital, prior to disposal, release out of VA control, or release for reuse; and Employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information. 	X	X	X
(1) The Operating Unit and OIT track, document, and verify media sanitization and disposal actions.	Not Selected	Not Selected	X
(2) OIT tests sanitization equipment and procedures to verify correct performance (See Attachment 3).	Not Selected	Not Selected	X
(3) OIT sanitizes portable, removable storage devices prior to connecting such devices to the information system under the identified circumstances (See Attachment 3).	Not Selected	Not Selected	X
Baseline allocation summary	MP-6	MP-6	MP-6 (1)(2)(3)

(a) Sanitization processes employed by the Operating Unit must cause the removal of all VA sensitive data from information systems storage devices and render the data from these systems unreadable. This control applies to all media subject to disposal or reuse, whether or not considered removable/portable/mobile.

(b) The ISO will coordinate and audit the media sanitization process and document the audit on an annual basis to ensure compliance with national media sanitization policy.

(c) Inventory and disposition records for information system media must be maintained to ensure control and accountability of VA information. The media related records must contain sufficient information to reconstruct the data in the event of a breach.

(d) Operating Units refer to the current version of SP 800-88, *Guidelines for Media Sanitization*, and VA Handbook 6500.1 for information on approved equipment, techniques, and procedures for media sanitization prior to disposal or release for reuse.

k. Physical and Environmental Protection (PE)

(1) PE-1: Physical and Environmental Protection Policy and Procedures

VA OIT in this Appendix has outlined VA’s system security controls based on the current version of SP 800-53 that are required for the effective implementation of the Physical and Environmental family. Local SOPs should be developed to facilitate the implementation and management of these controls at the local level, as needed. The Physical and Environmental Protection controls and procedures in this Appendix are consistent with applicable laws: Executive Orders, policies, regulations, standards, and guidance, and will be periodically reviewed, and, when necessary, updated ([See Attachment 2](#)). NOTE: Current version of VA Handbook 0730 applies in addition to the physical controls outlined in this handbook and should be implemented in conjunction with the Physical and Environmental protections.

(2) PE-2: Physical Access Authorizations (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT: <ul style="list-style-type: none"> • Develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); • Issues authorization credentials; and • Reviews and approves the access list and authorization credentials removing from the access list personnel no longer requiring access (See Attachment 3). 	X	X	X
Baseline allocation summary	PE-2	PE-2	PE-2

(a) Authorization credentials include, for example, badges, identification cards, and smart cards.

(b) The System Owner may designate an alternate for adding individuals to the access list for emergency situations.

(3) PE-3: Physical Access Control (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit: <ul style="list-style-type: none"> • Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible); • Verifies individual access authorizations before granting access to the facility; • Controls entry to the facility containing the information system using physical access devices and/or guards; • Controls access to areas officially designated as publicly accessible in accordance with the organization’s assessment of risk; • Secures keys, combinations, and other physical access devices. Keys will be controlled in accordance with the current version of VA Handbook 0730; • Inventories physical access devices (See Attachment 3); and • Changes combinations and keys as specified in the security plan or when keys are lost, combinations are compromised, or individuals are transferred or terminated (See Attachment 3). 	X	X	X
(1) The Operating Unit enforces physical access authorizations to the information system independent of the physical access controls for the facility.	Not Selected	Not Selected	X
Baseline allocation summary	PE-3	PE-3	PE-3 (1)

(a) VA and its Operating Units will determine the types of guards needed, for example, professional physical security staff or other personnel such as administrative staff or information system users, as deemed appropriate. Physical access point controls include physical access devices (e.g., keys, locks, combinations, card readers) and/or guards to control entry to facilities containing information systems.

(b) Workstations and associated peripherals connected to (and part of) the information system may be located in areas designated as publicly accessible with access to such devices being safeguarded.

(c) The requirement for independent physical access authorizations for high-impact systems applies to server rooms, media storage areas, communications centers, or any other areas within an organizational facility containing large concentrations of information system components. The intent is to provide additional physical security for those areas where VA may be more vulnerable due to the concentration of information system components.

(4) PE-4: Access Control for Transmission Medium (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit controls physical access to information system distribution and transmission lines within organizational facilities.	Not Selected	X	X
Baseline allocation summary	Not Selected	PE-4	PE-4

(a) Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protections are necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions.

(b) Protective measures to control physical access to information system distribution and transmission lines include:

1. Locked wiring closets;
2. Disconnected or locked spare jacks; and/or
3. Protection of cabling by conduit or cable trays.

(5) PE-5: Access Control for Output Devices (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.	Not Selected	X	X
Baseline allocation summary	Not Selected	PE-5	PE-5

Monitors (viewing), printers, and audio devices are examples of information system output devices. Monitors used by employees in public areas should be positioned, when possible, so the public cannot view the information on the monitor. When positioning is not possible, privacy screens will be used.

(6) **PE-6: Monitoring Physical Access (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit: <ul style="list-style-type: none"> Monitors physical access to the information system to detect and respond to physical security incidents; Reviews physical access logs (See Attachment 3); and Coordinates results of reviews and investigations with the VA's incident response capability. 	X	X	X
(1) The Operating Unit monitors real-time physical intrusion alarms and surveillance equipment.	Not Selected	X	X
(2) The Operating Unit employs automated mechanisms to recognize potential intrusions and initiate designated response actions.	Not Selected	Not Selected	X
Baseline allocation summary	PE-6	PE-6 (1)	PE-6 (1)(2)

Investigation of and response to detected physical security incidents, including apparent security violations or suspicious physical access activities are part of the organization's incident response capability.

(7) **PE-7: Visitor Control (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides (this includes but is not limited to server room, data closets, and records storage areas) other than areas designated as publicly accessible.	X	X	X
(1) The Operating Unit escorts visitors and monitors visitor activity, when required.	Not Selected	X	X
Baseline allocation summary	PE-7	PE-7 (1)	PE-7 (1)

Individuals (to include organizational employees, contract personnel, and others) with permanent authorization credentials for the facility are not considered visitors.

(8) PE-8: Access Records (P3)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT: <ul style="list-style-type: none"> Maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); and Reviews visitor access records (See Attachment 3). 	X	X	X
(1) OIT employs automated mechanisms to facilitate the maintenance and review of access records.	Not Selected	Not Selected	X
(2) OIT maintains a record of all physical access, both visitor and authorized individuals.	Not Selected	Not Selected	X
Baseline allocation summary	PE-8	PE-8	PE-8 (1)(2)

(a) Visitor access records will include, but are not limited to:

1. Name/organization of the person visiting;
2. Signature of the visitor;
3. Form(s) of identification;
4. Date of access;
5. Time of entry and departure;
6. Purpose of visit; and
7. Name/organization of person visited.

(b) A validation/redundancy procedure will ensure that access logs are reviewed as required.

(9) PE-9: Power Equipment and Power Cabling (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit protects power equipment and power cabling for the information system from damage and destruction.	Not Selected	X	X
Baseline allocation summary	Not Selected	PE-9	PE-9

This control may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Operating Units should avoid duplicating actions already covered.

(10) PE-10: Emergency Shutoff (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit: <ul style="list-style-type: none"> Provides the capability of shutting off power to the information system or individual system components in emergency situations; Places emergency shutoff switches or devices in locations to facilitate safe and easy access for personnel (See Attachment 3); and Protects emergency power shutoff capability from unauthorized activation. 	Not Selected	X	X
Baseline allocation summary	Not Selected	PE-10	PE-10

This control applies to facilities containing concentrations of information system resources, for example, data centers, server rooms, and mainframe computer rooms.

(11) PE-11: Emergency Power (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.	Not Selected	X	X
(1) The Operating Unit provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.	Not Selected	Not Selected	X
Baseline allocation summary	Not Selected	PE-11	PE-11 (1)

This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Operating Units should avoid duplicating actions already covered.

(12) PE-12: Emergency Lighting (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	X	X	X
Baseline allocation summary	PE-12	PE-12	PE-12

This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Operating Units should avoid duplicating actions already covered.

(13) PE-13: Fire Protection (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.	X	X	X
(1) The Operating Unit employs fire detection devices/systems for the information system that activate automatically and notify the organization and emergency responders in the event of a fire.	Not Selected	X	X
(2) The Operating Unit employs fire suppression devices/systems for the information system that provide automatic notification of any activation to the organization and emergency responders.	Not Selected	X	X
(3) The Operating Unit employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.	Not Selected	X	X
Baseline allocation summary	PE-13	PE-13 (1)(2)(3)	PE-13 (1)(2)(3)

(a) Fire suppression and detection devices/systems include but are not limited to sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.

(b) This control may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Operating Units should avoid duplicating actions already covered.

(14) PE-14: Temperature and Humidity Controls (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit: <ul style="list-style-type: none"> Maintains temperature and humidity levels within the facility where the information system resides at <u>acceptable levels</u> (See Attachment 3); and Monitors temperature and humidity levels (See Attachment 3). 	X	X	X
Baseline allocation summary	PE-14	PE-14	PE-14

This control may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Operating Units should avoid duplicating actions already covered.

(15) **PE-15: Water Damage Protection (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.	X	X	X
(1) The Operating Unit employs mechanisms that, without the need for manual intervention, protect the information system from water damage in the event of a water leak.	Not Selected	Not Selected	X
Baseline allocation summary	PE-15	PE-15	PE-15 (1)

This control may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Operating Units should avoid duplicating actions already covered.

(16) **PE-16: Delivery and Removal (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit authorizes, monitors, and controls types of information system components (i.e., hardware, firmware, software) entering and exiting the facility and maintains records of those items (See Attachment 3).	X	X	X
Baseline allocation summary	PE-16	PE-16	PE-16

a. Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries.

b. Facilities and remote facilities will maintain an approved list of personnel that are authorized to deliver or remove IT equipment in conjunction with the application of a property pass system as indicated in VA Handbook 7002, *Logistics Management*.

(17) PE-17: Alternate Work Site (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit: <ul style="list-style-type: none"> • Employs appropriate <u>controls</u> both physical and logical at alternate work sites (See Attachment 3); • Assesses, as feasible, the effectiveness of security controls at alternate work sites; and • Provides a means for employees to communicate with information security personnel in case of security incidents or problems. 	Not Selected	X	X
Baseline allocation summary	Not Selected	PE-17	PE-17

(a) Alternate work sites may include, but are not limited to, government facilities and private residences of employees.

(b) Operating Units will define security controls and policies for specific alternate work sites or types of sites. Telework and alternate work site practices will be conducted and carried out according to VA Directive and Handbook 5011, *Hours of Duty and Leave*, or other VA directives/handbooks that relate to Teleworking policy and procedures.

(18) PE-18: Location of Information System Components (P2)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	Not Selected	X	X
(1) The Operating Unit plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy.	Not Selected	Not Selected	X
Baseline allocation summary	Not Selected	PE-18	PE-18 (1)

(a) Physical and environmental hazards include, but are not limited to flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and electromagnetic radiation.

(b) VA and Operating Unit should consider the location or site of the facility with regard to physical and environmental hazards. In addition, the organization considers the location of physical entry points where unauthorized individuals, while not being granted access, might nonetheless be in close proximity to the information system and therefore, increase the potential for unauthorized access to organizational communications (e.g., through the use of wireless sniffers or microphones).

(c) This control may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Operating Units should avoid duplicating actions already covered.

(19) **PE-19: Information Leakage (P4)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit protects the information system from information leakage due to electromagnetic signals emanations.	Not Selected	Not Selected	Not Selected
Baseline allocation summary	Not Selected	Not Selected	Not Selected

VA does not require, at this time, application of control **PE-19: Information Leakage**. OIT may, at their discretion, elect to protect against information leakage.

c. **Planning (PL)**

(1) **PL-1: Security Planning Policy and Procedures**

VA OIT in this Appendix has outlined VA’s system security controls based on the current version of SP 800-53 that are required for the effective implementation of the Security Planning family. Local SOPs should be developed to facilitate the implementation and management of these controls at the local level, as needed. The Security Planning controls and procedures in this Appendix are consistent with applicable laws: Executive Orders, policies, regulations, standards, and guidance, and will be periodically reviewed, and, when necessary, updated ([See Attachment 2](#)).

(2) **PL-2: System Security Plan (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The System Owner: <ul style="list-style-type: none"> • Develops a security plan for the information system that: <ul style="list-style-type: none"> i. Is consistent with VA’s EA; ii. Explicitly defines the authorization boundary for the system; iii. Describes the operational context of the information system in terms of missions and business processes; iv. Provides the security categorization of the information system including supporting rationale; v. Describes the operational environment for the information system; vi. Describes relationships with or connections to other information systems; vii. Provides an overview of the security requirements for the system; viii. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and ix. Is reviewed and approved by the AO or designee prior to plan implementation; • Reviews the security plan for the information system (See Attachment 2); and • Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or subsequent reviews. 	X	X	X
Baseline allocation summary	PL-2	PL-2	PL-2

Every VA information system must be included/covered by an SSP that is compliant with guidance in the current versions of SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, and SP 800-53. VA systems include all systems owned and maintained by VA and that process VA information. The SSP must contain sufficient information to enable an implementation of the plan that is compliant with the intent and a subsequent determination of risk. The SSP provides an overview of system security requirements and the controls that are in place or planned to meet those requirements. SSPs are dynamic documents, undergoing initial development early in the system life cycle and constantly updated throughout the entire life cycle as materials are added and changed. SSPs are a major component in the authorization process for the system. SSPs should be considered sensitive documents and secured appropriately. SSPs are maintained in the VA approved FISMA database.

(3) **PL-3: System Security Plan Update**

Withdrawn from SP 800-53, Rev. 3, and incorporated into **PL-2: System Security Plan control.**

(4) **PL-4: Rules of Behavior (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT: <ul style="list-style-type: none"> Establishes and makes readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; and Receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the ROB, before authorizing access to information and the information system. 	X	X	X
Baseline allocation summary	PL-4	PL-4	PL-4

(a) The VA National ROB must be signed annually by all VA users of VA information systems or VA sensitive information.

(b) Electronic signatures are acceptable and recommended for use in acknowledging VA’s ROB. If signing manually using a hard copy, each page should be initialed and dated and the information completed on the last page.

(c) Appendix D of this Handbook includes VA’s National ROB, which encompasses VA’s Department-wide acceptability use policies.

(d) Contractors will sign the Contractor ROB that is contained in VA Handbook 6500.6.

(e) Both the VA National ROB and the Contractor ROB are included in VA’s OIT approved electronic Security/Privacy Awareness training.

(f) Other VA systems or external systems may require an additional ROB signed prior to access to that particular system.

(5) **PL-5: Privacy Impact Assessment (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit conducts a PIA on the information system in accordance with OMB policy.	X	X	X
Baseline allocation summary	PL-5	PL-5	PL-5

(6) PL-6: Security-Related Activity Planning (P3)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on VA operations (i.e., mission, functions, image, and reputation) and assets, individuals, and other organizations.	Not Selected	X	X
Baseline allocation summary	Not Selected	PL-6	PL-6

Security-related activities include, for example, security assessments, audits, system hardware and software maintenance, and contingency plan testing/exercises. VA advance planning and coordination includes both emergency and non-emergency (i.e., planned or non-urgent unplanned) situations.

d. Program Management (PM)

(1) PM-1: Information Security Program Plan [\(See Attachment 1\)](#)

(a) VA is required to implement security program management controls to provide a foundation for the organization’s information security program. The successful implementation of security controls for organizational information systems depends on the successful implementation of the VA’s Program Management controls.

(b) VA OIT information security has developed and disseminated VA Directive and Handbook 6500, along with other VA 6500 series of Handbooks that:

1. Provide an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
2. Provide sufficient information about the program management controls and common controls (including specification of parameters for any assignment and selection operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended;
3. Include roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
4. Is approved by OIT senior officials along with appropriate VA Administration Offices with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;

5. Is reviewed continuously and updated according to VA records management requirements; and

6. Is revised to address organizational changes and problems identified during plan implementation or subsequent reviews.

(c) Operating Units must create a local policy that states that VA Directive and Handbook 6500 are followed locally in implementing their local security program. Local policies may be more stringent than department policy, but not less stringent. Local policies should be reviewed/updated on an annual basis. Local SOPS should be created, as needed.

(2) **PM-2: Senior Information Security Officer (CISO)** ([See Attachment 1](#))

VA CIO has appointed a CISO with the mission and resources to coordinate, develop, implement, and maintain VA-wide information security program.

(3) **PM-3: Information Security Resources** ([See Attachment 1](#))

VA OIT ensures that all capital planning and investment requests include the resources necessary to implement the information security program and documents all exceptions to this requirement. This includes employing a business case/Exhibit 300/Exhibit 53 to record the resources required and ensuring that information security resources are available for expenditure as planned.

(4) **PM-4: Plan Of Action And Milestones (POA&M) Process** ([See Attachment 1](#))

(a) VA OIT has implemented a standardized process for ensuring that POA&Ms for the security program and the associated organizational information systems are maintained and documents the remedial information security actions to mitigate risk to VA operations and assets, individuals, other organizations, and the Nation.

(b) A POA&M is based on findings from SCAs, security impact analysis, continuous monitoring, and risk management activities.

(c) OMB and FISMA reporting guidance is used in developing the POA&M process.

(5) **PM-5: Information System Inventory** ([See Attachment 1](#))

OIT will develop and maintain an inventory of its information systems. Inventory will comply with current OMB and FISMA guidance, and include data points to identify physical location, logical location (MAC and IP address), ownership/assignment, tracking number, operating system type and version number, serial number, and model number. OIT organization responsible for the operations of the systems will provide the field with the procedures for conducting and maintaining the inventory of IT systems within VA.

(6) PM-6: Information Security Measures Of Performance ([See Attachment 1](#))

VA OIT will develop, monitor, and report on the results of information security measures of performance. This is accomplished by determining and establishing outcome based performance metrics and tracking the performance and providing feedback to the field to improve performance.

(7) PM-7: Enterprise Architecture (EA) ([See Attachment 1](#))

OIT's EA organization:

- (a) Aligns VA information system EA with Federal EA design;
- (b) Integrates enterprise architectural design with security requirements early in the SDLC;
- (c) Ensures security considerations and requirements are directly and explicitly related to VA's mission/business processes;
- (d) Effectively uses VA's RMF along with supporting security standards and guidelines to effectively address security requirements; and
- (e) Follows Federal Segment Architecture Methodology.

(8) PM-8: Critical Infrastructure Plan ([See Attachment 1](#))

VA OIT addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan. This is done by:

- (a) Defining the critical infrastructure for VA information systems.
- (b) Defining key critical infrastructure resources.
- (c) Defining key critical infrastructure personnel.

(9) PM-9: Risk Management Strategy ([See Attachment 1](#))

VA OIT has a comprehensive strategy to manage risk to VA operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; and is implementing the strategy consistently across VA.

(10) PM-10: Security Authorization Process ([See Attachment 1](#))

OIT has developed a security authorization process to manage and control VA information system security posture.

(11) **PM-11: Mission/Business Process Definition** ([See Attachment 1](#))

VA OIT is continually defining VA mission/business processes with consideration for information security and the resulting risk to VA operations and assets, individuals, other organizations, and the Nation and will revise the processes as necessary until an achievable set of protection needs are obtained. OIT works closely with VHA, VBA, and NCA to determine their missions and their security requirements and needs.

e. **Personnel Security (PS)**

(1) **PS-1: Personnel Security Policy and Procedures**

VA OIT in this Appendix has outlined VA’s system security controls based on the current version of SP 800-53 that are required for the effective implementation of the Personnel Security family. Local SOPs should be developed to facilitate the implementation and management of these controls at the local level, as needed. The Personnel Security controls and procedures in this Appendix are consistent with applicable laws: Executive Orders, policies, regulations, standards, and guidance, and will be periodically reviewed, and, when necessary, updated ([See Attachment 2](#)).

(2) **PS-2: Position Categorization (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
VA, per VA Directive and Handbook 0710: <ul style="list-style-type: none"> • Assigns a risk designation to all positions; • Establishes screening criteria for individuals filling those positions; and • Reviews and revises position risk designations consistent with policy and procedures as required by VA Directive and Handbook 0710. 	X	X	X
Baseline allocation summary	PS-2	PS-2	PS-2

(3) **PS-3: Personnel Screening (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
VA, per VA Directive and Handbook 0710: <ul style="list-style-type: none"> • Screens individuals prior to authorizing access to the information system; and • Rescreens individuals according to policy and procedures required by VA Directive and Handbook 0710. 	X	X	X
Baseline allocation summary	PS-3	PS-3	PS-3

(a) VA requires that all personnel be subject to an appropriate background screening (Special Agreement Check prior to permitting permanent access to VA information and

information systems, in accordance with requirements contained in VA Directive and Handbook 0710 and VA Directive 0735, *Homeland Security Presidential Directive 12 (HSPD-12) Program*.

(b) This includes VA applicants, appointees, employees, contractors, and other individuals as required in VA Directive and Handbook 0710.

(c) The COR will ensure screening is conducted for all contract personnel and HR personnel will ensure that screening is conducted for Federal employees and all other appointed workforce members.

(d) Position Descriptions: Supervisors will ensure position descriptions are written to reflect specific security responsibilities. Within this context, "significant security responsibilities", refer to employee obligations to protect VA sensitive information and to use such information, and the information derived from it, only in the execution of official duties.

(e) Background Investigations (BI): The level of BI required will vary, depending upon the sensitivity of the information to be handled and the risk and magnitude of loss or harm that could be caused by the individual. Procedures for completing BIs are contained in VA Directive and Handbook 0710.

(f) Contractors: All non-VA employees having access to VA information resources through a contract, agreement, or arrangement must meet the security levels defined by the contract, agreement, or arrangement.

(4) PS-4: Personnel Termination (P2)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit, upon termination of individual employment: <ul style="list-style-type: none"> Terminates information system access; Conducts exit interviews; Retrieves all security-related VA information system-related property; and Retains access to VA information and information systems formerly controlled by terminated individual. 	X	X	X
Baseline allocation summary	PS-4	PS-4	PS-4

(a) The Operating Unit must ensure appropriate personnel have access to official records, created by the departing VA employee, that are stored on VA information systems before the systems are recycled or disposed.

(b) When an employee is removed or discharged from his or her position, the following procedures should be implemented:

1. Termination of system access at the same time (or just before) the employee is notified of their dismissal or upon receipt of resignation; and

2. If applicable, during the “notice of removal/discharge” period the user may be assigned to a restricted area and function. This may be particularly true for employees capable of changing programs or modifying the system or applications.

(5) PS-5: Personnel Transfer (P2)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within VA and initiates <u>transfer/reassignment actions promptly</u> (See Attachment 3).	X	X	X
Baseline allocation summary	PS-5	PS-5	PS-5

(a) VA requires that Operating Units review information systems/facilities access authorizations when individuals are reassigned or transferred to other positions within the Operating Unit and initiate appropriate actions (e.g., reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts; and changing system access authorizations).

(b) When an employee transfers positions within the organization, both the losing and gaining services will adjust system menu access as necessary to ensure appropriate minimum-necessary access (only options required to perform his or her duties) is granted. When an employee resigns from his or her position, his or her supervisor will ensure that all access is removed. In both instances, the following must be ensured:

1. Employee no longer has possession of unneeded VA sensitive information media;
2. Employee has returned all unneeded keys and access devices as applicable;
3. Employee security codes, electronic signatures, system menu options, and security keys for both local and remote systems have been reviewed for either alteration or termination;
4. Employee is debriefed on his or her responsibility to protect the confidentiality of VA sensitive information used on the job from unauthorized disclosure; and
5. Appropriate personnel have access to official records created by the employee who has transferred or resigned that are stored on facility systems.

(c) When an employee or contractor is reassigned to a different position within VA, the reassigned position’s risk level will be reviewed by the new supervisor to ensure the previous risk designation is appropriate for the new position. For example a former low risk position may change to a moderate or high risk position. When a position’s risk level needs to be updated, the local HR Office should be notified for employees and the COR for contract employees.

(6) PS-6: Access Agreements (P3)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
VA: <ul style="list-style-type: none"> Ensures that users of VA information systems or VA sensitive information sign appropriate access agreements prior to being granted access; and Reviews/updates the access agreements as required (See Attachment 2). 	X	X	X
Baseline allocation summary	PS-6	PS-6	PS-6

(a) Access agreements include but are not limited to, non-disclosure agreements, acceptable use agreements, ROBs, and conflict-of-interest agreements (See **PL-4: Rules of Behavior** for VA’s ROB requirements).

(b) VA’s National ROB and Contractor ROB are reviewed, updated, as necessary. The current approved VA’s National ROB is attached as Appendix D of this Handbook. The current approved Contractor ROB is attached to VA Handbook 6500.6.

(7) PS-7: Third-Party Personnel Security (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
VA: <ul style="list-style-type: none"> Establishes personnel security requirements including security roles and responsibilities for third-party providers; Documents personnel security requirements; and Monitors provider compliance for third-party providers. 	X	X	X
Baseline allocation summary	PS-7	PS-7	PS-7

(a) VA includes personnel security requirements in acquisition-related documents.

(b) VA requires that Operating Units comply with the PS requirements for third-party providers (e.g., service bureaus, contractors, and other Operating Units providing information system development, information system services, outsourced applications, network and security management) established by VA Directive and Handbook 0710.

(8) **PS-8: Personnel Sanctions (P3)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
VA employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.	X	X	X
Baseline allocation summary	PS-8	PS-8	PS-8

(a) VA requires that Operating Units comply with the formal corrective action/sanction process established by the Office of HR Management for employees failing to comply with established information security policies and procedures.

(b) Violations of VA’s information security policies and procedures may result in disciplinary action, including dismissal and legal action against the offending employee(s), contractors, or other individuals requiring logical access to VA information or information systems, consistent with law or contract terms as applicable.

(c) The ISO will determine and provide evidence of a security violation. The employee’s supervisor will determine appropriate action and may, in conjunction with HR, take the necessary steps and apply appropriate corrective actions for employees who are non-compliant with the security policies and procedures. Actions may include, but are not limited to, progressive discipline or other resolutions. Appropriate legal authorities outside of VHA may levy civil or criminal sanctions as a result of a HIPAA security complaint.

f. **Risk Assessment (RA)**

(1) **RA-1: Risk Assessment Policy And Procedures**

VA OIT in this Appendix has outlined VA’s system security controls based on the current version of SP 800-53 that are required for the effective implementation of the Risk Assessment family. Local SOPs should be developed to facilitate the implementation and management of these controls at the local level, as needed. The Risk Assessment controls and procedures in this Appendix are consistent with applicable laws: Executive Orders, policies, regulations, standards, and guidance, and will be periodically reviewed, and, when necessary, updated ([See Attachment 2](#)).

(2) **RA-2: Security Categorization (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The System Owner: <ul style="list-style-type: none"> • Categorizes information and the information system in accordance with applicable Federal laws, Executive Orders, policies, regulations, standards, and guidance; • Documents the security categorization results (including supporting rationale) in the security plan for the information system; and • Ensures the security categorization decision is reviewed and approved by the AO or designee. 	X	X	X
Baseline allocation summary	RA-2	RA-2	RA-2

(a) All VA information systems must have their security categorized in accordance with FIPS 199 and current companion publication, SP 800-60, and the results of the categorization must be documented in the SSP. The security categorization describes the potential adverse impacts to VA operations and assets, individuals, other organizations, and the Nation should the information and information system be compromised through a loss of confidentiality, integrity, or availability. This determination, along with the likelihood of compromise occurring and the extent of protection required by law establishes the level of security adequate to protect the data as required by OMB circular A-130, Appendix III.

(b) To complete the security categorization of the information system the Operating Unit will follow the procedures and requirements designated in VA Handbook 6500.

(c) Nationally developed systems will have this categorization completed during the initiation phase of the SDLC and the categorization and baseline will be provided to the field as part of the SSP in the authorization package. Locally developed systems must ensure categorizations are determined at the local level.

(d) The AO or designee will review and approve an information system’s security categorization as part of the review and approval of the SSP in accordance with the RMF described in the current version of SP 800-37 and VA Directive 6500.

(3) **RA-3: Risk Assessment (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The System Owner: <ul style="list-style-type: none"> • Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; • Documents risk assessment results (See Attachment 2); • Reviews risk assessment results (See Attachment 2); and • Updates the risk assessment whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system (See Attachment 2). 	X	X	X
Baseline allocation summary	RA-3	RA-3	RA-3

VA System Owners will perform system risk assessments using VA OIT approved methodologies.

(4) **RA-4: Risk Assessment Update**

Withdrawn from SP 800-53, Rev. 3, and incorporated into **RA-3: Risk Assessment** control.

(5) RA-5: Vulnerability Scanning (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
<p>OIT</p> <ul style="list-style-type: none"> • Scans for vulnerabilities in the information system and hosted applications and when new vulnerabilities potentially affecting the system/applications are identified and reported (See Attachment 3); • Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for: <ul style="list-style-type: none"> ii. Enumerating platforms, software flaws, and improper configurations; iii. Formatting and making transparent, checklists and test procedures; and iv. Measuring vulnerability impact. • Analyzes vulnerability scan reports and results from SCAs; • Remediates legitimate vulnerabilities in accordance with an organizational assessment of risk (See Attachment 3); and • Shares information obtained from the vulnerability scanning process and SCAs with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies). 	X	X	X
(1) OIT employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned.	Not Selected	X	X
(2) OIT updates the list of information system vulnerabilities scanned periodically or when new vulnerabilities are identified and reported (See Attachment 3).	Not Selected	Not Selected	X
(3) OIT employs vulnerability scanning procedures that can demonstrate the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).	Not Selected	Not Selected	X
(4) OIT attempts to discern what information about the information system is discoverable by adversaries.	Not Selected	Not Selected	X
(5) OIT includes privileged access authorization to information system <u>components</u> for selected vulnerability scanning activities to facilitate more thorough scanning (See Attachment 3).	Not Selected	Not Selected	X
(7) OIT employs automated mechanisms to detect the presence of unauthorized software on organizational information systems and notify designated organizational officials (See Attachment 3).	Not Selected	Not Selected	X
Baseline allocation summary	RA-5	RA-5 (1)	RA-5 (1)(2)(3) (4)(5)(7)

(a) The security categorization of the information system guides the frequency and comprehensiveness of the vulnerability scans.

(b) Vulnerability scanning includes scanning for specific functions, ports, protocols, and services that should not be accessible to users or devices and for improperly configured or incorrectly operating information flow mechanisms.

(c) Vulnerability scanning tools will include the capability to readily update the list of vulnerabilities scanned. Each facility will update the list of information system vulnerabilities as required or when significant new vulnerabilities are identified and reported. This process may be conducted independently or as a coordinated effort with VA-NSOC.

(d) Vulnerability analysis for custom software and applications may require additional, more specialized techniques and approaches (e.g., web-based application scanners, source code reviews, source code analyzers).

(e) The information obtained from the vulnerability scanning process is freely shared with appropriate personnel throughout the facility to help eliminate similar vulnerabilities in other information systems. However, vulnerability scans are considered to be VA sensitive information and should be distributed, maintained and disposed of appropriately.

(f) System Owners, system managers, and other OIT personnel will review their systems on an ongoing basis to identify and when possible, eliminate unnecessary services (e.g., File Transfer Protocol, Hyper Text Transfer Protocol (HTTP), Internet Information Services).

(g) The Operating Unit utilizes patch and vulnerability management in accordance with the **SI-2, Flaw Mediation**, control outlined in this Handbook.

g. System and Services Acquisition (SA)

(1) SA-1: System and Services Acquisition Policy and Procedures

(a) VA OIT in this Appendix has outlined VA's system security controls based on the current version of SP 800-53 that are required for the effective implementation of the System and Services Acquisition family. Local SOPs should be developed to facilitate the implementation and management of these controls at the local level, as needed. The System and Services Acquisitions controls and procedures in this Appendix are consistent with applicable laws: Executive Orders, policies, regulations, standards, and guidance, and will be periodically reviewed, and, when necessary, updated ([See Attachment 2](#)).

(b) For additional information regarding SA see VA Handbook 6500.6.

(2) **SA-2: Allocation of Resources (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT management: <ul style="list-style-type: none"> Includes a determination of information security requirements for the information system in mission/business process planning; Determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process; and Establishes a discrete line item for information security in organizational programming and budgeting documentation. 	X	X	X
Baseline allocation summary	SA-2	SA-2	SA-2

The system life cycle requires consideration of IT security in the budget request. IT management must comply with the Department’s capital asset budget planning process and follow a methodology consistent with the current version of SP 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*. OMB Circular A-11, *Preparation, Submission and Execution of the Budget*, especially Part 7, as well as OMB Memorandum M-00-07, *Incorporating and Funding Security in Information Systems Investments*, require that security be built into and funded as part of the system architecture.

(3) **SA-3: Life Cycle Support (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT: <ul style="list-style-type: none"> Manages the information system using a SDLC methodology that includes information security considerations; Defines and documents information system security roles and responsibilities throughout the SDLC; and Identifies individuals having information system security roles and responsibilities. 	X	X	X
Baseline allocation summary	SA-3	SA-3	SA-3

(a) All new VA systems will include the capability for recovery/decryption of any encrypted/protected data. Successful demonstration that the recovery/decryption process works is required prior to being granted any authorization to operate (ATO). Systems that cannot provide such recovery/decryption capabilities must be reviewed by the OIG, then subsequently agreed to by VA CIO prior to system development and also prior to receiving ATO.

(b) All new VA systems must include read-only capability for OIG and other authorized oversight and law enforcement entities. This requirement must be functional prior to being granted any ATO and systems that cannot provide this capability must be agreed to by VA's CIO prior to system development and also prior to receiving ATO.

(c) The SDLC is a proven series of steps and tasks used to build and maintain quality systems faster, at lower costs, and with less risk. Each information system operates in one of the below stages of system development. Any locally developed system will follow the life cycle steps and be assessed and authorized prior to implementation. During the development of any system, security requirements will be defined. The steps of the SDLC are:

1. Initiation;
2. Acquisition and Development;
3. Implementation and Assessment;
4. Operations and Maintenance; and
5. Disposal.

(d) Operating Units should refer to VA Handbook 6500.5 for information on IT security considerations that occur in each of the phases of the SDLC.

(4) SA-4: Acquisitions (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit includes the following requirements and/or specifications, explicitly or by reference, in <u>information system</u> acquisition contracts based on an assessment of risk and in accordance with applicable Federal laws, Executive Orders, policies, regulations, and standards: <ul style="list-style-type: none"> • Security functional requirements/specifications; • Security-related documentation requirements; and • Developmental and evaluation-related assurance requirements. 	X	X	X
(1) The Operating Unit requires in acquisition documents that vendors/contractors provide information describing the functional properties of the security controls to be employed within the information system, information system components, or information system services in sufficient detail to permit analysis and testing of the controls.	Not Selected	X	X
(2) The Operating Unit requires in acquisition documents that vendors/contractors provide information describing the design and implementation details of the security controls to be employed within the information system, information system components, or information system services (including functional interfaces among control components) in sufficient detail to permit analysis and testing of the controls.	Not Selected	Not Selected	X
(4) The Operating Unit ensures that each information system component acquired is explicitly assigned to an information system, and that the owner of the system acknowledges this assignment.	Not Selected	X	X
Baseline allocation summary	SA-4	SA-4 (1)(4)	SA-4 (1)(2)(4)

(a) The acquisition documents for information systems, information system components, and information system services include, either explicitly or by reference, security requirements that describe: (i) required security capabilities (i.e., security needs and, as necessary, specific security controls and other specific FISMA requirements); (ii) required design and development processes; (iii) required test and evaluation procedures; and (iv) required documentation.

(b) Acquisition documents include requirements for appropriate information system documentation. The documentation addresses user and system administrator guidance and information regarding the implementation of the security controls in the information system. The level of detail required in the documentation is based on the security categorization for the information system. In addition, the required documentation includes security configuration settings and security implementation guidance.

(c) Requirements in acquisition documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented.

(d) Additional contract security policy and procedures are outlined in VA Handbook 6500.6.

(5) SA-5: Information System Documentation (P2)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
<p>The Operating Unit:</p> <ul style="list-style-type: none"> • Obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes: <ul style="list-style-type: none"> i. Secure configuration, installation, and operation of the information system; ii. Effective use and maintenance of security features/functions; and iii. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions. • Obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes: <ul style="list-style-type: none"> i. User-accessible security features/functions and how to effectively use those security features/functions; ii. Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and iii. User responsibilities in maintaining the security of the information and information system. • Documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent. 	X	X	X
(1) The Operating Unit obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing.	Not Selected	X	X
(2) The Operating Unit obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the security-relevant external interfaces to the information system with sufficient detail to permit analysis and testing.	Not Selected	Not Selected	X
(3) The Operating Unit obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.	Not Selected	X	X
Baseline allocation summary	SA-5	SA-5 (1)(3)	SA-5 (1)(2)(3)

System documentation contains descriptions of the system hardware, software, policies, standards, procedures, and approvals related to the system life cycle and to formalize the system’s security controls. VA requires that Operating Units ensure that sufficient documentation exists to provide an operating reference to effectively use software/hardware, and formal security and operational procedures have been documented, including the adequate completion of A&A processes. Documentation includes, but is not limited to, all documentation of the security planning, A&A process, configuration baseline of the hardware and software associated with the system, system POA&Ms, user manuals for software, in-house application documentation, any vendor supplied documentation, SOPs, network diagrams and documentation on setups of routers and switches, software and hardware testing procedures and results, hardware replacement agreements, and vendor maintenance agreements and maintenance records.

(6) SA-6: Software Usage Restrictions (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT: <ul style="list-style-type: none"> • Uses software and associated documentation in accordance with contract agreements and copyright laws; and • Employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; • Controls and documents the use of peer-to-peer (P2P) file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work. 	X	X	X
Baseline allocation summary	SA-6	SA-6	SA-6

(a) Tracking systems employed to control copying and distribution of software and associated documentation can include, for example, simple spreadsheets or fully automated, specialized applications depending on the needs of the organization.

(b) OIT prohibits the use of unauthorized 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.

(7) SA-7: User-Installed Software (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT enforces explicit rules governing the installation of software by users.	X	X	X
Baseline allocation summary	SA-7	SA-7	SA-7

OIT identifies what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software whose pedigree with regard to being potentially malicious is unknown or suspect). No software will be installed on VA information systems or VA network by users unless approved by OIT or system management.

(8) SA-8: Security Engineering Principles (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.	Not Selected	X	X
Baseline allocation summary	Not Selected	SA-8	SA-8

OIT designs and implements an information system using security engineering principles recommended by the current version of SP 800-27A, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*. The application of security engineering principles is primarily targeted at new development information systems or systems undergoing major upgrades and is integrated into the SDLC. For legacy information systems, security engineering principles are applied to system upgrades and modifications to the extent feasible, given the current state of the hardware, software, and firmware within the system. Examples of security engineering principles include, for example, developing layered protections; establishing sound security policy, architecture, and controls as the foundation for design; incorporating security into the SDLC; delineating physical and logical security boundaries; ensuring system developers and integrators are trained on how to develop secure software; tailoring security controls to meet organizational and operational needs; and reducing risk to acceptable levels, thus enabling informed risk management decisions.

(9) SA-9: External Information System Services (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT: <ul style="list-style-type: none"> Requires that providers of external information system services comply with VA information security requirements and employ appropriate security controls in accordance with applicable Federal laws, Executive Orders, policies, regulations, standards, and guidance; Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and Monitors security control compliance by external service providers. 	X	X	X
Baseline summary allocation	SA-9	SA-9	SA-9

(a) An external information system service is a service that is implemented outside of the authorization boundary of VA information system (i.e., a service that is used by, but not a part of, VA information system). Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges. The responsibility for adequately mitigating risks arising from the use of external information system services remains with the program office requesting the service. An appropriate chain of trust must be established with external service providers when dealing with the many issues associated with information security. For services external to VA, a chain of trust requires that VA establish and retain a level of confidence that each participating provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered to VA. The extent and nature of this chain of trust varies based on the relationship between VA and the external provider. Where a sufficient level of trust cannot be established in the external services and/or service providers, VA employs compensating security controls or accepts the greater degree of risk. The external information system services documentation includes government, service provider, and end user security roles and responsibilities, and any service-level agreements. Service-level agreements define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of noncompliance.

(b) When relying on contractors, VA transfers operational responsibilities for performing one or more IT service(s) to one or more external providers. However, the overall responsibility and accountability for securing the information and systems remains with VA. Therefore, VA requires that the Operating Units ensure that third-party providers of information system services employ adequate security controls in accordance with applicable Federal laws, Executive Orders, policies, regulations, standards, guidance, and established service level agreements. VA also requires that the Operating Units monitor security control compliance as discussed further in this Appendix. See VA Handbook 6500.6 for additional information.

(10) SA-10: Developer Configuration Management (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT requires that information system developers/integrators: <ul style="list-style-type: none"> • Perform configuration management during information system design, development, implementation, and operation. • Manage and control changes to the information system; • Implement only organization-approved changes; • Document approved changes to the information system; and • Track security flaws and flaw resolution. 	Not Selected	X	X
Baseline allocation summary	Not Selected	SA-10	SA-10

(11) SA-11: Developer Security Testing (P2)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT requires that information system developers/integrators, in consultation with associated security personnel (including security engineers): <ul style="list-style-type: none"> • Create and implement a security test and evaluation plan; • Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and • Document the results of the security testing/evaluation and flaw remediation processes. 	Not Selected	X	X
Baseline allocation summary	Not Selected	SA-11	SA-11

(a) Developmental security test results are used to the greatest extent feasible after verification of the results and recognizing that these results are impacted whenever there have been security-relevant modifications to the information system subsequent to developer testing. Test results may be used in support of the security authorization process for the delivered information system.

(b) Systems under development should not process “live data” or do any real processing in which true business decisions will be based. Test data that is de-identified should be used to test systems and develop systems that have not yet undergone security A&A. Furthermore, systems that are in development (pilot, proof-of-concept, or prototype) should not be attached to VA networks without first being assessed and authorized.

(12) SA-12: Supply Chain Protection (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit protects against supply chain threats by employing security <u>measures</u> as part of a comprehensive, defense-in-breadth information security strategy (See Attachment 3).	Not Selected	Not Selected	X
Baseline allocation summary	Not Selected	Not Selected	SA-12

A defense-in-breadth approach helps to protect information systems (including the IT products that compose those systems) throughout the SDLC (i.e., during design and development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement). This is accomplished by the identification, management, and elimination of vulnerabilities at each phase of the life cycle and the use of complementary, mutually reinforcing strategies to mitigate risk.

(13) SA-13: Trustworthiness (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT requires that the information system meets necessary level of <u>trustworthiness</u> according to risk-based criteria (See Attachment 3).	Not Selected	Not Selected	X
Baseline allocation summary	Not Selected	Not Selected	SA-13

(a) Trustworthiness is a characteristic or property of an information system that expresses the degree to which the system can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system. Trustworthy information systems are systems that are capable of being trusted to operate within defined levels of risk despite the environmental disruptions, human errors, and purposeful attacks that are expected to occur in the specified environments of operation. Two factors affecting the trustworthiness of an information system include:

1. Security functionality - Appropriate security functionality for the information system can be obtained by using the RMF (Steps 1, 2, and 3) in the core document to select and implement the necessary management, operational, and technical security controls necessary to mitigate risk to VA operations and assets, individuals, other organizations, and the Nation.

2. Security assurance - Appropriate security assurance can be obtained by: (i) the actions taken by developers and implementers of security controls with regard to the design, development, implementation, and operation of those controls; and (ii) the actions taken by assessors to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system.

(b) Developers and implementers can increase the assurance in security controls by employing well-defined security policy models, structured, disciplined, and rigorous hardware and software development techniques, and sound system/security engineering principles. Assurance is also based on the assessment of evidence produced during the initiation, acquisition/development, implementation, and operations/maintenance phases of the SDLC.

(14) **SA-14: Critical Information System Components (P4)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT: <ul style="list-style-type: none"> Determines <u>list of critical information system components that require re-implementation</u>; and Re-implements or custom develops such information system components. 	Not Selected	Not Selected	Not Selected
Baseline allocation summary	Not Selected	Not Selected	Not Selected

VA does not require, at this time, application of control **SA-14: Critical Information System Components**. OIT may, at their discretion, elect to implement this control.

h. **System and Communications Protection (SC)**

(1) **SC-1: System and Communications Protection Policy and Procedures**

VA OIT in this Appendix has outlined VA’s system security controls based on the current version of SP 800-53 that are required for the effective implementation of the System and Communications Protection family. Local SOPs should be developed to facilitate the implementation and management of these controls at the local level, as needed. The System and Communications Protection controls and procedures in this Appendix are consistent with applicable laws: Executive Orders, policies, regulations, standards, and guidance, and will be periodically reviewed, and, when necessary, updated ([See Attachment 2](#)).

(2) **SC-2: Application Partitioning (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system separates user functionality (including user interface services) from information system management functionality.	Not Selected	X	X
Baseline allocation summary	Not Selected	SC-2	SC-2

Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from information system management functionality is either physical or logical and is accomplished by using different computers, different computer processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate. An example of this type of separation is observed in web administrative interfaces that use separate authentication methods for users of any other information system resources. This may include isolating the administrative interface on a different domain and with additional access controls.

(3) **SC-3: Security Function Isolation (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system isolates security functions from non-security functions.	Not Selected	Not Selected	X
Baseline allocation summary	Not Selected	Not Selected	SC-3

The information system isolates security functions from non-security functions by means of an isolation boundary (implemented via partitions and domains) that controls access to and protects the integrity of, the hardware, software, and firmware that perform those security functions. The information system maintains a separate execution domain (e.g., address space) for each executing process.

(4) **SC-4: Information in Shared Resources (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system prevents unauthorized and unintended information transfer via shared system resources.	Not Selected	X	X
Baseline allocation summary	Not Selected	SC-4	SC-4

The purpose of this control is to prevent information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system. Control of information in shared resources is also referred to as object reuse. This control does not address:

- (a) Information remanence which refers to residual representation of data that has been in some way nominally erased or removed;
- (b) Covert channels where shared resources are manipulated to achieve a violation of information flow restrictions; or
- (c) Components in the information system for which there is only a single user/role.

(5) **SC-5: Denial of Service Protection (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT ensures that the information system protects against or limits the effects of the types of DoS attacks (See Attachment 2).	X	X	X
Baseline allocation summary	SC-5	SC-5	SC-5

A variety of technologies exist to limit, or in some cases, eliminate the effects of DoS attacks. For example, boundary protection devices can filter certain types of packets to protect devices on an organization’s internal network from being directly affected by DoS attacks. Employing increased capacity and bandwidth combined with service redundancy may reduce the susceptibility to some DoS attacks.

(6) **SC-6: Resource Priority (P4)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system limits the use of resources by priority.	Not Selected	Not Selected	Not Selected
Baseline allocation summary	Not Selected	Not Selected	Not Selected

VA does not require, at this time, application of control **SC-6: Resource Priority**. OIT may, at their discretion, elect to limit the use of resources by priority.

(7) **SC-7: Boundary Protection**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT: <ul style="list-style-type: none"> • Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and • Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with organizational security architecture. 	X	X	X
(1) OIT physically allocates publicly accessible information system components to separate subnetworks with separate physical network interfaces.	Not Selected	X	X
(2) The information system prevents public access into the organization's internal networks except as appropriately mediated by managed interfaces employing boundary protection devices.	Not Selected	X	X
(3) OIT limits the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic.	Not Selected	X	X
(4) OIT: <ul style="list-style-type: none"> • Implements a managed interface for each external telecommunication service; • Establishes a traffic flow policy for each managed interface; • Employs security controls as needed to protect the confidentiality and integrity of the information being transmitted; • Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; • Reviews exceptions to the traffic flow policy as required (See Attachment 2); and • Removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need. 	Not Selected	X	X
(5) The information system at managed interfaces, denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).	Not Selected	X	X
(6) OIT prevents the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.	Not Selected	Not Selected	X
(7) The information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks.	Not Selected	X	X
(8) The information system routes <u>internal communications traffic</u> to <u>external networks</u> through authenticated proxy servers within the managed interfaces of boundary protection devices (See Attachment 2).	Not Selected	Not Selected	X
Baseline allocation summary	SC-7	SC-7 (1)(2)(3) (4)(5)(7)	SC-7 (1)(2)(3) (4)(5)(6) (7)(8)

(a) Restricting external web traffic only to organizational web servers within managed interfaces and prohibiting external traffic that appears to be spoofing an internal address as the source are examples of restricting and prohibiting communications. Managed interfaces employing boundary protection devices include, for example, proxies, gateways, routers, firewalls, guards, or encrypted tunnels arranged in effective security architecture (e.g., routers protecting firewalls and application gateways residing on a protected subnetwork commonly referred to as a demilitarized zone).

(b) VA considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may include third-party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions. Therefore, when this situation occurs VA either implements appropriate compensating security controls or explicitly accepts the additional risk.

(c) Publicly accessible information system components include, for example, public web servers.

(d) The Trusted Internet Connection initiative is an example of limiting the number of managed network access points.

(e) External networks are networks outside the control of the organization. Proxy servers support logging individual TCP sessions and blocking specific Uniform Resource Locators, domain names, and IP addresses. Proxy servers are also configurable with organization defined lists of authorized and unauthorized Web sites.

(8) SC-8: Transmission Integrity (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system protects the integrity of transmitted information.	Not Selected	X	X
(1) OIT employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.	Not Selected	X	X
Baseline allocation summary	Not Selected	SC-8 (1)	SC-8 (1)

(a) This control applies to communications across internal and external networks. If an organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission integrity. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles VA either implements appropriate compensating security controls or explicitly accepts the additional risk.

(b) Alternative physical protection measures include, for example, protected distribution systems.

(9) SC-9: Transmission Confidentiality (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system protects the confidentiality of transmitted information.	Not Selected	X	X
(1) OIT employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures. (See Attachment 3).	Not Selected	X	X
Baseline allocation summary	Not Selected	SC-9 (1)	SC-9 (1)

(a) This control applies to communications across internal and external networks. If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, VA either implements appropriate compensating security controls or explicitly accepts the additional risk.

(b) Alternative physical protection measures include, for example, protected distribution systems.

(c) Private Branch Exchange (PBX) Voice/Data Telephone Systems

1. PBX security includes maintaining an audit trail to capture the date, time, user(s), and activities performed on the PBX system and implementing adequate investigations and audit methods to ensure appropriate and authorized access to the PBX system.

2. To reduce exposure to security risks, the following actions should be taken, if possible:

a. Assign authorization codes randomly on a need-to-have basis;

- b. Safeguard authorization codes and change them frequently;
- c. Limit remote access trunks to domestic calling;
- d. Implement the time-of-day PBX option;
- e. Implement a system-wide barrier code;
- f. Do not use or allow the use of trivial passwords such as "1111" or "2222";
- g. Do not include programmable function keys or speed dialing keys in the password;

h. Monitor telephone bills regularly, looking for increased activity. If increased activity is suspected, contact the telephone vendor to request an audit of the PBX system to determine if fraud has occurred. Use of the PBX system to monitor telephone calls must be authorized by the facility director/program manager; and

i. All unused telephone jacks should be disabled as soon as possible to prevent unauthorized usage.

(d) Electronic Mail

1. The VA e-mail system will be used for authorized government purposes and will contain only non-sensitive information unless the information is appropriately encrypted with VA approved encryption technologies. VA Directive 6609 provides policy that can be used for mailing personally identifiable and sensitive information when encrypted e-mail is not available. E-mail users must exercise common sense, good judgment, and propriety in the use of this government resource. E-mail is not inherently confidential and users should have no expectation of privacy when using government mail systems. A technical or administrative problem sometimes causes a situation where a system manager or management official may need to review e-mail messages. Such reviews will be handled in accordance with the Operating Unit's "Electronic Mail Review" SOP. The ISO will provide concurrence for requests for removal of e-mail messages when warranted.

2. Auto-forwarding of e-mail messages to addresses outside the VA network is strictly prohibited.

(e) Facsimile (Fax) Machines

Care should be taken to assure confidentiality when faxing sensitive information. Facilities must take reasonable steps to ensure the fax transmission is sent to the appropriate destination. Following are the precautions that must be taken to protect the security of fax transmissions:

1. VA facilities should only transmit individually-identifiable information via fax when no other means exists to provide the requested information in a reasonable manner or timeframe. VA health care facilities need to ensure individually-identifiable information is sent on a machine that is not accessible to the general public.

2. The HIPAA Security Rule does not apply to faxing because the information is not in electronic format prior to sending. The HIPAA Privacy Rule requirements do, however, apply when faxing PHI. In the event that a fax is sent via automated systems, or fax back from a computer, then the HIPAA Security Rule does apply because the information was already in electronic format before it was transmitted.

3. Do not fax individually-identifiable information unless someone is there to receive the information or the fax machine is in a secured location (e.g., locked room).

4. The following statement should be used on fax cover sheets: "This fax is intended only for the use of the person or office to which it is addressed and may contain information that is privileged, confidential, or protected by law. All others are hereby notified that the receipt of this fax does not waive any applicable privilege or exemption for disclosure and that any dissemination, distribution, or copying of this communication is prohibited. If you have received this fax in error, please notify this office immediately at the telephone number listed above."

5. Staff should be trained to double check the recipient's fax number before transmittal and to confirm delivery by telephone or review of the appropriate confirmation of fax transmittal. If there has been an error, the incorrect recipient must be immediately contacted and requested to return or destroy the fax.

6. Fax machines will be placed in controlled areas within VA office space sufficient to physically limit access to the machine by authorized VA staff only. Use of fax machines will be limited to authorized office personnel, and as necessary, or as equipment features allow, security codes used to prevent unauthorized use to transmit, or receive faxed documents.

7. Staff periodically reminds regular fax recipients to provide notification in the event that their fax number changes.

8. Fax transmittal summaries and confirmation sheets are saved and reviewed periodically for unauthorized access or use.

9. Staff have pre-programmed and tested destination numbers in order to minimize the potential for human error.

(f) Mailing of Personally Identifiable and Sensitive Information – for VA's policy see VA Directive 6609.

(10) **SC-10: Network Disconnect (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system terminates the network connection associated with a communications session at the end of the session or after a period of inactivity (See Attachment 3).	Not Selected	X	X
Baseline allocation summary	Not Selected	SC-10	SC-10

This control applies to both internal and external networks. Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating-system level, or de-allocating networking if multiple application sessions are using a single, operating system-level network connection. The time period of inactivity may, as the System Owner deems necessary, be a set of time periods by type of network access or for specific accesses.

(11) **SC-11: Trusted Path (P4)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system establishes a trusted communications path between the user and the following security functions of the system: <u>security functions (including authentication and reauthentication)</u> .	Not Selected	Not Selected	Not Selected
Baseline allocation summary	Not Selected	Not Selected	Not Selected

VA does not require, at this time, application of control **SC-11: Trusted Path**. OIT may, at their discretion, elect to establish a trusted communications path between the user and the listed security functions of the system.

(12) **SC-12: Cryptographic Key Establishment and Management (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT establishes and manages cryptographic keys for required cryptography employed within the information system.	X	X	X
(1) OIT maintains availability of information in the event of the loss of cryptographic keys by users.	Not Selected	Not Selected	X
Baseline allocation summary	SC-12	SC-12	SC-12 (1)

Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. In addition to being required for the effective operation of a cryptographic mechanism, effective cryptographic key management provides protections to maintain the availability of the information in the event of the loss of cryptographic keys by users.

(13) **SC-13: Use of Cryptography (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT requires that the information system implements required cryptographic protections using cryptographic modules that comply with applicable Federal laws, Executive Orders, policies, regulations, standards, and guidance.	X	X	X
Baseline allocation summary	SC-13	SC-13	SC-13

(a) When cryptography is required and employed within information systems, OIT must comply with applicable Federal laws, policies, regulations, standards, and guidance, including FIPS 140-2 (or its successor) validated encryption which requires the system to perform all cryptographic operations (including key generation) using FIPS 140-2 (or its successor) validated cryptographic modules operating in approved modes of operation.

(b) VA sensitive information must be encrypted during transmissions and at rest when outside of VA owned or managed facilities (e.g., medical centers, CBOCs, regional offices, etc.).

(14) **SC-14: Public Access Protections (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT requires that the information system protects the integrity and availability of publicly available information and applications.	X	X	X
Baseline allocation summary	SC-14	SC-14	SC-14

The purpose of this control is to ensure that organizations explicitly address the protection needs for public information and applications with such protection likely being implemented as part of other security controls.

(15) **SC-15: Collaborative Computing Devices (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT: <ul style="list-style-type: none"> Prohibits remote activation of collaborative computing devices unless an exception is defined when an approved collaborative tool is necessary for communications (See Attachment 3); and Provides an explicit indication of use to users physically present at the devices. 	X	X	X
Baseline allocation summary	SC-15	SC-15	SC-15

(a) The System Owner disables or removes collaborative computing devices from information systems after authorized use.

(b) Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.

(16) **SC-16: Transmission Of Security Attributes (P4)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system associates security attributes with information exchanged between information systems.	Not Selected	Not Selected	Not Selected
Baseline allocation summary	Not Selected	Not Selected	Not Selected

VA does not require, at this time, application of control **SC-16: Transmission of Security Attributes**. OIT may, at their discretion, elect to associate security attributes with information exchanged between information systems.

(17) **SC-17: Public Key Infrastructure Certificates (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
VA issues PKI certificates under an appropriate certificate policy or obtains PKI certificates under an appropriate certificate policy from an approved service provider (See Attachment 2).	Not Selected	X	X
Baseline allocation summary	Not Selected	SC-17	SC-17

For user certificates, each organization attains certificates from an approved, shared service provider, as required by OMB policy. For Federal agencies operating a legacy PKI cross-certified with the Federal Bridge Certification Authority at medium assurance or higher, this Certification Authority will suffice. This control focuses on certificates with a visibility external to the information system and does not include certificates related to internal system operations, for example, application-specific time services.

(18) **SC-18: Mobile Code (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT: <ul style="list-style-type: none"> • Defines acceptable and unacceptable mobile code and mobile code technologies; • Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and • Authorizes, monitors, and controls the use of mobile code within the information system. 	Not Selected	X	X
Baseline allocation summary	Not Selected	SC-18	SC-18

(a) OIT and Operating Units implementing mobile code must ensure compliance with the current version of SP 800-19, *Mobile Agent Security*, and SP 800-28, *Guidelines on Active Content and Mobile Code*, to ensure adequate controls have been considered. This methodology requires information System Owners to assess the risk of harm to IT systems from allowing mobile code, such as JavaScript, to run on its systems. The mobile code and mobile agent computing paradigm pose several privacy and security concerns, but applications are currently being developed by industry, government, and academia for use in such areas as telecommunications systems, PDA, information management, parallel processing, and computer simulation. Security issues include: authentication, identification, secure messaging, certification, trusted third-parties, non-repudiation, and resource control. Mobile agent frameworks must be able to counter new threats as agent hosts must be protected from malicious agents, agents must be protected from malicious hosts, and agents must be protected from malicious agents. NIST currently has a project under way to evaluate security countermeasures to attacks from malicious mobile code.

(b) Decisions regarding the employment of mobile code within organizational information systems are based on the potential for the code to cause damage to the system if used maliciously. Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations.

(19) **SC-19: Voice Over Internet Protocol (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT: <ul style="list-style-type: none"> Establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if used maliciously; and Authorizes, monitors, and controls the use of VoIP within the information system. 	Not Selected	X	X
Baseline allocation summary	Not Selected	SC-19	SC-19

VA requires that System Owners implement protective measures consistent with the requirements in the current version of SP 800-58, *Security Considerations for Voice Over IP Systems*.

(20) **SC-20: Secure Name/Address Resolution Service (Authoritative Source) (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries.	X	X	X
(1) The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.	X	X	X
Baseline allocation summary	SC-20 (1)	SC-20 (1)	SC-20 (1)

(a) This control enables remote clients to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. A domain name server is an example of an information system that provides name/address resolution service. Digital signatures and cryptographic keys are examples of additional artifacts. Domain name server resource records are examples of authoritative data. Information systems that use technologies other than the domain name server to map between host/service names and network addresses provide other means to assure the authenticity and integrity of response data. The domain name server security controls are consistent with, and referenced from, OMB Memorandum M-08-23, *Securing the Federal Government's Domain Name System Infrastructure*.

(b) An example of the "means to indicate the security status of child subspaces" as described in the second row of the table above is through the use of delegation signer resource records in the domain name server.

(21) SC-21: Secure Name/Address Resolution Service (Recursive or Caching Resolver) (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT authorizes the performance of data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources when requested by client systems.	Not Selected	Not Selected	X
Baseline allocation summary	Not Selected	Not Selected	SC-21

(a) A recursive resolving or caching domain name server is an example of an information system that provides name/address resolution service for local clients.

(b) Authoritative domain name servers are examples of authoritative sources. Information systems that use technologies other than the domain name server to map between host/service names and network addresses provide other means to enable clients to verify the authenticity and integrity of response data.

(22) SC-22: Architecture and Provisioning for Name/Address Resolution Service (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.	Not Selected	X	X
Baseline allocation summary	Not Selected	SC-22	SC-22

A domain name server is an example of an information system that provides name/address resolution service. To eliminate single points of failure and to enhance redundancy, there are typically at least two authoritative domain name server, one configured as primary and the other as secondary. Additionally, the two servers are commonly located in two different network subnets and geographically separated (i.e., not located in the same physical facility). With regard to role separation, domain name server with an internal role, only process name/address resolution requests from within the organization (i.e., internal clients). Domain name servers with an external role only process name/address resolution information requests from clients external to the organization (i.e., on the external networks including the Internet). The set of clients that can access an authoritative domain name server in a particular role is specified by the organization (e.g., by address ranges, explicit lists).

(23) **SC-23: Session Authenticity (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT provides mechanisms to protect the authenticity of communications sessions for the information system.	Not Selected	X	X
Baseline allocation summary	Not Selected	SC-23	SC-23

This control focuses on communications protection at the session, versus packet, level. The intent of this control is to establish grounds for confidence at each end of a communication's session in the ongoing identity of the other party and in validity of the information being transmitted. For example, this control addresses man-in-the-middle attacks including session hijacking or insertion of false information into a session. This control is only implemented where deemed necessary by the organization (e.g., sessions in service-oriented architectures providing web-based services).

(24) **SC-24: Fail in Known State (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system fails to a <u>known-state</u> when certain types of errors occur to preserve the system state (See Attachment 3).	Not Selected	Not Selected	X
Baseline allocation summary	Not Selected	Not Selected	SC-24

Failure in a known state can address safety or security in accordance with the mission/business needs of the organization. Failure in a known secure state helps prevent a loss of confidentiality, integrity, and availability in the event of a failure of the information system or a component of the system. Failure in a known safe state helps prevent systems from failing to a state that may cause injury to individuals or destruction to property. Preserving information system state information facilitates system restart and return to the operational mode of the organization with less disruption of mission/business processes.

(25) **SC-25: Thin Nodes (P4)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system employs processing components that have minimal functionality and information storage.	Not Selected	Not Selected	Not Selected
Baseline allocation summary	Not Selected	Not Selected	Not Selected

VA does not require, at this time, application of control **SC-25: Thin Nodes**. OIT may, at their discretion, elect to employ processing components that have minimal functionality and information storage.

(26) **SC-26: Honeypots (P4)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system includes components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, and analyzing such attacks.	Not Selected	Not Selected	Not Selected
Baseline allocation summary	Not Selected	Not Selected	Not Selected

VA does not require, at this time, application of control **SC-26: Honeypots**. OIT may elect to employ components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, and analyzing such attacks.

(27) **SC-27: Operating System-Independent Applications (P4)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system includes: <u>operating system independent applications</u> .	Not Selected	Not Selected	Not Selected
Baseline allocation summary	Not Selected	Not Selected	Not Selected

VA does not require, at this time, application of control **SC-27: Operating System Independent Applications**. OIT may, at their discretion, elect to employ operating system independent applications.

(28) **SC-28: Protection of Information at Rest (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system protects the confidentiality and integrity of information at rest.	Not Selected	X	X
Baseline allocation summary	Not Selected	SC-28	SC-28

(a) This control is intended to address the confidentiality and integrity of information at rest in non-mobile devices and covers user information and system information. Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive, tape drive) within an organizational information system.

(b) Physical security controls outlined in this handbook must be in place for all non-mobile devices to help protect the confidentiality and integrity of information at rest.

(c) Per OMB Memorandum M-06-16, *Protection of Sensitive Information*, to help protect VA sensitive information VA must log all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required. This involves retrieving data from a database through a query and saving the data into a separate computer-readable entity such as another database, a spreadsheet, or a text file. For additional information, a NIST Frequently Asked Question on this requirement is available on the Information Security Portal under the Policy Section.

(d) Database management systems used in VA will be encrypted using FIPS 140-2 (or its successor) validated encryption.

(29) **SC-29: Heterogeneity (P4)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT employs diverse information technologies in the implementation of the information system.	Not Selected	Not Selected	Not Selected
Baseline allocation summary	Not Selected	Not Selected	Not Selected

VA does not require, at this time, application of control **SC-29: Heterogeneity**. OIT may, at their discretion, elect to employ diverse information technologies.

(30) **SC-30: Virtualization Techniques (P4)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT employs virtualization techniques to present information system components as other types of components, or components with differing configurations.	Not Selected	Not Selected	Not Selected
Baseline allocation summary	Not Selected	Not Selected	Not Selected

VA does not require, at this time, application of control **SC-30: Virtualization Techniques**. OIT may, at their discretion, elect to employ virtualization techniques.

(31) **SC-31: Covert Channel Analysis (P4)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT requires that information system developers/integrators perform a covert channel analysis to identify those aspects of system communication that are potential avenues for covert storage and timing channels.	Not Selected	Not Selected	Not Selected
Baseline allocation summary	Not Selected	Not Selected	Not Selected

VA does not require, at this time, application of control **SC-31: Covert Channel Analysis**. OIT, may, at their discretion, elect to perform covert channel analysis.

(32) **SC-32: Information System Partitioning (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT partitions the information system into components residing in separate physical domains (or environments) as deemed necessary.	Not Selected	X	X
Baseline allocation summary	Not Selected	SC-32	SC-32

Information system partitioning is part of a defense-in-depth protection strategy. An organizational assessment of risk guides the partitioning of information system components into separate physical domains (or environments). The security categorization also guides the selection of appropriate candidates for domain partitioning. Managed interfaces restrict or prohibit network access and information flow among partitioned information system components.

(33) **SC-33: Transmission Preparation Integrity (P4)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system protects the integrity of information during the processes of data aggregation, packaging, and transformation in preparation for transmission.	Not Selected	Not Selected	Not Selected
Baseline allocation summary	Not Selected	Not Selected	Not Selected

VA does not require, at this time, application of control **SC-33: Transmission Preparation Integrity**. OIT may, at their discretion, elect to protect the integrity of information during the processes of data aggregation, packaging, and transformation in preparation for transmission.

(34) **SC-34: Non-Modifiable Executable Programs (P4)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system at <u>information system components</u> : <ul style="list-style-type: none"> • Loads and executes the operating environment from hardware-enforced, read-only media; and • Loads and executes <u>applications</u> from hardware enforced, read-only media. 	Not Selected	Not Selected	Not Selected
Baseline allocation summary	Not Selected	Not Selected	Not Selected

VA does not require, at this time, application of control **SC-34: Non-Modifiable Executable Programs**. OIT may, at their discretion, elect to use non-modifiable executable programs.

i. **System and Information Integrity (SI)**

(1) **SI-1: System and Information Integrity Policy and Procedures**

VA OIT in this Appendix has outlined VA’s system security controls based on the current version of SP 800-53 that are required for the effective implementation of the System and Information Integrity family. Local SOPs should be developed to facilitate the implementation and management of these controls at the local level, as needed. The system and information integrity controls and procedures in this Appendix are consistent with applicable laws: Executive Orders, policies, regulations, standards, and guidance, and will be periodically reviewed, and, when necessary, updated ([See Attachment 2](#)).

(2) **SI-2: Flaw Remediation (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT: <ul style="list-style-type: none"> • Identifies, reports, and corrects information system flaws; • Tests software updates related to flaw remediation for effectiveness and potential side effects on VA information systems before installation; and • Incorporates flaw remediation into VA configuration management process. 	X	X	X
(1) OIT centrally manages the flaw remediation process and installs software updates automatically.	Not Selected	Not Selected	X
(2) OIT employs automated mechanisms to determine the state of information system components with regard to flaw remediation (See Attachment 3).	Not Selected	X	X
Baseline allocation summary	SI-2	SI-2 (2)	SI-2 (1)(2)

(a) OIT identifies information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws) and reports this information to designated officials with information security responsibilities. VA (including any contractor to VA) promptly installs security-relevant software updates (e.g., patches, service packs, and hot fixes). Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling, are also addressed expeditiously. VA will use resources such as the Common Weakness Enumeration or Common Vulnerabilities and Exposures databases in remediating flaws discovered in VA information systems. By requiring that flaw remediation be incorporated into VA configuration management process, it is the intent of this control that required/anticipated remediation actions are tracked and verified. An example of expected flaw remediation that would be so verified is whether the procedures contained in US-CERT guidance and Information Assurance Vulnerability Alerts have been accomplished.

(b) VA has a Patch and Vulnerability Management Program managed by the PVT. The PVT operates under a charter approved by OIT management. The PVT charter describes the functions of the PVT and provides the processes that are consistent with the requirements of this Handbook and recommendations as described in SP 800-40, *Creating a Patch and Vulnerability Management Program*.

(c) OIT component inventories are made available to the PVT. When such inventories are not available, the PVT will develop and maintain appropriate VA system and application inventories for patch and vulnerability management purposes.

(d) OIT management defines the scope of system patching responsibilities for the PVT. The PVT is responsible for standard system configurations that are managed by OIT and are determined to be within the scope of the PVT. For systems that are identified as out of the scope of the PVT, the system owners and managers are responsible for monitoring the systems for vulnerabilities and remediation, testing remediation, and applying remediation in a manner consistent with NIST SP 800-40. OIT will develop a process for adding systems and non-standard system configurations to the scope of the PVT for inclusion in the central patch and vulnerability management program as advised.

(e) VHA implements an approved patch and non-patch remediation solutions for medical devices as possible, based on VA, Food and Drug Administration, and vendor requirements. Medical device managers may use the VA approved isolation architecture to provide compensating controls in lieu of patching, when necessary.

(f) OIT continuously monitors for vulnerabilities and identifies available and required patches for VA systems.

(g) OIT continuously monitors for threat, vulnerability, and remediation related information and disseminates the information internally as needed.

(h) OIT prioritizes patch and remediation applications according to the severity of the threat/vulnerability pair; the likelihood and magnitude of harm; the impact level of the system; any perceived risk involved in the remediation; and the effort level required. VA maintains a database of patches and remediation that have been tested and applied. A "Lessons Learned" journal associated with the implementation of the approved solutions is maintained in conjunction with the remediation database.

(i) OIT centrally tests patches and remediation on non-production systems prior to deployment to ensure that the impact from configuration change and the impact from any change to risk status are fully understood and any loss of security protection is compensated for and minimized. Testing may include but is not limited to: authentication checks (to detect unauthorized changes to software and information), malware detection scans, testing modifications on non-production systems, and checking to see if patches have a sequence dependency.

(j) OIT follows established change control procedures to ensure that appropriate steps have been taken (i.e., registration, analysis, approval, testing, scheduling, implementation, and verification). A change control process is in place to ensure that areas of VA that are affected and need to be part of the process are involved in the process.

(k) OIT ensures all appropriate documentation has been updated to reflect the patch prior to release.

(l) OIT uses a VA approved standard suite of automated patch management tools across the enterprise to expedite the distribution of patches to systems.

(m) OIT deploys patches and remediation promptly and in accordance with PVT developed procedures.

(n) OIT verifies that patches and remediation have been applied. This is accomplished using the VA approved centralized automated tools when possible. Automated patching tools may have this function built in, but when they are not available, verification can be done by a variety of methods, including but not limited to: examination of files and configuration settings, vulnerability scans, examination of logs and audit records, and penetration testing. These processes are also done routinely outside of the verification process. Tight integration of the verification process with these processes and other continuous monitoring processes offer VA gains in both cost effectiveness and security consistency and should be done where practical.

(o) The PVT establishes formal processes to disseminate information regarding existing and emerging threats and vulnerabilities and available patch and non-patch remediation solutions to local administrators and system owners. The system owner or administrator will assess the applicability of the information to their systems or applications.

(p) OIT provides role based training to OIT staff and Administration system owners involved in the patch and remediation effort, and to end users as appropriate.

(q) OIT consistently measures the effectiveness of the Patch and Vulnerability Management Program and applies corrective actions, as necessary.

(r) OIT assesses and mitigates the risks associated with deploying enterprise patch management tools.

(s) OIT uses OIT approved standardized configurations for IT resources, whenever possible.

(3) SI-3: Malicious Code Protection (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT: <ul style="list-style-type: none"> • Employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code. <ul style="list-style-type: none"> i. Transported by e-mail, e-mail attachments, web accesses, removable media, or other common means; or ii. Inserted through the exploitation of information system vulnerabilities. • Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with VA configuration management policy and procedures; and • Configures malicious code protection mechanisms to: <ul style="list-style-type: none"> i. Perform periodic scans of the information system and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with VA security policy (See Attachment 3); and ii. Respond to malicious code detection (See Attachment 3); and • Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. 	X	X	X
(1) OIT centrally manages malicious code protection mechanisms.	Not Selected	X	X
(2) The information system automatically updates malicious code protection mechanisms (including signature definitions)	Not Selected	X	X
(3) The information system prevents non-privileged users from circumventing malicious protection capabilities.	Not Selected	X	X
Baseline allocation summary	SI-3	SI-3 (1)(2)(3)	SI-3 (1)(2)(3)

Information system entry and exit points include, for example, firewalls, e-mail servers, web servers, proxy servers, and remote-access servers. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode) or contained within a compressed file. Removable media includes, for example, USB devices, diskettes, or CDs. A variety of technologies and methods exist to limit or eliminate the effects of malicious code attacks. Pervasive configuration management and strong software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf (COTS) software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect VA missions and business functions. Traditional malicious code protection mechanisms are not built to detect such code. In these situations, VA must rely instead on other risk mitigation measures to include, for example, secure coding practices, trusted procurement processes, configuration management and control, and monitoring practices to help ensure that software does not perform functions other than those intended.

(4) **SI-4: Information System Monitoring (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
<p>OIT:</p> <ul style="list-style-type: none"> Monitors events on the information system in accordance with <u>assigned objectives</u> to detect information system attacks (See Attachment 3); Identifies unauthorized use of the information system; Deploys monitoring devices: (i) strategically within the information system to collect VA-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to VA; Heightens the level of information system monitoring activity whenever there is an indication of increased risk to VA operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; and Obtains legal opinion with regard to information system monitoring activities in accordance with applicable Federal laws, Executive Orders, policies or regulations. 	Not Selected	X	X
(2) OIT employs automated tools to support near real-time analysis of events.	Not Selected	X	X
(4) The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.	Not Selected	X	X
(5) The information system provides near real-time alerts when indications of compromise or potential compromise occur (See Attachment 3).	Not Selected	X	X
(6) The information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities.	Not Selected	X	X
Baseline allocation summary	Not Selected	SI-4 (2)(4)(5)(6)	SI-4 (2)(4)(5) (6)

(a) Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the system (e.g., within internal VA networks and system components). Information system monitoring capability is achieved through a variety of tools and techniques (e.g., IDS, intrusion prevention systems, malicious code protection software, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, at selected perimeter locations and near server farms supporting critical applications, with such devices typically being employed at the managed interfaces associated with controls **SC-7: Boundary Protection** and **AC-17: Remote Access**. The granularity of the information collected is determined by VA based on its monitoring objectives and the capability of the information system to support such activities. An example of a specific type of transaction of interest to VA with regard to monitoring is HTTP traffic that bypasses organizational HTTP proxies, when use of such proxies is required.

(b) Unusual/unauthorized activities or conditions include, for example, internal traffic that indicates the presence of malicious code within an information system or propagating among system components, the unauthorized export of information, or signaling to an external information system. Evidence of malicious code is used to identify potentially compromised information systems or information system components.

(c) Alerts may be generated, depending on the OIT defined list of indicators, from a variety of sources, for example, audit records or input from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers.

(5) **SI-5: Security Alerts, Advisories, and Directives (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT: <ul style="list-style-type: none"> Receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis; Generates internal security alerts, advisories, and directives as deemed necessary; Disseminates security alerts, advisories, and directives to appropriate personnel as designated by the Operating Unit (should be defined by name and/or by role) (See Attachment 3); and Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance. 	X	X	X
(1) OIT employs automated mechanisms to make security alert and advisory information available throughout VA as needed.	Not Selected	Not Selected	X
Baseline allocation summary	SI-5	SI-5	SI-5 (1)

Security alerts and advisories are generated by the US-CERT to maintain situational awareness across the Federal Government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance to security directives is *essential* due to the critical nature of many of these directives and the potential immediate adverse affects on VA operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner.

(6) **SI-6: Security Functionality Verification (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system verifies the correct operation of security functions when anomalies are discovered and institutes appropriate corrections when anomalies are discovered (See Attachment 3).	Not Selected	Not Selected	X
Baseline allocation summary	Not Selected	Not Selected	SI-6

The need to verify security functionality applies to all security functions. For those security functions that are not able to execute automated self-tests, OIT either implements compensating security controls or explicitly accepts the risk of not performing the verification as required. Information system transitional states include, for example, startup, restart, shutdown, and abort.

(7) **SI-7: Software and Information Integrity (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system detects unauthorized changes to software and information.	Not Selected	X	X
(1) OIT reassesses the integrity of software and information by performing integrity scans of the information system (See Attachment 3).	Not Selected	X	X
(2) OIT employs automated tools that provide notification to designated individuals upon discovering discrepancies during integrity verification.	Not Selected	Not Selected	X
Baseline allocation summary	Not Selected	SI-7 (1)	SI-7 (1)(2)

(a) VA sensitive information must be protected from unauthorized changes.

(b) OIT employs integrity verification applications on the information system to look for evidence of information tampering, errors, and omissions. OIT employs good software engineering practices with regard to COTS integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and uses tools to automatically monitor the integrity of the information system and the applications it hosts.

(8) SI-8: Spam Protection (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT: <ul style="list-style-type: none"> Employs spam protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by e-mail, e-mail attachments, web accesses, or other common means; and Updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with VA configuration management policy and procedures. 	Not Selected	X	X
(1) OIT centrally manages spam protection mechanisms.	Not Selected	Not Selected	X
Baseline allocation summary	Not Selected	SI-8	SI-8 (1)

Information system entry and exit points include, for example, firewalls, e-mail servers, web servers, proxy servers, and remote-access servers.

(9) SI-9: Information Input Restrictions (P2)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT restricts the capability to input information to the information system to authorized personnel.	Not Selected	X	X
Baseline allocation summary	Not Selected	SI-9	SI-9

Restrictions on VA personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.

(10) **SI-10: Information Input Validation (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system checks validity of information inputs.	Not Selected	X	X
Baseline allocation summary	Not Selected	SI-10	SI-10

OIT establish rules for checking valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, acceptable values) to ensure that they are in place and to verify that inputs match specified definitions for format and content. Inputs passed to interpreters must be prescreened to prevent the content from being unintentionally interpreted as commands.

(11) **SI-11: Error Handling (P2)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system: <ul style="list-style-type: none"> Identifies potentially security-relevant error conditions; Generates error messages that provide information necessary for corrective actions without revealing VA <u>sensitive information</u> in error logs and administrative messages that could be exploited by adversaries (See Attachment 3); and Reveals error messages only to authorized personnel. 	Not Selected	X	X
Baseline allocation summary	Not Selected	SI-11	SI-11

The structure and content of error messages are carefully considered by OIT. The extent to which the information system is able to identify and handle error conditions is guided by OIT operational procedural requirements.

(12) **SI-12: Information Output Handling and Retention (P2)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
VA handles and retains both information within and output from the information system in accordance with applicable Federal laws, Executive Orders, policies, regulations, standards, and operational requirements.	X	X	X
Baseline allocation summary	SI-12	SI-12	SI-12

The output handling and retention requirements cover the full life cycle of the information, in some cases extending beyond the disposal of the information system. NARA provides guidance on records retention.

(13) **SI-13: Predictable Failure Prevention (P4)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OIT: <ul style="list-style-type: none"> Protects the information system from harm by considering mean time to failure for <u>list of information system components</u> in specific environments of operation; and Provides substitute information system components, when needed, and a mechanism to exchange active and standby roles of the components. 	Not Selected	Not Selected	Not Selected
Baseline allocation summary	Not Selected	Not Selected	Not Selected

VA does not require, at this time, application of control **SI-13: Predictable Failure Prevention**. OIT may, at their discretion, elect to ensure that information systems appropriately support and maintain the binding of security attributes and settings.

3. CONCLUSION

This Appendix has been developed to assist System Owners in selecting security controls to protect VA assets. The security control parameters will be selected by the System Owner based on the system design and the need to meet the security protections based on the level of risk. The selected controls should align with the actual operating environment of the system, will be documented in the SSP, and approved by the VA AO (CIO) or designee. The Attachments provide the following: VA common controls provided in Attachment 1; hybrid controls listed in Attachment 2; and system-specific controls in Attachment 3. Recommended parameters for implementation are provided for each control in the Attachment 2 and 3. The common controls are inherited as enterprise-wide controls and the hybrid controls contain a common control element and an adaptable element(s) while the system-specific controls may be selected based on the system requirements for establishing security parameters that will protect the system. This Appendix is intended to provide a means for Systems Owners to select controls that are necessary for protecting VA assets based on the level of risk and these risk-based decisions will supplant the necessity for waivers. Compensating controls may replace those controls that are not easily implemented and will meet the needs for providing security of the system.



DEPARTMENT OF VETERANS AFFAIRS



VA SYSTEM SECURITY CONTROLS

ATTACHMENT 1 COMMON CONTROLS

Common controls are security controls that are inherited by one or more organizational information systems.

COMMON CONTROLS

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	Value (if required)	Owner
PM-1	H, M, L	<p>Program Management – Information Security Program Plan</p> <p>OIT: a. develops and disseminates a VA-wide information security program plan that: (i) provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; (ii) provides sufficient information about the program management controls and common controls (including specification of parameters for any assignment and selection operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended; (iii) includes roles, responsibilities, management commitment, coordination among organizational entities, and compliance; (iv) is approved by the Assistant Secretary for OIT with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; b. Reviews the organization-wide information security program plan]; and, c. Revises the plan to address organizational changes and problems identified during plan implementation or SCAs.</p>	<p>Every 5 years per VA Directive 6330, <i>Directives Management Procedures</i>, and VA Handbook 6330, <i>Directives Management</i></p> <p>VA Directive and Handbook 6500 as well as other 6500 series handbooks fulfill this control.</p>	<p>DAS for the Office of Information Security (005R2)</p>
PM-2	H, M, L	<p>Program Management – Senior Information Security Officer</p> <p>OIT appoints a CISO with the mission and resources to coordinate, develop, implement, and maintain a VA-wide information security program.</p>	<p>DAS for Information Security</p>	<p>Assistant Secretary for OIT (005)</p>
PM-3	H, M, L	<p>Program Management – Information Security Resources</p> <p>OIT: a. ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement; b. employs a business case/Exhibit 300/exhibit 53 to record the resources required; and c. ensures that information security resources are available for expenditure as planned.</p>		<p>OIT Resource Management (005F)</p>

Control	Baseline High, Moderate , Low	Per NIST SP 800-53	Value (if required)	Owner
PM-4	H, M, L	<p>Program Management – Plan of Action and Milestones Process</p> <p>OIT implements a process for ensuring that POA&Ms for the security program and the associated organizational information systems are maintained and document the remedial information security actions to mitigate risk to VA operations and assets, individuals, other organizations, and the Nation.</p>	VA approved FISMA database	OIT OCS Certification Program Office (005R2)
PM-5	H, M, L	<p>Program Management – Information System Inventory</p> <p>OIT develops and maintains an inventory of its information systems.</p>	OIT Information System Inventory	<p>OIT Service Delivery and Engineering (005OP)</p> <p>OIT OCS Certification Program Office (005R2)</p>
PM-6	H, M, L	<p>Program Management – Information Security Measures of Performance</p> <p>OIT develops, monitors, and reports on the results of information security measures of performance.</p>		OIT Information Security Office (005R)
PM-7	H, M, L	<p>Program Management – Enterprise Architecture</p> <p>OIT develops EA with consideration for information security and the resulting risk to VA operations and assets, individuals, other organizations, and the Nation.</p>		OIT Architecture, Strategy, and Design (005E)
PM-8	H, M, L	<p>Program Management – Critical Infrastructure Plan</p> <p>OIT addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.</p>		<p>OIT Service Delivery and Engineering (005OP)</p> <p>OIT Business Continuity (005R4)</p>

Control	Baseline High, Moderate , Low	Per NIST SP 800-53	Value (if required)	Owner
PM-9	H, M, L	<p>Program Management – Risk Management Strategy</p> <p>OIT: a. Develops a comprehensive strategy to manage risk to VA operations and assets, individuals, other organizations, and the Nation associated with the operation use of information systems; and b. implements that strategy consistently across the VA.</p>		OIT Director Enterprise Risk Management
PM-10	H, M, L	<p>Program Management – Security Authorization Process</p> <p>OIT: a. manages (i.e., documents, tracks, and reports) the security state of organizational information systems through security authorization processes; b. designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and c. fully integrates the security authorization processes into a VA-wide program.</p>		OIT OCS Certification Program Office (005R2)
PM-11	H, M, L	<p>Program Management – Mission/Business Process Definition</p> <p>OIT: a. defines mission/business processes with consideration for information security and the resulting risk to VA operations and assets, individuals, other organizations, and the Nation; and b. determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.</p>		VHA, VBA and NCA with OIT, Service Delivery and Engineering (005OP)



DEPARTMENT OF VETERANS AFFAIRS



VA SYSTEM SECURITY CONTROLS

ATTACHMENT 2 HYBRID CONTROLS

This Attachment provides parameters and values for VA defined hybrid controls – part of the control is considered common (control value is based on VA policy requirements and is applicable for all VA systems) but the implementation of the control remains the responsibility of the field. The values provided will be used, but tailoring is permitted, when approved in the system security plan.

HYBRID CONTROLS

Control	Baseline High, Moderate , Low	Per NIST SP 800-53	Value
AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PS-1, RA-1, SA-1, SC-1, SI-1	H, M, L	<p>Policy and Procedures</p> <p>OIT develops, disseminates, and reviews/updates: a. A formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the control policy and associated controls.</p>	<p>Every 5 years per VA Directive and Handbook 6330</p> <p>VA Handbook 6500 provides VA's overarching policy and procedures that meet NIST's Family-1 controls.</p> <p>The field is responsible for creating a local policy that states they locally implement the policy and procedures outlined in VA Directive and Handbook 6500. The field also develops and maintains additional SOPs as needed.</p>
AC-2	H, M, L	<p>Account Management</p> <p>User Accounts</p> <p>VistA Menu Reviews (Supervisor)</p> <p>Other Account Reviews</p>	<p>At least quarterly or a frequency approved in the SSP</p> <p>At least every 6 months</p> <p>Frequency determined by the System Owner and approved in the SSP</p>
AC-2 (3)	H,M, L	<p>Account Management</p> <p>The information system automatically disables inactive accounts after [time period].</p>	<p>90 days</p> <p>Accounts should be terminated based on the SOPs developed by the Operating Unit.</p>
AC-17 (5)	H, M	<p>Remote Access</p> <p>OIT monitors for unauthorized remote connections to the information system [frequency] and takes appropriate action if an unauthorized connection is discovered</p>	<p>Continuous monitoring.</p>
AC-17 (7)	H, M	<p>OIT ensures that remote sessions for accessing specified security functions and security-relevant information automatically employ additional security measures and are audited.</p>	<p>System security files, system management/configuration files, and creation of system accounts and shared drives or other protected files</p> <p>NSOC specified additional security measures.</p>
AC-17 (8)	H, M	<p>OIT disables non-secure networking protocols except for explicitly identified components in support of specific operational requirements.</p>	<p>Networking protocols identified by NSOC as non-secure.</p>

Control	Baseline High, Moderate , Low	Per NIST SP 800-53	Value
AT-2	H, M, L	<p>Awareness and Training</p> <p>OIT provides basic security awareness training to all users (including managers, senior executives, and contractors) of VA information systems or VA sensitive information as part of initial training for new users, when required by system changes, and [frequency defined] thereafter.</p>	Annually
AT-3	H, M, L	<p>Security Training</p> <p>OIT provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [frequency] thereafter.</p>	Role-based training will be assigned based upon individual needs identified by employee self-assessment and supervisor validation of the self-assessment.
AT-4	H, M, L	<p>Security Training Records</p> <p>OIT retains individual training records for [defined time period].</p>	7 years
AU-11	H, M, L	<p>Audit Record Retention</p> <p>OIT retains audit records for [time period] to provide support for after-the-fact investigations of security incidents and to meet regulatory and VA information retention requirements.</p>	A minimum of three years or as documented in the NARA retention periods, HIPAA legislation (VHA), or whichever is greater. Audit logs which describe a security breach must be maintained for 6 years (HIPAA requirement).
CA-2	H,M,L	<p>Security Assessments</p> <p>OIT assesses the security controls in the information system [frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Assessments may also check non-security functions to ensure that they do not contain security vulnerabilities.</p>	No less than Annually
CA-2 (2)	H	OIT includes as part of SCAs other types of testing.	<p>OIT defined frequency</p> <p>OIT determined announced or unannounced testing</p> <p>OIT defined additional testing, which may include, but is not limited to, in-depth monitoring, malicious user testing, penetration testing, red team exercise, or other forms of security testing which are not included in the basic security assessments defined by OIT.</p>

Control	Baseline High, Moderate , Low	Per NIST SP 800-53	Value
CA-5	H, M, L	<p>Plan of Action and Milestones</p> <p>OIT updates existing POA&Ms [frequency] based on the findings from SCAs, security impact analyses, and continuous monitoring activities.</p>	At least quarterly
CA-6	H, M, L	<p>Security Authorization</p> <p>OIT updates the security authorization [frequency].</p>	Security authorization will be issued initially prior to a system becoming operational, at least every 3 years thereafter, or when significant changes occur to the system after its initial authorization.
CA-7	H, M, L	<p>Continuous Monitoring</p> <p>OIT establishes a continuous monitoring strategy and implements a continuous monitoring program that includes reporting the security state of the information system to appropriate VA officials [frequency].</p>	In accordance with a regular schedule as defined in the Continuous Monitoring Program.
CP-2	H, M, L	<p>Contingency Plan</p> <p>The System Owner reviews the contingency plan for the information system.</p>	Review annually and when one or more significant changes are made.
CP-3	H, M, L	<p>Contingency Training</p> <p>The Operating Unit trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training [frequency].</p>	At least annually
IA-5	H, M, L	<p>Authenticator Management</p> <p>Changing/refreshing authenticators [frequency]</p>	<p>User accounts will be changed every 90 days.</p> <p>Administrator accounts should be changed at a maximum of every 30 days and will be changed at a minimum of every 90 days.</p> <p>Service accounts will be changed at a minimum every 3 years.</p>

Control	Baseline High, Moderate , Low	Per NIST SP 800-53	Value
IA-5 (1)	H, M, L	<p>Authenticator Management</p> <p>The information system, for password-based authentication:</p> <p>Enforces minimum password complexity of [defined] requirements to include case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type.</p> <p>Enforces at least a (defined number of changed characters) when new passwords are created.</p> <p>Enforces password minimum and maximum lifetime restrictions.</p> <p>Prohibits password reuse for (defined number of generations).</p>	<p>User accounts must contain at least 8 non-blank characters. It must contain characters from 3 of the following four categories: English upper case characters, English lower case characters, Base 10 digits, Non-alphanumeric special characters. Six of the characters must not occur more than once in the password.</p> <p>System administrator and service accounts must contain at least 12 non-blank characters and use three of the four categories as outlined above.</p> <p>When changing a password 4 characters must be changed from the old password to the new password.</p> <p>See requirements for frequency for changing/refreshing authenticators.</p> <p>The same password should not be used if it has been used within the past two years; generation usage should prohibit the reuse of a password that has been used within the last 3 times the password has been changed regardless of timeframe.</p>
IA-5 (3)	H, M	OIT requires that the registration process to receive defined types of authenticators to be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).	PIV card
IR-2	H, M, L	<p>Incident Response</p> <p>OIT provides refresher training in incident response roles and responsibilities with respect to the information system.</p>	Annually
IR-3	H, M	<p>Incident Response Testing and Exercises</p> <p>OIT tests and/or exercises the incident response capability for the information system [frequency] using specified tests or exercises to determine the incident response effectiveness and documents the results.</p>	Annually and documents the completion of the testing and the type of testing or exercises conducted in the SSP.

Control	Baseline High, Moderate , Low	Per NIST SP 800-53	Value
IR-6	H, M, L	<p>Incident Reporting</p> <p>OIT requires personnel to report suspected security/privacy incidents to his/her ISO, PO, and supervisor. After normal business hours, notify the VA-NSOC. In this case, as the supervisor, ISO, and PO are not available, personnel may need to contact VA law enforcement, as necessary.</p>	Immediately upon suspicion.
PL-2	H, M, L	<p>System Security Plan</p> <p>The System Owner reviews the security plan for the information system [frequency].</p>	Annually
PS-6	H, M, L	<p>Access Agreements</p> <p>The Operating Unit reviews/updates the access agreements [frequency].</p>	ROB – sign annually Other agreements – annually or as defined in the agreement
RA-3	H, M, L	<p>Risk Assessment</p> <p>The System Owner documents risk assessment results for the system in [type of document].</p> <p>The System Owner reviews risk assessment results [frequency].</p> <p>The System Owner updates the risk assessment [frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.</p>	Document results in the SSP. As necessary to monitor and reduce risks. Annually
SC-5	H, M, L	<p>Systems and Communications Protection</p> <p><u>DoS</u> - OIT ensures that the information system protects against or limits the effects of DoS attacks.</p>	List DoS attack listing and resolution protocol, such as RFC 4732, in the SSP.
SC-7 (4)	H, M	<p>Boundary Protection</p> <p>OIT reviews exceptions to the traffic flow policy [frequency].</p>	As required, per OIT established processes and justified needs.
SC-7 (8)	H	The information system routes defined internal communications traffic to defined external networks through authenticated proxy servers within the managed interfaces of boundary protection devices.	OIT defined internal communication traffic to OIT defined external networks.
SC-17	H, M	<p>Public Key Infrastructure Certificates</p> <p>OIT issues public key certificates under a certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.</p>	VA purchases public key certificates from an approved, shared service provider.



DEPARTMENT OF VETERANS AFFAIRS



VA SYSTEM SECURITY CONTROLS

ATTACHMENT 3 SYSTEM SPECIFIC CONTROLS

This Attachment provides parameters and values for controls, but the controls may be tailored to meet the unique specifications and environment of the system as determined by the System Owner and approved in the system security plan.

SYSTEM SPECIFIC CONTROLS

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OIT Recommended Control Value Minimums	System Specific Control Value - TBD by System Owner for Secure Baseline
AC-2 (2)	H, M	<p>Account Management</p> <p>The System automatically terminates temporary and emergency accounts after use is no longer required.</p>	<p>Three days for Moderate</p> <p>Ten hours for High</p>	[Define time period]
AC-6 (1)	H, M	<p>Least Privilege</p> <p>The System Owner explicitly authorizes access to security functions and security-relevant information.</p>	System security files, system management/configuration files, and creation of system accounts and shared drives or other protected files	[Define security functions and security-relevant information]
AC-6 (2)	H, M	The System Owner requires that users of information system accounts, or roles, with access to security functions and security-relevant information, use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions.	System security files, system management/configuration files, and creation of system accounts and shared drives or other protected files	[Define security functions and security-relevant information]
AC-7	H, M, L	<p>Unsuccessful Login Attempts</p> <p>The System enforces a limit of consecutive invalid login attempts by a user during a specified time period.</p>	<p>Three attempts during a one hour period for Low</p> <p>Three attempts during a one day (24 hour) period for Moderate and High</p>	[Define number]
AC-7	H, M, L	The System automatically takes action when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.	<p>Locks the account</p> <p>One hour for Low</p> <p>Lock out until released by Administrator for Moderate and High</p>	[Define action]
AC-10	H	<p>Concurrent Session Control</p> <p>The System Owner limits the number of concurrent sessions for each system account.</p>	One session for general users and three sessions for users with elevated privileges.	[Define number]

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OIT Recommended Control Value Minimums	System Specific Control Value - TBD by System Owner for Secure Baseline
AC-11	H, M	<p>Session Lock</p> <p>The System Owner prevents further access to the system by initiating a session lock after a period of inactivity or upon receiving a request from a user.</p>	<p>Fifteen minutes</p> <p>(Requests for increased time for specific individuals will be approved by the local ISO and CIO).</p>	<p>[Define time period]</p>
AC-18 (2)	H	<p>Wireless Access</p> <p>OIT monitors for unauthorized wireless connections to the information system, including scanning for unauthorized wireless access points and takes appropriate action if an unauthorized connection is discovered.</p>	<p>Monthly monitoring and scanning activity.</p>	<p>[Define frequency]</p>
AC-19	H, M, L	<p>Access Control for Mobile Devices</p> <p>OIT applies inspection and preventative measures to mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.</p>	<p>Examine mobile devices upon return from travel outside the US for signs of physical tampering and will reimaging the hard disk drive.</p>	<p>[Define inspection and preventative measures]</p>
AC-22	H, M, L	<p>Publicly Accessible Content</p> <p>The Operating Unit assigned individuals reviews the content on the publicly accessible VA information system for non-public information.</p>	<p>Daily</p>	<p>[Define frequency]</p>
AU-2	H, M, L	<p>Auditable Events</p> <p>OIT determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing events as defined by the System Owner.</p>	<p>System Owner defines the auditable events which may include: Actions of system administrators and operators; Production of printed output; new objects and deletion of objects in user address space; security relevant events, system configuration activities and events; events relating to use of privileges, all events relating to user identification and authentication; the setting of user identifiers.</p>	<p>[Define list of auditable events]</p>

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OIT Recommended Control Value Minimums	System Specific Control Value - TBD by System Owner for Secure Baseline
AU-2	H, M, L	The System Owner determines, based on current threat information and ongoing assessment of risk which security events are to be audited within the information system including the frequency for each event.	System Owner defines subset of auditable events to be audited. Quarterly for Low. Monthly for Moderate. Weekly for High. Immediate when threat is identified for Low, Moderate, and High.	[Define subset of auditable events and frequency or situation requiring auditing]
AU-2 (3)	H, M	The System Owner reviews and updates the list of auditable security events.	Annually or following an incident	[Define frequency]
AU-3 (1)	H, M	Content of Audit Records The information system includes detailed information in the audit records for audit events identified by type, location, or subject.	Document and maintain information such as full text recording of privileged commands and individual identities of group account users.	[Define detailed information by type, locations, or subject]
AU-3 (2)	H	OIT centrally manages the content of audit records generated by information system components.	Audit records may be centrally managed for mainframes, workstations, servers, network components, operating systems, middleware, and applications.	[Define components]
AU-5	H, M, L	Response to Audit Processing Failures The information system takes additional actions in the event of an audit processing failure.	Takes additional actions based on a local risk based decision documented in the SSP. Possible actions: <ul style="list-style-type: none"> • Notifies System Administrator by e-mail when approaching capacity. • Overwrites oldest audit records • Stops generating audit records. 	[Define actions to be taken]
AU-5 (1)	H	The information system provides a warning when allocated audit record storage volume reaches a percentage of maximum audit record storage capacity.	75%	[Define percentage]

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OIT Recommended Control Value Minimums	System Specific Control Value - TBD by System Owner for Secure Baseline
AU-5 (2)	H	The information system provides a real-time alert when defined audit failure events occur.	System administrator defined events requiring real-time alerts: Software/hardware errors, failures in the audit capturing mechanisms, and when audit storage capacity being reached or exceeded.	[Define event for alert]
AU-6	H, M, L	Audit Review, Analysis, and Reporting The System Owner reviews and analyzes information system audit records for indications of inappropriate or unusual activity, and reports findings to designated organizational officials.	At least weekly	[Define frequency]
AU-8 (1)	H, M	Time Stamps The System Owner synchronizes internal information system clocks.	At least monthly and on system reset or restart Implement national time standard for location	[Define frequency and time source]
AU-12	H, M, L	Audit Generation The information system provides audit record generation capability for the list of auditable events defined in AU-2 at [defined system components].	System Owner defined components	[Define system components]
AU-12 (1)	H	The information system compiles audit records [from defined information system components] into a system-wide (logical or physical) audit trail that is time correlated to within a defined level of tolerance for relationship between time stamps of individual records in the audit trail.	System Owner defined components System Owner defined tolerance.	[Define system components and level of tolerance for relationship between time stamps and audit trail]
CM-2 (1)	H, M	Baseline Configuration The System Owner reviews and updates the baseline configuration of the information system periodically, upon a system change and as an integral part of information system component installations and upgrades.	Review of security controls baseline conducted on a semi-annual basis A significant change to the system occurs that affects security.	[Define frequency of baseline review and for what circumstances]
CM-2 (4)	M	The System Owner develops and maintains a list of software programs not authorized to execute on the system.	Define in SSP.	[Define not authorized software programs]

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OIT Recommended Control Value Minimums	System Specific Control Value - TBD by System Owner for Secure Baseline
CM-2 (5)	H	The System Owner develops and maintains a list of software programs authorized to execute on the system.	Define in SSP.	[Define list of authorized software programs for system]
CM-3	H, M	<p>Configuration Change Control</p> <p>OIT coordinates and provides oversight for configuration change control activities through configuration change control element (e.g., committee, board) that convenes on assigned schedule.</p>	<p>Local CCB and the National Executive CCB.</p> <p>Meeting frequency or conditions requiring a meeting to be determined by the individual change control elements.</p>	[Define configuration control element and meeting frequency/conditions]
CM-3 (1)	H	The System Owner employs automated mechanisms to highlight approvals that have not been received by assigned time frame.	Organization will prepare time frame according to guidance from CCB.	[Define time frame]
CM-5 (2)	H	<p>Access Restrictions for Change</p> <p>The System Owner conducts audits of information system changes and when indications so warrant to determine whether unauthorized changes have occurred.</p>	Monthly audits of changes	[Define frequency]
CM-5 (3)	H	The System Owner prevents the installation of critical software programs that are not signed with a certificate that is recognized and approved by VA.	Critical software programs will include patches, service packs and device drivers.	[Define critical software programs]
CM-6	H, M, L	<p>Configuration Settings</p> <p>OIT establishes and documents mandatory configuration settings for IT products employed within the information system using security configuration checklists that reflect the most restrictive mode consistent with operational requirements.</p>	OIT prepared and approved configuration settings.	[Define security configuration checklists]
CM-6 (2)	H, M, L	OIT employs automated mechanisms to respond to unauthorized changes to organization-defined configuration settings.	OIT approved automated mechanisms.	[Define mechanism(s) used]
CM-7	H, M, L	<p>Least Functionality</p> <p>System Owner configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of other identified functions, ports, protocols, and/or services.</p>	Restricts the use of functions, ports, protocols, and services to only essential services/ports based on business need and risk. Services/ports are properly secured. Open ports and services must be identified in the SSP with justification. All other ports must be closed.	[Define prohibited or restricted functions, ports, protocols, and/or services]

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OIT Recommended Control Value Minimums	System Specific Control Value - TBD by System Owner for Secure Baseline
CM-7 (1)	H, M	The System Owner reviews the information system to identify and eliminates unnecessary functions, ports, protocols, and/or services.	At a minimum, annually review systems for unauthorized ports/services.	[Define frequency]
CM-7 (2)	H	The System Owner employs automated mechanisms to prevent program execution in accordance with one of the following specifications: list of authorized software programs; list of unauthorized software programs; and rules authorizing the terms and conditions of software program usage.	System Owner selects specification.	[Select from options provided]
CM-8	H, M, L	Information System Component Inventory The System Owner develops, documents, and maintains an inventory of information system components that includes information necessary for effective property accountability.	Required information as outlined by OIT Service Delivery and Engineering	[Define necessary information for property accountability]
CM-8 (3)	H	The System Owner employs automated mechanisms to detect the addition of unauthorized components/devices into the information system and disables network access by such components/devices or notifies designated organizational officials.	Continuous monitoring established on a schedule determined by System Owner and documented in security plan.	[Define frequency]
CM-8 (4)	H	The System Owner includes in property accountability information for information system components, a means for identifying individuals responsible for administering those system components.	Identify system users by name, position, or role.	[Define property accountability responsibilities]
CP-2	H, M, L	Contingency Plan The System Owner distributes copies of the contingency plan.	Key personnel identified in the contingency plan.	[Define list of key contingency personnel for distribution]
CP-2	H, M, L	The System Owner communicates contingency plan changes.	Key personnel identified in the contingency plan.	[Define list of key contingency personnel for change control communications]

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OIT Recommended Control Value Minimums	System Specific Control Value - TBD by System Owner for Secure Baseline
CP-2 (3)	H	The System Owner plans for the resumption of essential missions and business functions after contingency plan activation.	Identify time period that the System Owner determines when essential operations will resume once the contingency plan has been activated.	[Define time period]
CP-4	H, M, L	<p>Contingency Plan Testing and Exercises</p> <p>The System Owner tests and/or exercises the contingency plan for the information system using OIT defined tests and/or exercises to determine the plan's effectiveness and the organization's readiness to execute the plan.</p>	<p>Annually test contingency plan.</p> <p>Tests will have a specific objective such as: determining the availability of needed back-up files; validity/functionality of the back-up files; and implementation of fire and evacuation procedures and implementation of manual procedures.</p>	[Define frequency and type of test]
CP-7	H, M	<p>Alternate Processing Site</p> <p>OIT establishes an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions when the primary processing capabilities are unavailable.</p>	This trigger point (downtime before contingency plan is activated) set by criticality to VA mission and business need and identified within the contingency plan and tested for in the SCA.	[Define time period according to recovery time objectives]
CP-8	H, M	<p>Telecommunications Services</p> <p>OIT establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions when the primary telecommunications capabilities are unavailable.</p>	This trigger point (downtime before contingency plan is activated) set by criticality to VA mission and business need and identified within the contingency plan and tested for in the SCA.	[Define time period]
CP-9	H, M, L	<p>Information System Backup</p> <p>The System Owner conducts backups of user-level information contained in the information system consistent with recovery time and recovery point objectives.</p>	<p>Weekly for Low</p> <p>Daily or Real-time with Real-time Mirroring/Shadowing for Moderate and High</p>	[Define frequency according to recovery time and point objective]
CP-9	H, M, L	The System Owner conducts backups of system-level information contained in the information system consistent with recovery time and recovery point objectives.	<p>Weekly for Low</p> <p>Daily or Real-time with Real-time Mirroring/Shadowing for Moderate and High</p>	[Define frequency according to recovery time and point objective]

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OIT Recommended Control Value Minimums	System Specific Control Value - TBD by System Owner for Secure Baseline
CP-9	H, M, L	The System Owner conducts backups of information system documentation including security-related documentation consistent with recovery time and recovery point objectives.	System backups are conducted on a semi-annual basis for Low System backups are scheduled on a monthly basis for Moderate and High	[Define frequency according to recovery time and point objective]
CP-9 (1)	H, M	The System Owner tests backup information to verify media reliability and information integrity.	At least weekly (or daily with some real-time self-assurance mechanism in place)	[Define frequency]
CP-10 (3)	H, M	Information System Recovery and Reconstitution The System Owner provides compensating security controls for circumstances that inhibit recovery and reconstitution to a known state.	Identify circumstances that can inhibit recovery and reconstitution to a known state.	[Define circumstances that inhibit recovery and reconstitution]
CP-10 (4)	H	The System Owner provides the capability to reimage information system components from configuration-controlled and integrity-protected disk images representing a secure, operational state for the components.	Within recovery-restoration time periods.	[Define restoration time period(s)]
IA-2 (8)	H, M	Identification And Authentication (Organizational Users) The System Owner uses replay-resistant authentication mechanisms for network access to privileged accounts.	Replay resistant authentication mechanisms installed according to security plan	[Define replay resistant authentication mechanisms]
IA-2 (9)	H	The System Owner uses replay-resistant authentication mechanisms for network access to non-privileged accounts.	Replay resistant authentication mechanisms installed according to security plan	[Define replay resistant authentication mechanisms]
IA-3	H, M	Device Identification and Authentication The information system uniquely identifies and authenticates a list of specific and/or types of devices before establishing a connection.	Devices on a LAN or WAN attempting to establish a connection.	[Define list of specific and type of device(s)]
IA-4	H, M, L	Identifier Management The System Owner manages information system identifiers for users and devices by preventing reuse of user or device identifiers.	At least 2 years	[Define time period]
IA-4	H, M, L	The System Owner manages information system identifiers for users and devices by disabling the user identifier after a time period of inactivity.	Ninety days	[Define time period of inactivity]

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OIT Recommended Control Value Minimums	System Specific Control Value - TBD by System Owner for Secure Baseline
IR-8	H, M, L	<p>Incident Response Plan</p> <p>The Operating Unit distributes copies of the incident response plan to a list of incident response personnel (identified by name and/or by role) and organizational elements.</p>	<p>Key personnel identified in the incident response plan and reviewed/updated annually or when change in personnel occurs.</p>	<p>[Define list of IR personnel by name/role for copies]</p>
IR-8	H, M, L	<p>The Operating Unit reviews the incident response plan.</p>	<p>Annually</p>	<p>[Define frequency]</p>
IR-8	H, M, L	<p>The Operating Unit communicates incident response plan changes to a defined list of incident response personnel (identified by name and/or by role) and organizational elements.</p>	<p>Prepare and distribute incident response plan to key personnel and provide updates when incurred.</p>	<p>[Define list of IR personnel by name/role for copies]</p>
MA-6	H, M	<p>Timely Maintenance</p> <p>The System Owner obtains maintenance support and/or spare parts for security-critical information system components and/or key IT components within a time frame suitable to avoid failure.</p>	<p>Components are selected in accordance with criticality, business need, and risk. Semi-annual review of components. Document changes and replacements and update SSP when required by criticality, business need, and risk following a failure per contract vehicle, maintenance contract, or warranty terms and conditions.</p> <p>System Owner defines time period for delivery of support or parts.</p>	<p>[Define list of security-critical system components and time period]</p>
MP-2	H, M, L	<p>Media Access</p> <p>The System Owner restricts media access to a defined list of authorized individuals using defined security measures.</p>	<p>Information systems media both paper and electronic.</p> <p>Establish access list for Low, Moderate, and High.</p> <p>Measures taken to restrict access are defined in the SSP.</p>	<p>[Define types of media, list authorized individuals, and define security measure]</p>

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OIT Recommended Control Value Minimums	System Specific Control Value - TBD by System Owner for Secure Baseline
MP-3	H, M	<p>Media Marking</p> <p>The System Owner may exempt removable media types from marking as long as the exempted items remain within the designated controlled areas.</p>	<p>Removable media documented in SSP, such as Disk Packs and backup tapes</p> <p>Secured computer room is the designated controlled area.</p>	<p>[Define list of exempted media types and the designated controlled area(s)]</p>
MP-4	H, M	<p>Media Storage</p> <p>The System Owner physically controls and securely stores types of digital and non-digital media within controlled areas according to defined security measures.</p>	<p>Information systems media, both paper and electronic ;</p> <p>Controlled area defined by the System Owner</p> <p>Measures taken to physically control and security store the media are documented in the SSP.</p>	<p>[Define media, controlled areas, and security measures]</p>
MP-5	H, M	<p>Media Transport</p> <p>The Operating Unit protects and controls types of digital and non-digital media during transport outside of controlled areas using security measures.</p>	<p>Information systems media, both paper and electronic;</p> <p>Double-wrap and secure physical container when appropriate to prevent loss or compromise</p>	<p>[Define type of media and security measures for transport]</p>
MP-6 (2)	H	<p>Media Sanitization</p> <p>OIT tests sanitization equipment and procedures to verify correct performance.</p>	<p>Annually</p>	<p>[Define frequency]</p>
MP-6 (3)	H	<p>OIT sanitizes portable, removable storage devices prior to connecting such devices to the information system in defined circumstances.</p>	<p>Sanitization occurs upon purchase or prior to initial use.</p> <p>Mobile devices may require sanitization prior to use outside of US or upon return from travel outside of the US.</p> <p>Sanitization requirements are based upon VA Handbook 6500.1.</p>	<p>[Define circumstances requiring sanitization]</p>

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OIT Recommended Control Value Minimums	System Specific Control Value - TBD by System Owner for Secure Baseline
PE-2	H, M, L	Physical Access Authorizations The System Owner (or designee) reviews and approves the access list and authorization credentials removing from the access list personnel no longer requiring access.	Bi-annually for Low Quarterly for Moderate and High	[Define frequency]
PE-3	H, M, L	Physical Access Control The Operating Unit inventories physical access devices.	Semi-annually for Low and Moderate Quarterly for High	[Define frequency]
PE-3	H, M, L	The Operating Unit changes combinations and keys as specified in the security plan and when keys are lost, combinations are compromised, or individuals are transferred or terminated.	Define frequency within security plan.	[Define frequency]
PE-6	H, M, L	Monitoring Physical Access The Operating Unit reviews physical access logs.	Quarterly for Low Monthly for Moderate and High	[Define frequency]
PE-8	H, M, L	Access Records The System Owner (or designee) reviews visitor access records.	Quarterly for Low Weekly for Moderate Daily for High	[Define frequency]
PE-10	H, M	Emergency Shutoff The Operating Unit places emergency shutoff switches or devices in location by information system or system component to facilitate safe and easy access for personnel;	Switches are installed and location documented in the SSP for the shutoff switch/device by system or component	[Define location by system component]
PE-14	H, M, L	Temperature and Humidity Controls The Operating Unit maintains temperature and humidity levels within the facility where the information system resides.	Document acceptable levels in SSP in compliance with recommended manufacturer requirements.	[Define acceptable levels]
PE-14	H, M, L	The Operating Unit monitors temperature and humidity levels	Consistently monitor according to recommended manufacturer requirements.	[Define frequency]

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OIT Recommended Control Value Minimums	System Specific Control Value - TBD by System Owner for Secure Baseline
PE-16	H, M, L	<p>Delivery and Removal</p> <p>The Operating Unit authorizes, monitors, and controls types of information system components entering and exiting the facility and maintains records of those items.</p>	Information system-related items (i.e., hardware, firmware, software)	[Define types of components]
PE-17	H, M	<p>Alternate Work Site</p> <p>The Operating Unit employs management, operational, and technical information system security controls at alternate work sites.</p>	Controls established per VA Handbook 6500	[Identify any unique specific controls required]
PS-5	H, M, L	<p>Personnel Transfer</p> <p>The Operating Unit reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within VA and initiate transfer or reassignment actions promptly.</p>	<p>Appropriate transfer/reassignment actions to be initiated include: reissuing keys, identification cards, and building passes; closing old accounts and establishing new accounts; and changing system access authorizations.</p> <p>Changes should occur as soon as possible but no later than 30 days of the transfer action.</p>	[Define action and time period]
RA-5	H, M, L	<p>Vulnerability Scanning</p> <p>OIT scans for vulnerabilities in the information system and hosted applications periodically and when new vulnerabilities potentially affecting the system/applications are identified and reported.</p>	Monthly	[Define frequency and process]
RA-5	H, M, L	The System Owner remediates legitimate vulnerabilities in accordance with an OIT assessment of risk.	Applying patches as they are released and mandated.	[Define response times]
RA-5 (2)	H	The System Owner updates the list of information system vulnerabilities scanned periodically or when new vulnerabilities are identified and reported.	Monthly	[Define frequency]
RA-5 (5)	H	The System Owner includes privileged access authorization for selected vulnerability scanning activities to facilitate more thorough scanning.	Customized applications and peripherals	[Define system components]
RA-5 (7)	H	The System Owner employs automated mechanisms to detect the presence of unauthorized software on VA information systems and notify designated VA officials.	Test monthly	[Define frequency]

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OIT Recommended Control Value Minimums	System Specific Control Value - TBD by System Owner for Secure Baseline
SA-12	H	<p>Supply Chain Protection</p> <p>The Operating Unit protects against supply chain threats by employing a list of measures to protect against supply chain threats as part of a comprehensive, defense-in-breadth information security strategy.</p>	<p>An initial plan for security measures is adapted for: One or more of the following:</p> <ul style="list-style-type: none"> • Purchasing spares in the initial acquisition • Conducting due diligence review of suppliers prior to acquisitions • Using trusted shipping and warehousing • Employing a diverse set of suppliers • Employing standard configurations • Minimizing time between purchase decision and delivery • Employing independent analysis and penetration testing, 	<p>[Define list of measures to protect supply chain]</p>
SA-13	H	<p>Trustworthiness</p> <p>The System Owner requires that the information system meets necessary level of trustworthiness.</p>	<p>System Owner defines according to risk-based criteria.</p>	<p>[Define level of trustworthiness]</p>
SC-9 (1)	H, M	<p>Transmission Confidentiality</p> <p>The System Owner employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures.</p>	<p>Alternative physical measures will be determined by the System Owner and may include protected distribution systems.</p>	<p>[Define alternative physical measures]</p>
SC-10	H, M	<p>Network Disconnect</p> <p>The information system terminates the network connection associated with a communication session at the end of the session or after inactivity.</p>	<p>The time period of inactivity will be determined by the System Owner. It may be a set of time periods by type of network access or for specific accesses.</p>	<p>[Define time period of inactivity]</p>

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OIT Recommended Control Value Minimums	System Specific Control Value - TBD by System Owner for Secure Baseline
SC-15	H, M, L	<p>Collaborative Computing Devices</p> <p>The System Owner prohibits remote activation of collaborative computing devices unless an exception is defined where remote activation is to be allowed.</p>	Circumstances documented in the SSP.	[Define exceptions for remove activation]
SC-24	H	<p>Fail in Known State</p> <p>The information system will fail to a known-state for defined types of failures preserving system state information in failure.</p>	System Owners will determine types of failures and system state.	[Define types of failures and system state]
SI-2 (2)	H, M	<p>Flaw Remediation</p> <p>The System Owner employs automated mechanisms to determine the state of information system components with regard to flaw remediation.</p>	Testing of information systems is conducted as required by VA's PVT requirements.	[Define frequency]
SI-3	H, M, L	<p>Malicious Code Protection</p> <p>OIT configures malicious code protection mechanisms to perform periodic scans of the information system and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with OIT approved processes and to respond to malicious code detection.</p>	<p>Per VA-NSOC and OIT Operations approved processes.</p> <p>Report to the VA-NSOC.</p>	[Define frequency and response to malicious code detection]
SI-4	H, M	<p>Information System Monitoring</p> <p>OIT monitors events on the information system in accordance with monitoring objectives and detects information system attacks.</p>	Ensure proper system functioning, confirm system functioning, and detect indicators of system malfunction or compromise	[Define monitoring objectives]
SI-4 (5)	H, M	The information system provides near real-time alerts when indications of compromise or potential compromise occur.	Examples are audit records or input from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers.	[Define list of compromise indicators]
SI-5	H, M, L	<p>Security Alerts, Advisories, and Directives</p> <p>OIT disseminates security alerts, advisories, and directives to authorized personnel.</p>	ISOs, IT Staff, Service Line Managers, local CIOs and Chief Technology Officers. Other personnel may be added at local level through locally defined distribution lists.	[Define list of personnel, identified by name/and or by role]

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OIT Recommended Control Value Minimums	System Specific Control Value - TBD by System Owner for Secure Baseline
SI-6	H	<p>Security Functionality Verification</p> <p>The System Owner verifies the correct operation of security functions and takes action when anomalies are discovered.</p>	<p>Verification is continuous monitoring and occurs upon system startup and restart; upon command by user with appropriate privilege; or at least quarterly. Any discrepancy is immediately reported to system administrator</p>	<p>[Define state(s), privilege, time period, and condition]</p>
SI-7 (1)	H, M	<p>Software and Information Integrity</p> <p>The System Owner reassesses the integrity of software and information by performing integrity scans of the information system.</p>	<p>Quarterly</p>	<p>[Define frequency]</p>
SI-11	H, M	<p>Error Handling</p> <p>The information system generates error messages that provide information necessary for corrective actions without revealing sensitive or potentially harmful information in error logs and administrative messages that could be exploited by adversaries.</p>	<p>Error messages will not reveal VA sensitive information.</p>	<p>[Define type of sensitive or harmful information]</p>