DEPARTMENT OF VETERANS AFFAIRS
Washington, DC 20420

VA HANDBOOK 6500
Transmittal Sheet
March 10, 2015

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

1. REASON FOR ISSUE: This Handbook provides the risk-based process for selecting system security controls, including the operational requirements for Department of Veterans Affairs (VA) information technology systems per VA Directive 6500, *Managing Information Security Risk: VA Information Security Program.* This policy is consistent with VA's information security statutes; 38 United States Code (U.S.C.) §§ 5721-5728, *Veterans' Benefits, Information Security*; 44 U.S.C. §§ 3541-3549, *Federal Information Security Management Act of 2002*; 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, an updated VA National Rules of Behavior, and an appendix addressing VA privacy controls. The Handbook is based on National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

3. RESPONSIBLE OFFICE: The Office of the Assistant Secretary for Information and Technology (005), Information Security (005R), Cyber Security (005R2), is responsible for the security content, and the VA Privacy Office (005R1) is responsible for the privacy content outlined in Appendix E of this Handbook.

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

5. RESCISSIONS: VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program*, dated September 20, 2012, and its appendices. Note: This rescission does not include the other handbooks in the VA 6500 series.

CERTIFIED BY:

/s/
Stephen W. Warren
Executive in Charge and Chief Information Officer for Information and Technology

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/
Stephen W. Warren
Executive in Charge and Chief Information Officer for Information and Technology

Distribution: Electronic Only

This page is intentionally blank for the purpose of printing front and back copies.

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

CONTENTS

PARAGRAPH **PAGE**

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

CONTENTS, cont.

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 and privacy 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*; NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*; and NIST SP 800-53, *Security and Privacy 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 includes VA's privacy controls, which are based on the privacy controls outlined in NIST SP 800-53. These are intended to address the privacy needs across all of VA.

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

e. 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 identified in Appendix C.

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 information. Contractors are required to sign VA's Contractor ROB, which describes the responsibilities and expected

behavior of contractors who use VA systems or VA 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. Appendix E contains a table of NIST's security control families that are used to secure VA's information and information systems.

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

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

3. BACKGROUND/OVERVIEW

a. 44 United States Code (U.S.C.) §§ 3541-3549, *Federal Information Security Management Act (*FISMA*) of 2002* promotes 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, as outlined in FIPS 199; and

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

b. The RMF outlined in NIST 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 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. Sections 6-11 of this Handbook provide additional information on each of the six risk framework steps listed above.

FIGURE 1: RISK MANAGEMENT FRAMEWORK

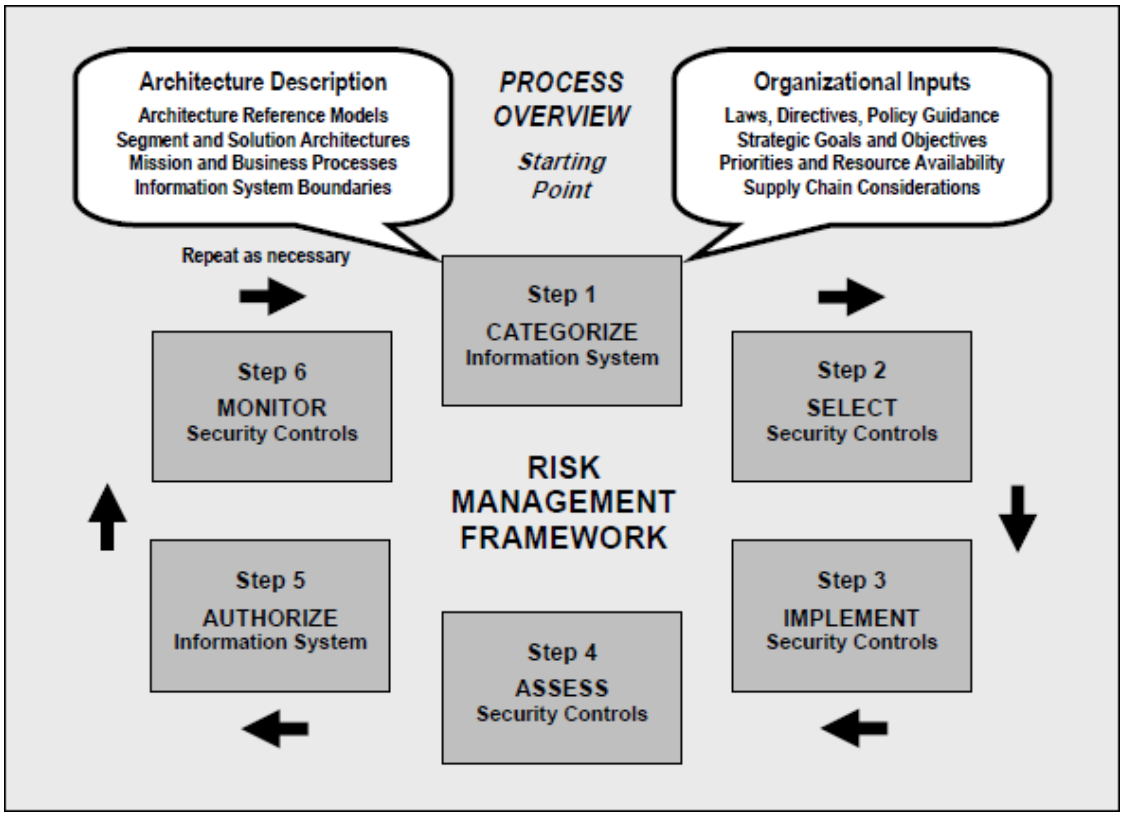


Figure 1, above, illustrates the six steps required within the RMF, which includes:

(1) Step 1: Categorize the information system

(2) Step 2: Select the security controls

(3) Step 3: Implement the security controls

(4) Step 4: Assess the security controls

(5) Step 5: Authorize the information system

(6) 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**, as the VA Chief Information Officer (CIO), is responsible for:

(a) Assuming the responsibility as the Authorizing Official (AO) to ensure that systems under OI&T'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 personnel are adequately trained;

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

(f) Coordinating with other senior officials, report 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** is responsible for:

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

1. Processing background investigations as required for VA employees, contractors, and affiliates. The background investigations are conducted at a level commensurable 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 – is responsible for:

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

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

3. Collaborating with OIS and program directors to investigate potential violations of privacy and security laws and VA policies, and enforce penalties against violators.

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

(a) Providing guidance based on VA's Human Resources 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 authorized to access information systems.

(4) **Deputy Assistant Secretary for Acquisition and Logistics** is responsible for:

(a) Providing acquisition policy/procedures to VA Contracting Officers (CO), Program Managers and Contracting Officer 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 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 security language 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) **Deputy Assistant Secretary for IT Resource Management** is responsible for:

(a) Aggregating all capital planning and investment requests for the Deputy Assistant Secretary (DAS) for Information Security needed to implement the information security program and documenting 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 Chief Information Officer for Architecture, Strategy, and Design** is responsible for ensuring 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 resulting information systems supporting those missions and business processes.

(7) **Deputy Chief Information Officer for Product Development** is responsible for:

(a) Conducting information system security engineering activities; and

(b) Employing Federal requirements, VA policy, and industry best practices when implementing security controls within an information system, software engineering methodologies, system/security engineering principles, secure design, secure architecture, and secure coding techniques**.**

(8) **Deputy Chief Information Officer 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 each system is assigned an Information System Owner and that the Information System Owner is responsible for the security of the system;

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

(d) Providing appropriate access to VA systems (including types of privileges or access), in coordination with VA managers and ISOs ;

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

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

(g) Ensuring the development and maintenance of SSPs and contingency plans are 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 OCS 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 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, regularly reviewed/updated, and when there is a major change to the system, reviewed and updated as required;

(n) Ensuring the information system receives authorization prior to operational deployment, is reauthorized when a significant change in the system or a major change in the data occurs, and is continuously monitored;

(o) Assisting other VA officials with significant information security responsibilities in remediating the weaknesses or deficiencies identified in the plan of action and milestones (POA&M) and updating the POA&M, conducting periodic compliance validation reviews, and completing 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 Security Operations Center (VA-NSOC) and the OIG as appropriate per VA Handbook 6500.2, *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;

(t) Chartering, organizing, and maintaining VA's Patch and Vulnerability Team (PVT) Program;

(u) Collaborating with VA Identity Safety Service to monitor for identity theft when appropriate;

(v) Nominating a COR for all contracts impacted by this directive and ensuring CORs complete the required COR training;

(w) Ensuring security requirements and security specifications are explicitly included in VA contracts, as appropriate;

(x) Working with the ISO and PO to ensure contracts contain the required security language necessary for compliance with FISMA and 38 U.S.C. 5721-5728 and to provide adequate security for information and information systems used by the contractor, including the requirement for signing the VA Contractor ROB;

(y) Ensuring contractors meet the appropriate background investigation requirements in accordance with VA Directive and Handbook 0710;

(z) Ensuring contractors complete VA's security and privacy awareness training and any additional role-based training, as outlined in the contract;

(aa) Monitoring the contract to ensure that security requirements are met, consulting the ISO and PO as necessary; and

(9) **Deputy Assistant Secretary 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 (whose role includes AO) to the Information System Owners and ISOs;

(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) Establishing the VA National and Contractor ROB for appropriate use and protection of VA information systems and VA information that are used to support Department missions and functions;

(g) Providing ISO support to the Department through Field Security Service (FSS);

(h) Managing and ensuring the ISOs of the Department comply with VA cyber security directives and handbooks (Note: 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, 38 U.S.C. § 5705, Confidentiality of Medical Quality-Assurance Records, and 38 U.S.C. § 7332, Confidentiality of Certain Medical Records;

(j) Providing guidance and procedures for protecting information as required by 38 U.S.C. §§ 5721-5728 , *Veterans' Benefits, Information Security*;

(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. Law 104-191, 110 Stat. 1936; the Health Information Technology for Economic and Clinical Health (HITECH) Act, Pub. Law 111-5, Title XIII, 123 Stat. 226, and their implementing regulations at 45 Code of Federal Regulations (C.F.R.) Part 160, *General Administrative Requirements* and 45 C.F.R. Part 164, *Privacy and Security Rules* and NIST SP 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*;

(l) Establishing VA requirements and providing guidance regarding the development, completion, and updating of PIA;

(m) Ensuring Privacy Awareness Training is provided and available for VA employees, contractors, volunteers, and interns;

(n) Ensuring VA privacy and information system security policies complement and support each other;

(o) Directing 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 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;

(s) Coordinating with Federal oversight agencies and VA management regarding privacy violations and their resolution, as required;

(t) Submitting to the Secretary, at least once every quarter, a report on deficiencies of the Department, and any Administration, office, and facility of the Department, in compliance with 44 U.S.C. §§ 3541-3549;

(u) Reporting immediately to the Secretary on any significant deficiency in accordance with paragraph (t) above;

(v) Evaluating, monitoring, and coordinating data breach quarterly reports. These data breach reports are provided to Congress by the Secretary of VA;

(w) Providing central coordination and incident response functions for all security and privacy events impacting and affecting VA;

(x) Coordinating incident response with outside agencies such as the United States Computer Emergency Readiness Team (US-CERT);

(y) Establishing and maintaining a formal incident response capability;

(z) Establishing and providing supervision over an effective incident reporting system;

(aa) Ensuring remediation instructions and remediation timelines are provided to Information System Owners when systems require remediation due to an incident;

(bb) Establishing standard remediation timelines for different remediation actions;

(cc) Establishing performance metrics to measure the effectiveness of incident response activities;

(dd) Approving and managing all VA information and information systems incident response efforts based on VA-NSOC SOPs, as directed by the guidance of VA OI&T and the US-CERT;

(ee) Actively monitoring all VA network intrusion detection sensors, firewall alerts, network operations, security logs for abnormal activity, attempted intrusions/ compromises, and other manners of security alerts that may be generated; follow up as appropriate to minimize the impact of security incidents on VA information systems;

(ff) Identifying, validating, and managing all information and information system incidents including(security and privacy) reporting and response efforts;

(gg) Providing immediate notice to the VA Secretary of any presumptive data breach;

(hh) Reporting all privacy-related incidents to the US-CERT within one hour of discovery of event;

(ii) 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;

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

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

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

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

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

(oo) 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;

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

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

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

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

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

(uu) Executing initial and periodic information identity risk assessments and conducting related ongoing compliance monitoring activities in coordination with other compliance and operational assessment functions;

(vv) 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;

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

(xx) 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;

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

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

(aaa) Overseeing the process of defining business continuity problems and implementing solutions;

(bbb) Developing and providing identity theft training or incorporating it into the privacy and security training;

(ccc) Developing outreach and communication activities to assist in the prevention of identity theft;

(ddd) Collaborating with stakeholders to monitor for identity theft and to establish best practices and standards;

(eee) Conducting identity theft analysis to review for identity theft; and

(fff) Enforcing penalties, conducting investigations, and assisting victims in remedies.

(10) **Executive Director for Quality, Performance and Oversight** in OI&T 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 weaknesses described in POA&Ms and identified in the VA-approved FISMA database;

(c) Conducting an on-site assessment of the security controls employed or inherited by an information system to determine the overall effectiveness of the controls (i.e., to determine if the documented controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements identified for protecting the system at its specified level of sensitivity);

(d) Ensuring VA systems that have undergone an assessment and authorization (A&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) **Executive Director of Enterprise Communications** in OI&T is responsible for all voice, data, and video systems, as well as network transport. The Office of Enterprise Communications is responsible for:

(a) Monitoring and managing the network down to the VA facility; and

(b) Managing the budget, capacity planning, and design (in conjunction with Enterprise Systems Engineering) of all communications systems and infrastructure enterprise-wide.

(12) **Information Owners/Stewards (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;

(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; and

(d) Collaborating with VA Identity Safety Service to increase awareness of potential identity theft and fraud and to prevent potential identity theft and fraud.

(13) **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 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 commensurable 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 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; implement the provisions of a bulletin or alert of the VA-NSOC; and ensuring 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; 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 are assigned;

(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, and ensuring employees complete role-based training as required by their specific duties/responsibilities.

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

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

(b) Ensuring a VA ISO and a VHA Health Care Security Requirements Security Analyst (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 OI&T and OMB; and

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

(15) **Information Security Officers** are agency officials who OI&T Field Security Service has assigned responsibility to ensure the appropriate operational security posture is maintained for an information system or program. VA ISOs are responsible for:

(a) Providing official guidance on information security matters to local management and staff;

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

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

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

(e) Assisting in the determination of the appropriate security categorization of the IT system commensurate with the FIPS 200 impact level;

(f) 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;

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

(h) Working with the Information 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 (Note: controls most apt to change over time must be included and these tests and results must be documented to support the continuous monitoring program);

(i) 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;

(j) Assisting other VA officials with significant information security responsibilities in remediating the weaknesses or deficiencies identified in the POA&M, updating the POA&M, conducting periodic compliance validation reviews, and completing the FISMA annual assessment to reduce or eliminate system vulnerabilities;

(k) Notifying the VA-NSOC of any confirmed or suspected incident within one hour of discovery of the potential incident and assisting in the investigation, if necessary;

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

(m) Monitoring compliance with the security awareness training requirements for each employee and contractor;

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

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

(p) 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;

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

(r) Coordinating with OI&T staff to add, change, suspend, and 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;

(s) Participating in the Institutional Review Board (IRB) protocol review and approval process, evaluating the study's data usage, and making recommendations to ensure implementation of reasonable safeguards for the data;

(t) Ensuring VHA facilities implement reasonable and appropriate safeguards to secure electronic protected health information as required by the HIPAA Security Rule;

(u) Ensuring compliance with identity theft prevention and mitigation based practices; and

(v) Collaborating with VA Identity Safety Service to provide training on identity theft; fraud prevention and mitigation; and to assist in the prevention and mitigation of potential identity theft and fraud.

(16) **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 supervisors are responsible for:

(a) Ensuring ISOs are consulted on information security matters;

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

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

(d) Determining the Federal employee's or contractor's "need-to-know" before access is granted;

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

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

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

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

(i) 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;

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

(k) 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;

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

(m) Assisting other VA officials with significant information security responsibilities in remediating the weaknesses or deficiencies identified in the POA&M; updating the POA&M, conducting periodic compliance validation reviews, and completing the FISMA annual assessment to reduce or eliminate system vulnerabilities;

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

(o) Serving as the liaison to the OIG and other auditors within their area of responsibility;

(p) Nominating a COR for all contracts impacted by this directive and ensuring CORs complete the required COR training.

(q) Ensuring security requirements and security specifications are explicitly included in VA contracts, as appropriate;

(r) Working with the ISO and PO to ensure that contracts contain the required security language necessary for compliance with FISMA, and 38 USC §§ 5721-5728, and to provide adequate security for information and information systems used by the contractor; including the requirement for signing VA Contractor ROB, when applicable'

(s) Ensuring contractors meet the appropriate background investigation requirements in accordance with VA Directive and Handbook 0710;

(t) Ensuring contractors complete VA's security and privacy awareness training and any additional role-based training, as outlined in the contract

(u) Monitoring the contract to ensure that security requirements are being met, consulting the ISO and PO as necessary; and

(v) Assisting other VA officials with significant information security responsibilities in remediating the weaknesses or deficiencies identified in the POA&M and updating the POA&M, conducting periodic compliance validation reviews, and completing the FISMA annual assessment to reduce or eliminate system vulnerabilities.

(17) **Information System Owners, Local CIOs, or Designees / 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. These roles are responsible for:

(a) Ensuring ISOs are consulted on information security matters;

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

(c) Assisting Information System Owners in the development and maintenance of SSPs and contingency plans for all systems within their area of responsibility;

(d) Participating in risk assessments as outlined in the SSP;

(e) Participating in self-assessments, external and internal audits of system safeguards and program elements, including A&A of the system;

(f) Evaluating proposed technical security controls to assure proper integration with other system operations;

(g) Identifying requirements for resources needed to effectively implement technical security controls;

(h) Ensuring the integrity in implementation and operational effectiveness of technical security controls by conducting technical control testing;

(i) Developing system administration, operational procedures, and manuals as directed by the Information System Owner;

(j) Evaluating and developing procedures that assure proper integration of service continuity with other system operations;

(k) Notifying the responsible ISO and PO of any suspected incidents within one hour upon discovery and assisting in the investigation of incidents if necessary;

(l) Reading and understanding all applicable training and awareness materials;

(m) Providing information on users and/or the system in support of any reports or documents necessary for oversight and authorization;

(n) 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;

(o) 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;

(p) Serving as owner for all local systems (e.g., tenant systems, guest networks) for which he/she is assigned, establishing standards (based on Federal requirements and VA security policies) for operating the systems within a VA facility, and removing non-compliant systems from use at the VA facility;

(q) 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;

(r) Assisting other VA officials with significant information security responsibilities in remediating the weaknesses or deficiencies identified in the POA&M; updating the POA&M, conducting periodic compliance validation reviews, and completing the FISMA annual assessment to reduce or eliminate system vulnerabilities;

(s) Ensuring compliance with identity theft prevention and mitigation based practices; and

(t) Collaborating with VA Identity Safety Service to provide training on identity theft and fraud prevention and mitigation and to assist in the prevention and mitigation of potential identity theft and fraud.

(18) **Contracting Officers** are responsible for:

(a) Ensuring that security requirements and security specifications are explicitly included in VA contracts, as per requiring or program direction;

(b) Coordinating contract documentation with the ISO and PO to ensure that contracts contain the required security language necessary for compliance with FISMA, and 38 U.S.C. §§ 5721-5728, 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) Monitoring COR surveillance to ensure contract requirements for contractors meet the appropriate background investigation requirements in accordance with VA Directive and Handbook 0710;

(d) Monitoring COR surveillance to ensure contractors complete VA's security and privacy awareness training and additional role-based training, as outlined in the contract;

(e) Monitoring COR surveillance of the contract to ensure security requirements are being met, consulting the ISO and/or PO as necessary; and

(f) Assisting other VA officials with significant information security responsibilities in remediating the weaknesses or deficiencies identified in the POA&M; updating the POA&M, conducting periodic compliance validation reviews, and completing the FISMA annual assessment to reduce or eliminate system vulnerabilities.

(19) **Contracting Officer's Representatives**

(a) Working with the ISO and PO to ensure contracts contain the required security language necessary for compliance with FISMA and 38 U.S.C. §§ 5721-5728 and to provide adequate security for information and information systems used by the contractor, including the requirement for signing VA Contractor ROB, when applicable;

(b) Ensuring contract requirements for contractors meet the appropriate background investigation requirements in accordance with VA Directive and Handbook 0710;

(c) Ensuring contractors complete VA's security and privacy awareness training and any additional role-based training, as outlined in the contract; and SOP

(d) Monitoring of the contract to ensure that security requirements are being met, consulting the ISO and/or PO as necessary;

(20) **Local Human Resources 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;

(b) Assisting other VA officials with significant information security responsibilities in remediating the weaknesses or deficiencies identified in the POA&M; updating the POA&M, conducting periodic compliance validation reviews, and completing the FISMA annual assessment to reduce or eliminate system vulnerabilities; and

(c) Ensuring the investigation of potential violations of security and privacy laws; VA policy, enforcement of consequences, and penalties against violators.

(21) **Users of VA Information Systems or VA Information** are responsible for complying with Appendix D, VA National ROB. The security responsibilities for general users have been extracted from this Handbook and are included in the 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 SYSTEM BOUNDARIES

a. VA will follow NIST's RMF in developing, operating, modifying, and removing systems. Procedures in this Handbook and other related OI&T 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, functions, 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 NIST 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, Information System Owners (in coordination with Information 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, and 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 will be used to determine the overall 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 using these steps:

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

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

(3) Determine the information system security categorization, 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.

c. Document the security categorization in the SSP.

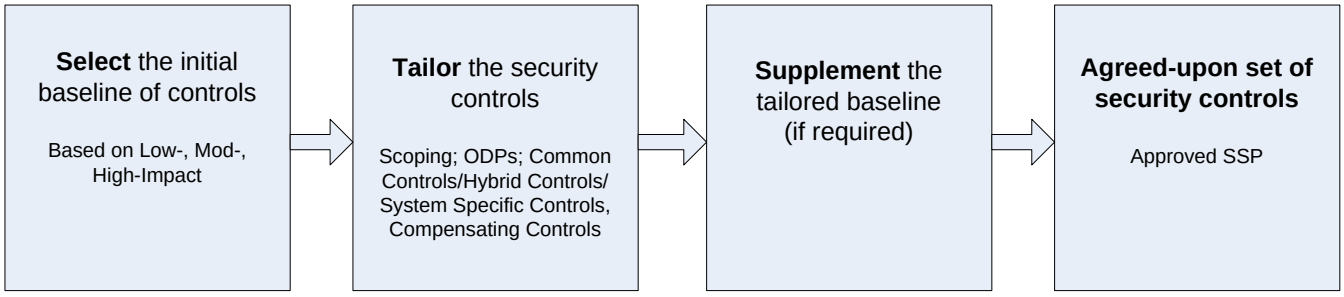
d. Describe the information system (including system boundary) and document the description in the SSP.

e. Register the information system in the VA-approved FISMA database.

7. SELECTION OF SECURITY CONTROLS – RMF STEP 2

When system categorization has been performed by determining the FIPS 200 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 NIST 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:

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

(2) Step 2: Tailor the security controls (common controls, scoping considerations, compensating controls, organization-defined parameters (ODP)).

(3) Step 3: Supplement the tailored baseline (if required).

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

a. **Selecting the Initial Baseline of Security Controls**: The selection of a set of baseline controls is based on the FIPS 200 impact level of the information as determined by the security categorization process. Information System Owners select one of three sets of security control baselines 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.)

b. **Tailoring the Security Controls:** Prior to implementing the applicable security control baseline, the controls must be tailored to align with the specific operating conditions of the information system to achieve a cost-effective and risk-based approach to providing information security. Information System Owners will ensure that appropriate Administration or Program Office officials are involved in evaluating the impact of security control implementation on mission and business processes to facilitate the tailoring of the security controls for the system. 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:

(1) Identifying and designating common controls – 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 Information 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. VA common controls are identified in

Appendix F, Attachment 1. System-specific controls are identified in Appendix F, Attachment 3. All other controls in Appendix F, including those in Appendix F, Attachment 3, are considered hybrid controls.

(2) Applying tailoring guidance to the baselines to develop a set of security controls for community-wide use or to address specialized requirements, technologies, or unique missions and environments of operation might be beneficial to VA in certain situations. This is known as creating overlays. See NIST SP 800-53 for additional information on overlays.

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

(a) *Control Allocation and Placement 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.

(b) *Operational/Environmental-Related Considerations:* Controls that depend upon operational/environmental factors may only apply if the factors are present in the environment. Where these factors are absent or significantly diverge from the baseline assumptions, it is justifiable to tailor the baseline. Some of the more common factors include:

1. Mobility: Since the control baseline assumes the operation of information systems in fixed facilities and non-mobile locations, when the systems operate primarily in mobile locations, the security controls should be tailored appropriately to account for the differences.

2. Single-User Operations: Security controls that address sharing among users may not be required for information systems that are designed to operate as single-user systems.

3. Data Connectivity and Bandwidth: Security controls that are related to a network environment may not be required for non-networked systems. For systems that have limited or sporadic bandwidth availability, a careful examination of the practicality of implementing network-related controls may be required.

4. Limited Functionality Systems: Machines that can be categorized as information systems but have limited functionality may also lack some general processing capabilities that are assumed in the security control baselines. These constraints may limit the nature of threats and also the appropriateness of some controls. System capabilities and the risk of compromise must be carefully balanced when controls are limited in this manner.

5. Information and System Non-Persistence: Security control baselines assume that information has some level of persistence. When information persistence is limited in duration, security controls may become candidates for removal or other forms of tailoring. This consideration may also apply to information systems and services when they also exist in non-persistent forms or forms of short duration. This is most likely to apply when virtualization techniques are involved.

6. Public Access: Public access to information systems may limit the applicability of some security controls. A careful balancing of the risk posture is required in this case.

(c) *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.

(d) *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:

1. 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;

2. Is supported by an assessment of risk; and

3. Does not affect the security-relevant information within the information system.

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

(e) *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.

(f) *Mission Requirements-Related Considerations:* If implementing security controls degrades, debilitates, or otherwise hampers critical VA missions or business functions, those controls may not be appropriate.

(4) Compensating Security Controls: After applying the scoping considerations, if the Information 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 controls described in Appendix F. The compensating controls must be designed to provide an equivalent or comparable level of protection to the information and information system to that of the original control. Information System Owners will ensure appropriate Administration or Program Office officials are involved in evaluating the impact of compensating security controls on mission and business processes to facilitate selection of appropriate compensating controls for the system. Compensating controls may be employed only under the following conditions:

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

(b) 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) The Information System Owner documents any compensating controls employed in lieu of the normal baseline control outlined in Appendix F in the SSP and obtains approval for the compensating controls from Office of Information Security (OIS) management with an OIS Risk-Based Decision (RBD). (See the Policy Section on the OCS Portal for information on the OIS RBD process.) OIS RBDs will expire annually or on the date identified in the OIS RBD, which must be less than 12 months from the requested date.

(5) ODPs: ODPs are portions of security controls containing VA management-defined parameters. VA identifies ODPs for common, hybrid, and system-specific controls in attachments to VA Handbook 6500, Appendix F. VA's ODPs are specified in VA Handbook 6500, Appendix F.

(a) The ODPs outlined in the Common ODPs, Attachment 1 are program management controls and have been determined to be applicable to all OI&T systems. OI&T management is responsible for implementing and managing these controls.

(b) The ODPs outlined in the Hybrid ODPs, Attachment 2 have been determined to be appropriate for all VA systems. The Information System Owner documents any deviation from these values or from the controls outlined in Appendix F (other than Attachment 3 controls) in the SSP and obtains approval for the deviation from OCS management with an OIS RBD. (See the Policy Section on the OCS Portal for information on the OIS RBD process.)

(c) The ODPs outlined in the System-Specific ODPs, Attachment 3 are recommended security control values for systems. Information System Owners should tailor these ODPs to align with the specific operating conditions of the information system as described above. ISOs must document any changes from the recommended values provided in Attachment 3 in a Local Risk-Based Decision (LRBD). Information System Owners should document the LRBD security control in the system's SSP.

c. **Supplementing the Baseline:**

(1) 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 tailored security controls are not adequate, additional security controls or control enhancements may be needed and added to the baseline. When this becomes necessary, existing controls and enhancements from NIST SP 800-53 should be used first. The following conditions are examples that might require supplemental controls to be added:

(a) Advanced Persistent Threat: security control baselines do not assume that attackers may have secured a presence within an information system. This threat may require additional controls.

(b) Cross-Domain Services: security control baselines assume no significant change in security policies when information flows across authorization boundaries. When security policies do differ across boundaries, it may become necessary to examine enhancements to security control, AC-4: Information Flow Enforcement and other security protections. More information is available in NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*.

(c) Mobility: security control baselines assume the operation of information systems in fixed facilities and non-mobile locations. When the systems operate primarily in mobile locations, additional controls and enhancements may be needed.

(d) Highly Sensitive Information and Information Sharing: when all users do not have the same privileges and authorization to access sensitive information, additional security controls and enhancements may be needed to protect that privileged access.

(e) Application-Layer Security: security controls that are normally implemented at the operating system level (such as access control) may also be employed at the application level to create an additional layer of protection.

(f) Documenting security control decisions and the rationale involved in the SSP is essential for the authorization process.

(2) Restrictions on the types of technologies used and how information systems are employed provide an alternative means to reduce or mitigate risk. Restrictions can be used in conjunction with or instead of, supplemental controls and may in some cases, be the most practical or reasonable actions to take. Examples of restrictions include:

(a) Limiting the information that can be processed, stored, and transmitted or the manner in which functions are automated;

(b) Prohibiting external access to information by removing network components that permit access (air-gapping); and

(c) Prohibiting sensitive information on system components that allow public access, unless an explicit risk determination can justify the access.

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

(4) The relevant risk management decisions that are made during the control selection and tailoring process must be documented in the SSP. This documentation, which shows the understanding, assumptions, constraints, and rationale supporting the decisions, is essential for making informed authorization decisions on information systems.

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

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

8. IMPLEMENT SECURITY CONTROLS – RMF STEP 3

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

b. Information System Owners will implement the VA-approved U.S. Government Configuration Baseline (USGCB) controls, formerly known as the Federal Desktop Core Configuration (FDCC), or Defense Information Systems Agency Security Technical Implementation Guides (DISA STIG).

9. ASSESS SECURITY CONTROLS – RMF STEP 4

a. OI&T 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 assessments and associated procedures.

c. The assessment plan reflects the type of assessment to be conducted (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. OI&T will employ assessors to assess the security controls in accordance with the procedures defined in the security assessment plan.

e. Information System Owners will ensure 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. Information 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.

h. The security assessment process is further defined in VA Handbook 6500.3, *Assessment, Authorization and Continuous Monitoring of VA Information Systems*.

10. AUTHORIZE INFORMATION SYSTEM – RMF STEP 5

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

c. The Information 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, and reputation), 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.

g. The security authorization process is further defined in VA Handbook 6500.3.

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. VA will define an Information Security Continuous Monitoring strategy to maintain visibility into VA assets, awareness of threats and vulnerabilities, and the effectiveness of deployed security controls and will determine the frequency with which each security control is assessed.

c. 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.

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

e. 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 the monitoring strategy.

f. 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, assets, individuals, and other organizations remains acceptable.

g. The Information System Owner follows VA Handbook 6500.1, *Electronic Media Sanitization* requirements when a system is removed from service.

h. Additional information regarding continuous monitoring in VA may be found in VA Handbook 6500.3.

This page is intentionally blank for the purpose of printing front and back copies.

APPENDIX A. TERMS AND DEFINITIONS

1. Application: A software program hosted by an information system. SOURCE: NIST SP 800-137

2. Application Wrapping: Applying additional security features, such as encryption, to a mobile application or group of applications to add layers of protection to mobile application(s) requiring additional security. SOURCE: VA Adapted

3. 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: NIST SP 800-37; VA Adapted

4. Authentication: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-27A; FIPS 200

5. 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: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37. In VA, this is the VA CIO.

6. Availability: Ensuring timely and reliable access to and use of information. SOURCE: 38 U.S.C. § 5727

7. Business Associate: An entity, including any individual, company, or organization that, performs or assists in the performance of a function or activity on behalf of VHA that involves the creation, receipt, maintenance, or transmission of protected health information (PHI), or that provides to or for VHA certain services as specified by the HIPAA Privacy Rule that involves the disclosure of PHI by VHA. SOURCE: 45 C.F.R. § 160.103; VHA Handbook 1605.05

8. Common Security Control: Security control that is inherited by one or more organizational information systems. SOURCE: NIST SP 800-53

These controls affect all VA facilities and systems with operations at the local site(s).

9. 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 NIST SP 800-53 and the Committee on National Security Systems Instruction (CNSSI) 1253, that provide equivalent or comparable protection for an information system. SOURCE: NIST SP 800-53

10. Confidentiality: Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. SOURCE: 38 U.S.C. § 5727

11. 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

12. Covered Entity: A covered entity subject to the HIPAA Privacy and Security Rules is (a) a health care provider who transmits any health information in electronic form in connection with a transaction covered by the Rules; (b) a health care clearinghouse; or (c) a health insurance plan. SOURCE: 45 C.F.R. §160.103

13. Critical Security Parameter (CSP): Security-related information (e.g., secret and private cryptographic keys, and authentication data such as passwords and PINs) whose disclosure or modification can compromise the security of a cryptographic module. SOURCE: FIPS 140-2

14. 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 HIPAA Privacy and Security Rules, which define ‘‘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 these Rules, 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

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

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

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

17. 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: NIST SP 800-53

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

19. Health Information: Health Information is any information, whether oral or recorded in any form or medium, created or received by a health care provider, health plan, public health authority, employer, life insurers, school or university, or health care clearinghouse or health plan that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. This encompasses information pertaining to examination, medical history, diagnosis, and findings or treatment, including laboratory examinations, X-rays, microscopic slides, photographs, and prescriptions. SOURCE: 45 C.F.R. § 160.103

20. 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: NIST SP 800-37; NIST SP 800-53; NIST SP 800-60; FIPS 200

21. 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: NIST SP 800-37; NIST SP 800-53; NIST SP 800-53A; CNSSI-4009

22. 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; NIST SP 800-53

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

23. Identity Theft: A fraud committed using the identifying information of another person. SOURCE: 15 U.S.C. § 1681a

24. Identity Theft Analysis: The regular analysis of all identity data housed in the Beneficiary Identification Records Locator Subsystem database on a quarterly basis to detect any organized misuse of those identities in the US commercial marketplace. SOURCE: VA Adapted

25. Individually Identifiable Health Information: 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 an individual, or the past, present, or future payment for the provision of health care to an individual, and (b) identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. SOURCE: 45 C.F.R. § 160.103

26. 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, or disposal which responsibilities may extend to interconnected systems or groups of interconnected systems. SOURCE: 38 U.S.C. § 5727

27. 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

28. 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

29. 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

30. 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: NIST SP 800-37; NIST SP 800-53; NIST SP 800-53A

31. 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

32. 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

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

34. 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: NIST SP 800-53; NIST SP 800-53A

35. Information Type: A specific category **o**f 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: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37; NIST SP 800-18; NIST SP 800-60; FIPS 200; FIPS 199; CNSSI-4009; 40 U.S.C. § 11101 and § 1401

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

37. 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 (MOU) or Memorandum of Agreement (MOA) between the organizations. SOURCE: NIST SP 800-47

38. 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

39. 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: NIST SP 800-37; NIST SP 800-53; NIST SP 800-60; FIPS 200

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

41. 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: NIST SP 800-37; NIST SP 800-53; NIST SP 800-53A; FIPS 200

42. 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; NIST SP 800-53; CNSSI-4009

43. Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA): 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 or MOA defines the responsibilities of two or more organizations in establishing, operating, and securing a system interconnection. SOURCE: NIST SP 800-47

44. Mobile Device: A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smartphones, tablets, and E-readers. SOURCE: NIST SP 800-53

45. 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: NIST SP 800-53; NIST SP 800-60; NIST SP 800-37; FIPS 200

46. Non-Sensitive Information/Data: Information for which the potential impact on organizational operations, operational assets, and individuals 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,or is not exempt from release under the Freedom of Information Act. SOURCE: FIPS 199

47. 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 Adapted

48. 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: NIST SP 800-53; NIST SP 800-37; FIPS 200

49. Overlays: A specification of security controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines. The overlay specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems. SOURCE: NIST SP 800-53

50. 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 which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. Information does not have to be retrieved by any specific individual or unique identifier (i.e., covered by the Privacy Act) to be PII. (See Sensitive Personal Information, below). SOURCE: OMB M-07-16

51. 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.

52. Portable Storage Devices: An information system component that can be inserted into and removed from an information system, and that is used to store data or information (e.g., text, video, audio, and/or image data). Such components are typically implemented on magnetic, optical, or solid state devices (e.g., floppy disks, compact/digital video disks, flash/thumb drives, external hard disk drives, and flash memory cards/drives that contain non-volatile memory). SOURCE: NIST SP 800-53

53. 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: NIST SP 800-53; NIST SP 800-60; NIST SP 800-37; FIPS 199

54. 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 confidentially or integrity of the data regardless of the manner in which the breach might have occurred. SOURCE: VA Directive 6509

55. 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; NIST SP 800-53; NIST SP 800-18; NIST SP 800-122; CNSSI-4009; OMB Memorandum 03-22

56. 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

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

58. 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: NIST SP 800-53

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

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

60. 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 OI&T, are business associates of VHA. SOURCE: 45 C.F.R. § 160.103; VA Directive 6066.

61. 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

62. Remote Access: Access by users (or information systems) communicating externally to an information system security perimeter. SOURCE: NIST 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 (email) 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.

63. 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: NIST SP 800-60

64. 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: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37

65. 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: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37

66. 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

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

68. 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

69. 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: NIST SP NIST 800-53; NIST SP 800-37; NIST SP 800-53A; NIST SP 800-60; FIPS 200; FIPS 199; CNSSI-4009

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

71. 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

72. 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

73. 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: NIST SP 800-37; NIST SP 800-53; NIST SP 800-53A; NIST SP 800-18; FIPS 200

74. 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: NIST SP 800-37; NIST SP 800-53; NIST SP 800-53A; CNSSI-4009

75. 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: NIST SP 800-37; NIST SP 800-53; NIST SP 800-53A; CNSSI-4009

76. 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: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37; FIPS 200

77. 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: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-27A; SP 800-60; NIST SP 800-37; CNSSI-4009

78. 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

79. Transient Electromagnetic Pulse Standard (TEMPEST): A name referring to the investigation, study, and control of unintentional compromising emanations from telecommunications and automated information systems equipment. SOURCE: FIPS 140-2

80. User: Individual or (system) process acting on behalf of an individual, and authorized to access an information system. SOURCE: NIST SP 800-53; NIST 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 information or VA information systems, these individuals must complete VA-approved security and privacy awareness training, sign the VA National ROB or Contractor ROB, and complete appropriate background screening before such access may be granted.

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

82. 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. SOURCE: 38 U.S.C. § 5727

83. VA Information/Data: Information collected or maintained by or on behalf of VA. 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

84. 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 information. SOURCE: 38 U.S.C. § 5727

85. 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 not only information that identifies an individual but also other 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 U.S.C. § 5727

86. 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: NIST SP 800-113

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

88. 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. SOURCE: VA Adapted

APPENDIX B. ACRONYMS AND ABBREVIATIONS

Acronym/ Abbreviation	Definition
A&A	Assessment and Authorization
AC	Access Control
AO	Authorizing Official
AT	Awareness and Training
ATO	Authority to Operate
AU	Audit and Accountability
CA	Security Assessment and Authorization
CBA	Certificate-Based Authentication
CBOC	Community Based Outpatient Clinic
CCB	Change Control Board
CD	Compact Disc
C.F.R.	Code of Federal Regulations
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CM	Configuration Management
CNSSI	Committee on National Security Systems Instruction
CO	Contracting Officer
COOP	Continuity of Operations Plan
COR	Contracting Officer's Representative
COTS	Commercial Off-The-Shelf
CP	Contingency Planning
CPO	Chief Privacy Officer
DAS	Deputy Assistant Secretary
DISA STIG	Defense Information Systems Agency Security Technical Implementation Guides
DoS	Denial of Service
DVD	Digital Video Disc
Email	Electronic Mail
EA	Enterprise Architecture
FDCC	Federal Desktop Core Configuration
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FSS	Field Security Service
GFE	Government Furnished Equipment

Acronym/ Abbreviation	Definition
HIPAA	Health Insurance Portability and Accountability Act
HISD	Health Information Security Division
HITECH	Health Information Technology for Economic and Clinical Health
HSPD	Homeland Security Presidential Directive
HTM	Healthcare Technical Management
HTTP	Hyper Text Transfer Protocol
IA	Identification and Authentication
ID	Identification
IRB	Institutional Review Board
IP	Individual Participation and Redress
IP	Internet Protocol
IR	Incident Response
ISA	Interconnection Security Agreement
ISO	Information Security Officer
IT	Information Technology
ITWD	Information Technology Workforce Development
LAN	Local Area Network
LRBD	Local Risk-Based Decision
MA	Maintenance
MAC	Media Access Control
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MP	Media Protection
NARA	National Archives and Records Administration
NCA	National Cemetery Administration
NIST	National Institute of Standards and Technology
VA-NSOC	Veterans Affairs Network Security Operations Center
OCS	Office of Cyber Security
ODP	Organization-Defined Parameters
OIG	Office of Inspector General
OIS	Office of Information Security
OI&T	Office of Information and Technology
OMB	Office of Management and Budget
OTP	One-Time Passcodes
P0	Priority Code 0 (Unspecified Priority Code)
P1	Priority Code 1
P2	Priority Code 2

Acronym/ Abbreviation	Definition
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
Pub.	Public
PS	Personnel Security
PVT	Patch and Vulnerability Team
RA	Risk Assessment
RBD	Risk-Based Decision
RMF	Risk Management Framework
ROB	Rules of Behavior
SA	System and Services Acquisition
SAML	Security Assertion Markup Language
SAOP	Senior Agency Official for Privacy
SC	System and Communications Protection
SCA	Security Control Assessment
SDLC	System Development Life Cycle
SI	System and Information Integrity
SOP	Standard Operating Procedure
SOW	Statement of Work
SP	Special Publication
SPI	Sensitive Personal Information
SSP	System Security Plan
TCP	Transmission Control Protocol
TEMPEST	Transient Electromagnetic Pulse Standard
TIC	Trusted Internet Connection
TMS	Talent Management System

Acronym/ Abbreviation	Definition
TLS	Transport Layer Security
TRM	Technical Reference Model
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	Department of Veterans Affairs
VBA	Veterans Benefits Administration
VHA	Veterans Health Administration
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network

APPENDIX C. REFERENCES

1. STATUTES AND REGULATIONS

a. 20 U.S.C. § 1232g, *Family Educational Rights and Privacy Act*

b. 38 C.F.R. § 1.201, *Employee's Duty to Report*

c. 38 C.F.R. § 1.204, *Information to be Reported to the Office of Inspector General*

d. 38 C.F.R. § 1.218, *Security and Law Enforcement at VA Facilities*

e. 38 C.F.R. §§ 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*

f. 38 C.F.R. §§ 1.500-1.527, *Release of Information from Department of Veterans Affairs Claimant Records*

g. 38 C.F.R. §§ 1.575-1.582, *Safeguarding Personal Information in Department of Veterans Affairs Records*

h. 38 C.F.R. §§ 17.500-17.511, *Confidentiality of Healthcare Quality Assurance Review Records*

i. 38 C.F.R. §§ 75.111-75.119, *Data Breaches*

j. 15 U.S.C. § 1681, *Fair Credit Reporting Act*

k. 38 U.S.C. § 5701, *Confidential Nature of Claims*

l. 38 U.S.C. § 5705, *Confidentiality of Medical Quality-Assurance Records*

m. 38 U.S.C. §§ 5721-5728, *Veteran's Benefits, Subchapter III - Information Security*

n. 38 U.S.C. § 7332, *Confidentiality of Certain Medical Records*

o. 40 U.S.C. § 11101, *Definitions*

p. Former 40 U.S.C. § 1401, *Definitions*

q. 44 U.S.C. §§ 3541-3549, *Federal Information Security Management Act of 2002 (FISMA)*

r. 45 C.F.R. Parts 160 and 164, *HIPAA Privacy and Security Rules45* C.F.R. §§ 164.103, 164.402, *Definitions*

s. 5 U.S.C., *Government Organization and Employees*

t. 5 U.S.C. § 552, *Freedom of Information Act*

u. 5 U.S.C. § 552a, *Privacy Act of 1974*

v. Pub. Law 104-191 § 264, 110 Stat. 1936, *Health Insurance Portability and Accountability Act*

w. Pub. Law 107-347 § 208, 116 Stat. 2899, 2921, *E-Government Act of 2002*

x. Pub. Law 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 140-2, *Security Requirements for Cryptographic Modules*

b. FIPS 191, *Guideline for The Analysis of Local Area Network Security*

c. FIPS 196, *Entity Authentication Using Public Key Cryptography*

d. FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*

e. FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*

f. FIPS 201, *Personal Identity Verification (PIV) 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, *Guide to Enterprise Patch Management Technologies*

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, *Security and Privacy Controls for Federal Information Systems and Organizations*

k. NIST SP 800-53 A, *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*: *Part 1: General; Part 2: Best Practices for Key Management Organizations; Part 3: Application-Specific Key Management Guidance*

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 I: Guide for Mapping Types of Information and Information Systems to Security Categories; and, Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*

o. NIST SP 800-61, *Computer Security Incident Handling Guide*

p. NIST SP 800-63-2, *Electronic Authentication Guideline*

q. NIST SP 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*

r. NIST SP 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*

s. NIST SP 800-73-3, *Interfaces for Personal Identity Verification (4 parts): Part 1: End Point PIV Card Application Namespace, Data Model and Representation; Part 2: PIV Card Application Card Command Interface; Part 3: PIV Client Application Programming Interface; and Part 4: The PIV Transitional Interfaces and Data Model Specification*

t. NIST SP 800-76, *Biometric Specifications for Personal Identity Verification*

u. NIST SP 800-78-3, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification (PIV)*

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*

i. OMB Memorandum M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12-Policy for a Common Identification Standard for Federal Employees and Contractors*

5. VA DIRECTIVES AND HANDBOOKS

a. VA Directive 0735, *Homeland Security Presidential Directive 12 (HSPD-12) Program*

b. VA Directive 5011/2, *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 0710, *Personnel Security and Suitability Program*

r. VA Handbook 0710, *Personnel Security and Suitability Program*

s. VA Directive 0730, *Security and Law Enforcement*

t. VA Handbook 0730, *Security and Law Enforcement*

u. VA Handbook 5011/5, *Hours of Duty and Leave*

v. VA Handbook 6300.6, *Procedures for Releasing Lists of Veterans' and Dependents' Names and Addresses*

w. VA Handbook 6330, *Directives Management Procedures*

x. VA Handbook 6500.1, *Electronic Media Sanitization*

y. VA Handbook 6500.2, *Management of Data Breaches Involving Sensitive Personal Information (SPI)*

z. VA Handbook 6500.3, *Assessment, Authorization and Continuous Monitoring of VA Information Systems*

aa. VA Handbook 6500.5, *Incorporating Security and Privacy into the System Development Life Cycle*

bb. VA Handbook 6500.6, *Contract Security*

cc. VA Handbook 6500.8, *Information System Contingency Planning*

dd. VA Handbook 6502.1, *Privacy Event Tracking*

ee. VA Handbook 6508.1, *Privacy Impact Assessment (PIA)*

ff. VA Handbook 7002-1, *Logistics Management Procedures*

6. VHA HANDBOOKS

a. VHA Handbook 1080.01, *Data Use Agreements*

b. VHA Handbook 1200.05, *Requirements for the Protection of Human Subjects in Research*

c. VHA Handbook 1605.05, *Business Associate Agreements*

7. OTHER REFERENCES

d. CNSSI-4009, *National Information Assurance Glossary*

e. Homeland Security Presidential Directive (HSPD) 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*

APPENDIX D. DEPARTMENT OF VETERANS AFFAIRS NATIONAL RULES OF BEHAVIOR

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 missions and functions." OMB Circular A-130, Appendix III, paragraph 3a(2)(a) requires that all Federal agencies promulgate 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. ROB must be signed annually by all users of VA information systems or VA information. All users of VA information systems or VA information, other than contractors/subcontractors, must sign the VA National Rules of Behavior. Contractors/subcontractors authorized to use VA information systems or access VA information, must sign the VA Contractor ROB, as 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 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 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), in 38 U.S.C. § 7332, 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, benefit, 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 Security and Privacy Awareness 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.

g. For Other Federal Government Agency users, documentation of a signed ROB will be provided by the VA requesting official to the TMS administrator for recording in TMS.

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 information, are required to sign in order to obtain access to VA information systems or VA information.

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 U.S. Department of Veterans Affairs (VA) information or information systems.

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 they contain or that may be accessed through them, as well as the security and protection of VA information in any form (e.g., digital, paper, verbal).

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 Information Security Officers (ISOs). Appropriate action may include monitoring, recording, copying, inspecting, restricting access, blocking, tracking, and disclosing information to authorized Office of Inspector General (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, and 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 Privacy Officer (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; Information System Owner, local Chief Information Officer (CIO), or designee; 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 Rules of Behavior (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 in 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 provides 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 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, POs, 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 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

(5) I understand VA's system of records may contain Confidential Medical Information that relates to the diagnosis or treatment of drug abuse, alcoholism or alcohol abuse, infection with the human immunodeficiency virus (HIV), or sickle cell anemia. I will not disclose information relating to the diagnosis or treatment of drug abuse, alcoholism or alcohol abuse, HIV, or sickle cell anemia without appropriate legal authority as outlined in applicable federal laws and regulations, including 38 U.S.C. § 7332. I understand my responsibilities as outlined in 38 U.S.C. § 7332, and I understand unauthorized disclosure of this information may have a serious adverse effect on agency operations, agency assets, or individuals.

b. Data Protection

(1) I will safeguard electronic VA sensitive information at work and remotely. I understand that all VA owned mobile devices and portable storage devices must be encrypted using Federal Information Processing Standards (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 Deputy Assistant Secretary for Information Security (DAS for OIS). This includes laptops, flash drives, and other removable storage devices and storage media (e.g., Compact Discs (CD), Digital Video Discs (DVD)).

(2) I understand that per VA Directive 6609, Mailing of Sensitive Personal Information (SPI), the following types of SPI 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 his or her personal representative (e.g., guardian, attorney-in-fact, attorney, or Veteran Service Organization contact person). 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 when sent to a person or entity that does not have the capability of decrypting the data, provided that the mailing is approved in advance and in writing by my supervisor or ISO.

(3) I understand that I must have approval from my supervisor to use, process, transport, transmit, download, or store electronic VA sensitive information remotely (outside of VA owned or managed facilities (e.g., medical centers, community based outpatient clinics (CBOC), or 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. VA owned and approved storage devices/media must use VA's approved configuration and security control requirements. The Information System Owner, local CIO, or designee, and ISO and PO must review and authorize the mechanisms for using,

processing, transporting, transmitting, downloading, or storing VA sensitive data outside of VA owned or managed facilities.

(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, whether regional-level 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 record retention requirements. Two secure options that can be used are to utilize a cross-cut shredder that meets VA and National Institute of Standards and Technology (NIST) 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 devices and portable storage devices (e.g., laptops, Universal Serial Bus (USB) flash drives, smartphones, tablets, personal digital assistants (PDA)).

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

(11) I will not auto-forward email 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 secure location.

(13) I will protect VA sensitive information from unauthorized disclosure, use, modification, or destruction, and will use 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, ISO, and/or Information System Owner, local CIO, or designee 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 Office of Information and Technology (OI&T) 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, ISO, and/or Information System Owner, local CIO, or designee when the access is no longer needed.

(2) I will only use 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 not share my password or verify codes. 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 by my VA supervisor, ISO, and/or Information System Owner, local CIO, or designee.

(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 are adequately secured in remote locations (e.g., at home and during travel). I agree that if I work from a remote location, pursuant to an approved telework agreement with VA sensitive information, authorized OI&T personnel may periodically inspect the remote location for compliance with security requirements.

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

(7) I will notify my VA supervisor, ISO, and/or Information System Owner, local CIO, or designee 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.

(9) I understand that VA prohibits access to VA's internal network from countries that pose a significant security risk. I will therefore not access VA's internal network from any foreign country designated as such unless approved by my VA supervisor, ISO, local CIO, and Information System Owner. This prohibition does not affect access to VA external web applications.

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 authorized in advance by my VA supervisor, ISO, and Information System Owner, local CIO, or designee. 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. I will follow VA Handbook 6500 requirements for connecting any non-VA equipment to VA's network.

(3) I will not use personally-owned information systems (capable of storing data) on-site at a VA facility to directly connect to VA's network. I will not use personally-owned information systems on-site to perform assigned official duties unless approved by the Information System Owner, local CIO, or designee. I will obtain my Information System Owner, local CIO, or designee's approval prior to using remote access capabilities to connect personally-owned equipment to VA's network while 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 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 OI&T 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 by my Information System Owner,

local CIO, or designee 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 time frames, 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 OI&T 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.

(5) If as an Other Federal Government Agency employee, I cause any level of data breach, I understand it may result in disciplinary or other adverse action, as well as criminal or civil penalties; and I recognize that I will be required to complete VA's security and privacy awareness training as part of incident remediation measures.

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

This page is intentionally blank for the purpose of printing front and back copies.

APPENDIX E. VA SYSTEM PRIVACY CONTROLS

1. BACKGROUND/OVERVIEW

a. Privacy, with respect to Personally Identifiable Information (PII), is a core value that can be obtained only with appropriate legislation, policies, procedures, and associated controls to ensure compliance with requirements. Protecting the privacy of PII collected, used, maintained, shared, and disposed of by programs and information systems, is a fundamental responsibility of VA. Effective privacy for individuals depends on the safeguards employed within the information systems that are processing, storing, and transmitting PII. VA cannot have effective privacy without a foundation of information security. However, privacy is more than security and includes, for example, the principles of transparency, notice, and choice.

b. This Appendix provides a structured set of controls for protecting privacy. It also serves as a roadmap for VA to use in identifying and implementing privacy controls concerning the entire life cycle of PII, whether in paper or electronic form. The controls focus on information privacy as a value distinct from, but highly interrelated with, information security. The privacy controls are based on the Fair Information Practice Principles embodied in the Privacy Act of 1974, Section 208 of the E-Government Act of 2002, and related OMB guidance. Fair Information Practice Principles are designed to build public trust in VA's privacy practices and to help VA avoid tangible costs and intangible damages stemming from privacy incidents.

c. Privacy controls are the administrative, technical, and physical safeguards employed within VA to protect and ensure the proper handling of PII. There are eight privacy control families with each family aligning with one of the Fair Information Practice Principles. The privacy control families can be implemented at VA, Department, Agency, component, office, program, or information system level, under the leadership of the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and in coordination with the CISO, CIO, program officials, and legal counsel. Table 1, taken from the privacy control catalog, provides a summary of the privacy controls by family.

TABLE 1: SUMMARY OF PRIVACY CONTROLS BY FAMILY

ID	PRIVACY CONTROLS
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-6	Privacy Reporting
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

d. There is a strong similarity in the structure of the privacy controls in this Appendix and the security controls in Appendix F of this Handbook. Moreover, the use of privacy plans in conjunction with security plans can provide an opportunity for VA to select the appropriate set of security and privacy controls in accordance with VA mission/business requirements and the environments in which VA operates. Incorporating the fundamental concepts associated with managing information security risk helps to ensure that the employment of privacy controls is carried out in a cost-effective and risk-based manner while simultaneously meeting compliance requirements.

2. PRIVACY CONTROLS

a. Authority and Purpose (AP)

This family furthers compliance with the Privacy Act by ensuring VA will: (i) identify the legal basis that authorize a particular PII collection or activity that impacts privacy; and (ii) specify in their notices, the purpose(s) for which PII is collected.

(1) AP-1: Authority to Collect

(a) Control: VA will determine the legal authority that permits the collection, use, maintenance, and sharing of PII, either generally or in support of a specific program or information system need.

(b) Supplemental Guidance: Before collecting PII in connection with an information system or program, VA will determine whether the contemplated collection of PII is legally authorized. Program officials consult with the SAOP/CPO and legal counsel regarding the authority of any program or activity to collect PII. The authority to collect PII is documented in the System of Records Notice (SORN), Privacy Act Statement and PIAs.

(2) AP-2: Purpose Specification

(a) Control: VA will describe the purpose(s) for which PII is collected, used, maintained, and shared in its privacy notices.

(b) Supplemental Guidance: Often, statutory language expressly authorizes specific collections and uses of PII. When statutory language is written broadly and thus subject to interpretation, VA will ensure, in consultation with the SAOP/CPO and legal counsel, that there is a close nexus between the general authorization and any specific collection of PII. Once the specific purposes have been identified, the purposes are clearly described in the related privacy compliance documentation, including but not limited to PIAs, SORNs, and Privacy Act Statements on forms VA uses to collect PII. Further, in order to avoid unauthorized collections or uses of PII, personnel who handle PII receive training on VA authorities for collecting PII and on the contents of notice.

b. **Accountability, Audit, and Risk Management (AR)**

This family enhances public confidence through effective controls for governance, monitoring, risk management, and assessment to demonstrate that VA complies with applicable privacy protection requirements thus minimizing overall privacy risk.

(1) **AR-1: Governance and Privacy Program**

(a) Control: VA will:

1. Appoint a SAOP/CPO accountable for developing, implementing, and maintaining a VA-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of PII by programs and information systems;

2. Monitor federal privacy laws and policy for changes that affect the privacy program;

3. Allocate sufficient budget and staffing resources to successfully implement and operate a VA-wide privacy program;

4. Develop a strategic VA privacy plan for implementing applicable privacy controls, policies, and procedures;

5. Develop, disseminate, and implement operational privacy policies and procedures that govern the appropriate privacy controls for programs, information systems, or technologies involving PII; and

6. Update privacy plan, policies, and procedures every 5 years in accordance with VA Directive 6330, *Directives Management*.

(b) Supplemental Guidance:

1. The development and implementation of a comprehensive governance and privacy program demonstrates VA accountability for, and commitment to, the protection of individual privacy. Accountability begins with the appointment of an SAOP/CPO with the authority, mission, resources, and responsibility to develop and implement a multifaceted privacy program. The SAOP/CPO, in consultation with legal counsel and information security officials: (i) ensures the development, implementation, and enforcement of privacy policies and procedures; (ii) defines roles and responsibilities for protecting PII; (iii) determines the level of information sensitivity with regard to PII holdings; (iv) identifies the laws, regulations, and internal policies that apply to the PII; (v) monitors privacy best practices; and (vi) monitors/audits compliance with identified privacy controls.

2. To further accountability, the SAOP/CPO develops privacy plans to document the privacy requirements of VA and the privacy and security controls in place or planned for meeting those requirements. The plan serves as evidence of VA privacy operations and supports resources requested by the SAOP/CPO. A single plan or multiple plans may be necessary depending upon VA structures, requirements, and resources, and the plan(s) may vary in comprehensiveness. For example, a one-page privacy plan may cover privacy policies, documentation, and controls already in place, such as PIAs and SORNs. A comprehensive plan may include a baseline of privacy controls selected from this Appendix and include: (i) processes for conducting privacy risk assessments; (ii) templates and guidance for completing PIAs and SORNs; (iii) privacy training and awareness requirements; (iv) requirements for contractors processing PII; (v) plans for eliminating unnecessary PII holdings; and (vi) a framework for measuring annual performance goals and objectives for implementing identified privacy controls.

(2) **AR-2: Privacy Impact and Risk Assessment**

(a) Control: VA will:

1. Establish a privacy risk assessment process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, and use of PII;

2. Conduct a PIA for information systems and programs in accordance with applicable law, OMB policy, and any existing VA policies and procedures; and

3. Follow a documented, repeatable process for conducting, reviewing, and approving PIAs.

(b) Supplemental Guidance: VA privacy risk assessment processes operate across the life cycles of all mission/business processes that collect, use, maintain, share, or dispose of PII. OMB M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, includes guidance on when PIAs are required for information systems. VA may be required by law or policy to extend the PIA requirements to other activities involving PII or otherwise impacting privacy, for example, programs, projects, or regulations. PIAs are conducted to identify privacy risks and identify methods to mitigate those risks. PIAs are also conducted to ensure that programs or information systems comply with legal, regulatory, and policy requirements. PIAs also serve as notice to the public privacy practices. PIAs are performed before developing or procuring information systems, or initiating programs or projects, that collect, use, maintain, or share PII and are updated when changes create new privacy.

(3) **AR-3: Privacy Requirements for Contractors and Service Providers**

(a) Control: VA will:

1. Establish privacy roles and responsibilities for contractors and service providers; and

2. Include privacy requirements in contracts and other acquisition-related documents.

(b) Supplemental Guidance:

1. Contractors and service providers include, but are not limited to, service bureaus, information providers, information processors, and other organizations providing information system development, IT services, and other outsourced applications.

2. VA will consult with legal counsel, SAOP/CPO, and COs about applicable laws, directives, policies, or regulations that may impact implementation of this control.

(4) **AR-4: Privacy Monitoring and Auditing**

(a) Control: VA will monitor and audit privacy controls and internal privacy policy every 5 years in accordance with VA Directive 6330 to ensure effective implementation.

(b) Supplemental Guidance:

1. To promote accountability, VA will identify and address gaps in privacy compliance, management, operational, and technical controls by conducting regular assessments (e.g., internal risk assessments). These assessments can be self-assessments or third-party audits that result in reports on compliance gaps identified in programs, projects, and information systems.

2. In addition to auditing for effective implementation of all privacy controls identified in this Attachment, VA will assess whether it should: (i) implement a process to embed privacy considerations into the life cycle of programs, information systems, mission/business processes, and technology; (ii) monitor for changes to applicable privacy laws, regulations, and policies; (iii) track programs, information systems, and applications that collect and maintain PII to ensure compliance; (iv) ensure access to PII is only on a need-to-know basis; and (v) ensure PII is being maintained and used only for the legally authorized purposes identified in the public notice(s).

3. VA will also: (i) implement technology to audit for the security, appropriate use, and loss of PII; (ii) perform reviews to ensure physical security of documents containing PII; and (iii) assess contractor compliance with privacy requirements.

4. The SAOP/CPO coordinates monitoring and auditing efforts with information security officials and ensures that the results are provided to senior managers and oversight officials.

(5) **AR-5: Privacy Awareness and Training**

(a) Control: VA will:

1. Develop, implement, and update a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures;

2. Administer basic privacy awareness training annually and targeted, role-based privacy training for personnel having responsibility for PII or for activities that involve PII annually; and

3. Ensure that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements annually.

(b) Supplemental Guidance:

1. Specific training methods may include: (i) mandatory annual privacy awareness training; (ii) targeted, role-based training; (iii) internal privacy program Web sites; (iv) manuals, guides, and handbooks; (v) slide presentations; (vi) events (e.g., privacy awareness week, privacy clean-up day); (vii) posters and brochures; and (viii) email messages to all employees and contractors.

2. VA will update training based on changing statutory, regulatory, mission, program, business process, and information system requirements, or on the results of compliance monitoring and auditing.

(6) **AR-6: Privacy Reporting**

(a) Control: VA will develop, disseminate, and update reports to OMB and Congress to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.

(b) Supplemental Guidance:

1. Through external and internal privacy reporting, VA will promote accountability and transparency in VA privacy operations. Reporting also helps VA determine progress in meeting privacy compliance requirements and privacy controls, compare performance across the federal government, identify vulnerabilities and gaps in policy and implementation, and identify success models. Types of privacy reports include: (i) annual SAOP reports to OMB; (ii) reports to Congress required by Pub. Law 110-53, *Implementing Regulations of the 9/11 Commission Act*; (iii) other public reports required by specific statutory mandates or internal policies of VA.

2. The SAOP/CPO consults with legal counsel, where appropriate, to ensure that VA meets all applicable privacy reporting requirements.

(7) **AR-7: Privacy-Enhanced System Design and Development**

(a) Control: VA will design information systems to enhance privacy by automating privacy controls.

(b) Supplemental Guidance:

1. To the extent feasible when designing VA information systems, VA will employ technologies that automate privacy controls on the collection, use, and disclosure of PII.

2. When building privacy controls into system design, VA will mitigate privacy risks to PII, thereby reducing the likelihood of information system breaches and other privacy-related incidents.

3. VA will also conduct periodic reviews of systems' collection, use, and disclosure of PII to assess compliance with the Privacy Act and VA's privacy policy.

4. VA will regularly monitor information system use and sharing of PII to ensure that the use/sharing is consistent with the authorized purposes identified in the Privacy Act and/or in the public notice of VA, or in a manner compatible with those purposes.

(8) **AR-8: Accounting of Disclosures**

(a) Control: VA will, consistent with, and subject to, exceptions in the Privacy Act:

1. Keep an accurate accounting of disclosures of information held in each system of records under its control, including:

a. Date, nature, and purpose of each disclosure of a record; and

b. Name and address of the person or agency to which the disclosure was made.

2. Retain the accounting of disclosures for the life of the record or 5 years after the disclosure is made, whichever is longer; and

3. Make the accounting of disclosures available to the person named in the record upon request.

(b) Supplemental Guidance: The SAOP/CPO periodically consults with managers of VA systems of record to ensure that the required accountings of disclosures of records are being properly maintained and provided to persons named in those records consistent with the provisions of the Privacy Act.

c. **Data Quality and Integrity (DI)**

This family ensures compliance with Section 552a (e)(2) of the Privacy Act of 1974 and enhances public confidence that any PII collected and maintained by VA is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in public notices.

(1) **DI-1: Data Quality**

(a) Control: VA will:

1. Confirm to the greatest extent practicable upon collection or creation of PII, the accuracy, relevance, timeliness, and completeness of that information;

2. Collect PII directly from the individual to the greatest extent practicable;

3. Check for, and correct as necessary, any inaccurate or outdated PII used by its programs or systems annually; and

4. Issue guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

(b) Supplemental Guidance:

1. VA will take reasonable steps to confirm the accuracy of PII. Such steps may include, for example, editing and validating addresses as they are collected or entered into information systems using automated address verification look-up application programming interfaces (API). The types of measures taken to protect data quality may be based on the nature and context of the PII, how it is to be used, and how it was obtained. Measures taken to validate the accuracy of PII that is used to make determinations about the rights, benefits, or privileges of individuals under federal programs may be more comprehensive than those used to validate less sensitive PII. Additional steps may be necessary to validate PII that is obtained from sources other than individuals or the authorized representatives of individuals.

2. When PII is of a sufficiently sensitive nature, VA will incorporate mechanisms into information systems and develop corresponding procedures for how frequently, and by what method, the information is to be updated.

(c) Control Enhancements:

1. Data Quality | Validate PII: VA will request that the individual or individual's authorized representative validate PII during the collection process.

2. Data Quality | Re-validate PII: VA will request that the individual or individual's authorized representative revalidate PII when possible.

(2) **DI-2: Data Integrity and Data Integrity Board**

(a) Control: VA will:

1. Document processes to ensure the integrity of PII through existing security controls; and

2. Establish a Data Integrity Board when appropriate to oversee VA Computer Matching Agreements and to ensure that those agreements comply with the computer matching provisions of the Privacy Act.

(b) Supplemental Guidance: VA will conduct or participate in Computer Matching Agreements with other organizations regarding applicants for and recipients of financial assistance or payments under federal benefit programs, and applicants for and holders of positions as Federal personnel, establish a Data Integrity Board to oversee and coordinate their implementation of such matching agreements. In many organizations, the Data Integrity Board is led by the SAOP/CPO. The Data Integrity Board ensures that the controls are in place to maintain both the quality and the integrity of data shared under Computer Matching Agreements.

d. **Data Minimization and Retention (DM)**

This family helps VA implement the data minimization and retention elements of the Privacy Act of 1974, which requires VA to collect, use, and retain only PII that is relevant and necessary for the specified purpose it was originally collected. VA will retain PII for only as long as necessary to fulfill the specified purpose(s) and in accordance with a National Archives and Records Administration (NARA)-approved record retention schedule.

(1) **DM-1: Minimization of Personally Identifiable Information**

(a) Control: VA will:

1. Identify the minimum PII elements (e.g., name, address, date of birth) that are relevant and necessary to accomplish the mission and are legally authorized to collect;

2. Limit the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent; and

3. Conduct an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings annually to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.

(b) Supplemental Guidance:

1. The collection of PII is consistent with a purpose authorized by law or regulation. The minimum set of PII elements required to support a specific VA business process may be a subset of the PII VA is authorized to collect. Program officials consult with SAOP/CPO and legal counsel to identify the minimum PII elements required by the information system or activity to accomplish the legally authorized purpose.

2. VA can further reduce their privacy and security risks by also reducing their inventory of PII, where appropriate. OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, requires VA to conduct both an initial review and subsequent reviews of their holdings of all PII and ensure, to the maximum extent practicable, that such holdings are accurate, relevant, timely, and complete. VA is also directed by OMB to reduce their holdings to the minimum necessary for the proper performance of a documented VA business purpose. OMB M-07-16 requires VA to develop and publicize, either through a notice in the Federal Register or on their Web sites, a schedule for periodic reviews of their holdings to supplement the initial review. Reductions in VA holdings of PII are consistent with NARA retention schedules.

(c) Control Enhancement: *Minimization of Personally Identifiable Information* | *Locate/Remove/Redact/Anonymize PII:* VA, where feasible and within the limits of technology, will locate and remove/redact specified PII and/or use anonymization and de-identification techniques to permit use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure. Refer to NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, for further guidance on anonymization.

(2) **DM-2: Data Retention and Disposal**

(a) Control: VA will:

1. Retain PII for the minimum amount of time to fulfill the purpose(s) identified in the notice or as required by law;

2. Dispose of, destroy, erase, and/or anonymize the PII, regardless of the method of storage in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and

3. Use approved records disposition schedules to ensure secure deletion or destruction of PII (including originals, copies, and archived records).

(b) Supplemental Guidance:

1. Program officials coordinate with records officers and with NARA to identify appropriate retention periods and disposal methods.

2. Certain read-only archiving techniques, such as DVDs, CDs, microfilm, or microfiche may not permit the removal of individual records without the destruction of the entire database contained on such media.

(c) Control Enhancement: *Data Retention and Disposal* | *System Configuration:* VA, where feasible, will configure its information systems to record the date PII is collected, created, or updated and when PII is to be deleted or archived under an approved record retention schedule.

(3) **DM-3: Minimization of PII Used in Testing, Training, and Research**

(a) Control: VA will:

1. Develop policies and procedures for the use of PII for testing, training, and research; and

2. Implement controls to protect PII used for testing, training, and research.

(b) Control Enhancement: *Minimization for PII Used in Testing, Training, and Research* | *Risk* Minimization *Techniques:* VA, where feasible, will use techniques to minimize the risk to privacy of using PII for testing, training, and research.

e. **Individual Participation and Redress (IP)**

This family addresses the need to make individuals active participants in the decision-making process regarding the collection and use of their PII, as required by the Privacy Act of 1974. By providing individuals with access to PII and the ability to have their PII corrected or amended, as appropriate, the controls in this family enhance public confidence in VA decisions made based on the PII.

(1) **IP-1: Consent**

(a) Control: VA will:

1. Provide means, where feasible and appropriate, for individuals to authorize the collection, use, maintenance, and sharing of PII prior to its collection;

2. Provide appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII;

3. Obtain consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and

4. Ensure that individuals are aware of, and where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time VA collected the PII.

(b) Supplemental Guidance:

1. To obtain consent, VA will provide individuals appropriate notice of the purposes of the PII collection or technology used and a means for individuals to consent to the activity. VA will tailor the public notice and consent mechanisms to meet operational needs.

2. VA may obtain consent through opt-in, opt-out, or implied consent. Opt-in consent is the preferred method, but it is not always feasible. Opt-in requires that individuals take affirmative action to allow VA to collect or use PII. In contrast, opt-out requires individuals to take action to prevent the collection or use of such PII. Implied consent is the least preferred method and should be used in limited circumstances. Implied consent occurs where individuals' behavior or failure to object indicates agreement with the collection or use of PII (e.g., by entering and remaining in a building where notice has been posted that security cameras are in use, the individual implies consent to the video recording). Depending on the nature of the program or information system, it may be appropriate to allow individuals to limit the types of PII they provide and subsequent uses of that PII. VA consent mechanisms include a discussion of the consequences to individuals for failure to provide PII.

(c) Control Enhancement: Consent | Mechanisms Supporting Itemized or Tiered Consent: VA will implement mechanisms to support itemized or tiered consent for specific uses of data.

(2) **IP-2: Individual Access**

(a) Control: VA will, consistent with, and subject to, exceptions in the Privacy Act:

1. Provide individuals the ability to have access to their PII maintained in its system(s) of records in order to determine whether to have the PII corrected or amended, as appropriate;

2. Publish rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records;

3. Publish access procedures in SORNs; and

4. Adhere to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

(b) Supplemental Guidance:

1. Access affords individuals the ability to review their own PII held within VA systems of records. Access includes timely, simplified, and inexpensive access to data.

2. The SAOP/CPO is responsible for the content of Privacy Act regulations and record request processing, in consultation with legal counsel.

(3) **IP-3: Redress**

(a) Control: VA will:

1. Provide a process for individuals to have inaccurate PII maintained by VA corrected or amended, as appropriate; and

2. Establish a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information sharing partners, and where feasible and appropriate, notifies affected individuals that their information has been corrected or amended.

(b) Supplemental Guidance:

1. Effective redress processes demonstrate VA commitment to data quality especially in those business functions where inaccurate data may result in inappropriate decisions or denial of benefits and services to individuals.

2. VA will apply direction in determining if records are to be corrected or amended, based on the scope of redress requests, the changes sought, and the impact of the changes. Individuals may appeal an adverse decision and have incorrect information amended, where appropriate.

3. VA will: (i) provide effective notice of the existence of a PII collection; (ii) provide plain language explanations of the processes and mechanisms for requesting access to records; (iii) establish criteria for submitting requests for correction or amendment; (iv) implement resources to analyze and adjudicate requests; (v) implement means of correcting or amending data collections; and (vi) review any decisions that may have been the result of inaccurate information

4. VA redress processes will provide responses to individuals of decisions to deny requests for correction or amendment, including reasons for those decisions, a means to record individual objections to VA decisions, and a means of requesting VA reviews of the initial determinations.

5. Where PII is corrected or amended, VA will take steps to ensure that all authorized recipients of that PII are informed of the corrected or amended information.

6. In instances where redress involves information obtained from other organizations, redress processes included coordination with organizations that originally collected the information.

(4) **IP-4 – Complaint Management**

(a) Control: VA will implement a process for receiving and responding to complaints, concerns, or questions from individuals about VA privacy practices.

(b) Supplemental Guidance:

1. VA will provide complaint mechanisms that are readily accessible by the public, include all information necessary for successfully filing complaints (including contact information for the SAOP/CPO or other official designated to receive complaints), and are easy to use.

2. VA complaint management processes will include tracking mechanisms to ensure that all complaints received are reviewed and appropriately addressed in a timely manner.

f. **Security (SE)**

This family supplements the security controls in Appendix F of this Handbook to ensure administrative, technical, and physical safeguards are in place to protect PII collected or maintained by VA against loss, unauthorized access, or disclosure, as required by the Privacy Act, and to ensure that VA planning and responses to privacy incidents comply with OMB policies and guidance. The controls in this family are implemented in coordination with information security personnel and in accordance with the existing NIST RMF.

(1) **SE-1: Inventory of Personally Identifiable Information**

(a) Control: VA will:

1. Establish, maintain, and update annually an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII; and

2. Provide each update of the PII inventory to the CIO and ISO annually to support the establishment of information security requirements for all new or modified information systems containing PII.

(b) Supplemental Guidance:

1. As one method of gathering information for its PII inventory, VA may extract the following information elements from PIAs of information systems containing PII: (i) the name and acronym for each system identified; (ii) the types of PII contained in that system; (iii) classification of level of sensitivity of all types of PII, as combined in that information system; and (iv) classification of level of potential risk of substantial harm, embarrassment, inconvenience, or unfairness to affected individuals, as well as the financial or reputational risks to VA, if PII is exposed.

2. VA will take due care in updating the inventories by identifying linkable data that could create PII.

(2) **SE-2: Privacy Incident Response**

(a) Control: VA will:

1. Develop and implement a Privacy Incident Response Plan; and

2. Provide an organized and effective response to privacy incidents in accordance with VA Privacy Incident Response Plan.

(b) Supplemental Guidance:

1. A VA Privacy Incident Response Plan includes: (i) the establishment of a cross-functional Privacy Incident Response Team that reviews, approves, and participates in the execution of the Privacy Incident Response Plan; (ii) a process to determine whether notice to affected individuals is required, and where appropriate, to provide that notice; (iii) a privacy risk assessment process to determine the extent of harm, embarrassment, inconvenience, or unfairness to affected individuals and, where appropriate, to take steps to mitigate any such risks; and (iv) internal procedures to ensure prompt reporting by employees and contractors of any privacy incident to ISOs and the SAOP/CPO, consistent with VA incident management structures.

2. VA may choose to integrate Privacy Incident Response Plans with Security Incident Response Plans, or keep the plans separate.

g. **Transparency (TR)**

This family implements Section 552a (e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act, which require public notice of VA information practices and the privacy impact of government programs and activities.

(1) **TR-1: Privacy Notice**

(a) Control: VA will:

1. Provide effective notice to the public and to individuals regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal for PII; (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how VA uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary;

2. Describe: (i) the PII VA collects and the purpose(s) for which it collects that information; (ii) how VA uses PII internally; (iii) whether VA shares PII with external entities, the categories of those entities, and the purposes for such sharing; (iv) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (v) how individuals may obtain access to PII for the purpose of having it amended or corrected, where appropriate; and (vi) how the PII will be protected; and

3. Revise its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change.

(b) Supplemental Guidance:

1. VA may provide general public notice through a variety of means, as required by law or policy, including SORNs, PIAs, in a Web site privacy policy, or in an Information Sharing Privacy Policy.

2. As required by the Privacy Act, VA will also provide direct notice to individuals via Privacy Act Statements on the paper and electronic forms it uses to collect PII.

3. VA SAOP/CPO is responsible for the content of VA's public notices, in consultation with legal counsel and relevant program managers.

(c) Control Enhancement:

1. *Privacy* Notice | Real-Time or Layered Notice: VA provides real-time and/or layered notice when it collects PII.

2. Supplemental Guidance: A layered notice approach involves providing individuals with a summary of key points in VA's privacy policy. A second notice provides more detailed/specific information.

(2) **TR-2: System of Records Notices and Privacy Act Statements**

(a) Control: VA, consistent with the Privacy Act, will:

1. Publish in the Federal Register, SORNs for information systems containing PII;

2. Keep SORNs current; and

3. Include Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.

(b) Supplemental Guidance:

1. VA will issue SORNs to provide the public notice regarding PII collected in a system of records.

2. Privacy Act Statements provide notice of: (i) the authority of VA to collect PII; (ii) whether providing PII is mandatory or optional; (iii) the principal purpose(s) for which the PII is to be used; (iv) the intended disclosures (routine uses) of the information; and (v) the consequences of not providing all or some portion of the information requested.

(c) Control Enhancement: System of Records Notices and Privacy Act Statements | Public Web Site Publication: VA will publish SORNs on its public Web site.

(3) **TR-3: Dissemination of Privacy Program Information**

(a) Control: VA will:

1. Ensure that the public has access to information about its privacy activities and is able to communicate with its SAOP/CPO; and

2. Ensure that its privacy practices are publicly available through VA Web sites or otherwise.

(b) Supplemental Guidance: VA will employ different mechanisms for information from the public about their privacy practices including, but not limited to, PIAs, SORNs, privacy reports, publicly available web pages, email distributions, blogs, and periodic publications (e.g., quarterly newsletters). VA will also employ publicly facing email addresses and/or phone lines that enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices.

h. **Use Limitation (UL)**

This family helps VA comply with the Privacy Act, which prohibits the use of PII that is either not specified in notices, incompatible with the specified purposes, or not otherwise permitted by law. Implementation of the controls in this family will ensure that the scope of PII use is limited accordingly.

(1) **UL-1: Internal Use**

(a) Control: VA will use PII internally only for authorized purpose(s) identified in the Privacy Act and/or in public notices.

(b) Supplemental Guidance:

1. VA will take steps to ensure that they use PII only for legally authorized purposes and in a manner compatible with uses identified in the Privacy Act and/or in public notices. These steps include monitoring and auditing VA use of PII and training VA personnel on the authorized uses of PII.

2. With guidance from the SAOP/CPO and where appropriate, legal counsel, assess whether they fall within the scope of VA authorities.

3. Where appropriate, VA will obtain consent from individuals for the new use(s) of PII.

(2) **UL-2: Information Sharing with Third Parties**

(a) Control: VA will:

1. Share PII externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or in a manner compatible with these purposes;

2. Where appropriate, enter into MOU or MOA, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used;

3. Monitor, audit, and train its staff on the authorized uses and sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and

4. Evaluate any proposed new instances of sharing PII with third parties to assess whether they are authorized and whether additional or new public notice is required.

(b) Supplemental Guidance: VA SAOP/CPO and, where appropriate, legal counsel review and approve any proposed external sharing of PII, including with other public and private sector entities, for consistency with uses described in the existing VA public notice(s). Where a new instance of external sharing of PII is authorized but not compatible with the purpose(s) specified in existing public notices, or as otherwise permitted by the Privacy Act, VA will review, update, and republish their PIAs, SORNs, Web site privacy policies, and other public notices, if any, to include specific descriptions of the new use(s) and obtain consent where appropriate and feasible. Information-sharing agreements also include security protections consistent with the sensitivity of the information being shared.

APPENDIX F. VA SYSTEM SECURITY CONTROLS

3. 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 OI&T systems and other designated systems when appropriate and technically possible. The VA CIO has delegated the implementation of appropriate security controls to the Information System Owner. This Appendix has been prepared to assist the Information 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 NIST 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 Information System Owner, they are documented in the SSP and approved by the VA CIO (as the AO) 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 systems.

b. Information 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. Information System Owners should use the current version of NIST SP 800-53 for supplemental controls required for their systems.

c. FIPS 200 and the current version of NIST 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 NIST 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:

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

d. 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 NIST 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.

e. VA requires that Operating Units comply with all FIPS mandates and recommendations of the current version of NIST 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 NIST SP 800-53 and VA's organizational controls based on VA's specific environment.

f. 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.

g. Security controls can be designated as one of three types:

(1) Common Controls: 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; or (iii) common information systems, subsystems, or applications (i.e., common hardware, software, and/or firmware) deployed at multiple operational sites. Common security controls, typically identified during a collaborative agency-wide process with the involvement of the VA CIO (who is the AO), 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:

(a) 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

(b) 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.

(c) 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. Controls not listed in **Attachment 1** (common controls) or **Attachment 3** (system-specific controls) are hybrid controls. Hybrid controls with ODPs are identified 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.

h. Information 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 security control baselines.

i. Figure-3: *Security Control Selection Process* is a flowchart that describes the security control selection process.

FIGURE 3: SECURITY CONTROL SELECTION PROCESS

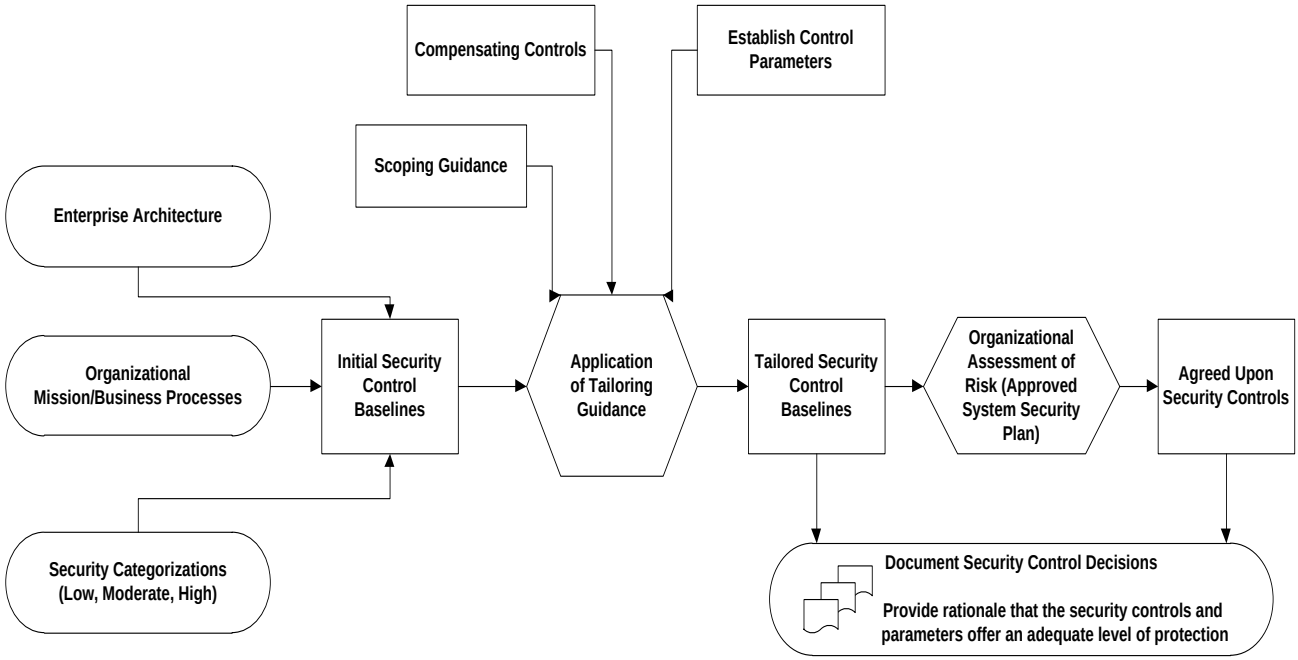


Figure 3 is a flowchart that describes the security control selection process that has been defined in VA Handbook 6500.

Table 2, below, summarizes sequence priority codes for the security control baselines identified in Table 3: Security Controls Baselines, which follows.

TABLE 2: SECURITY CONTROLS PRIORITIZATION CODES

Priority Code	Sequencing	Action
Unspecified Priority Code **(P0)**	NONE	Security control not selected in any baseline
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

Table 3, below, describes the initial security controls baselines for systems designated as low-impact, moderate-impact, and high-impact.

TABLE 3: SECURITY CONTROLS BASELINES

Control Number	Control Name	Priority	Initial 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)(5)(11)(12)(13)
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)(5)(9)(10)	AC-6 (1)(2)(3)(5)(9)(10)
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	P0	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	P3	Not Selected	Not Selected	AC-10
AC-11	Session Lock	P3	Not Selected	AC-11 (1)	AC-11 (1)
AC-12	Session Termination	P2	Not Selected	AC-12	AC-12
AC-13	Withdrawn	---	---	---	---
Access Controls, concluded					
AC-14	Permitted Actions without Identification or Authentication	P3	AC-14	AC-14	AC-14
AC-15	Withdrawn	---	---	---	---
AC-16	Security Attributes	P0	Not Selected	Not Selected	Not Selected
AC-17	Remote Access	P1	AC-17	AC-17 (1)(2)(3)(4)	AC-17 (1)(2)(3)(4)
AC-18	Wireless Access	P1	AC-18	AC-18 (1)	AC-18 (1) (4)(5)
AC-19	Access Control for Mobile Devices	P1	AC-19	AC-19 (5)	AC-19 (5)
AC-20	Use of External Information Systems	P1	AC-20	AC-20 (1)(2)	AC-20 (1)(2)
AC-21	Information Sharing	P2	Not Selected	AC-21	AC-21
AC-22	Publicly Accessible Content	P3	AC-22	AC-22	AC-22
AC-23	Data Mining Protection	P0	Not Selected	Not Selected	Not Selected
AC-24	Access Control Decisions	P0	Not Selected	Not Selected	Not Selected
AC-25	Reference Monitor	P0	Not Selected	Not Selected	Not Selected

Control Number	Control Name	Priority	Initial Control Baselines		
			Low	Moderate	High
Awareness and Training					
AT-1	Security Awareness and Training Policy and Procedures	P1	AT-1	AT-1	AT-1
AT-2	Security Awareness Training	P1	AT-2	AT-2 (2)	AT-2 (2)
AT-3	Role-Based Security Training	P1	AT-3	AT-3	AT-3
AT-4	Security Training Records	P3	AT-4	AT-4	AT-4
AT-5	Withdrawn	--	--	--	--
Audit and Accountability					
AU-1	Audit and Accountability Policy and Procedures	P1	AU-1	AU-1	AU-1
AU-2	Audit Events	P1	AU-2	AU-2 (3)	AU-2 (3)
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 (1)(3)	AU-6 (1)(3)(5)(6)
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 (4)	AU-9 (2)(3)(4)
Audit and Accountability, concluded					
AU-10	Non-repudiation	P2	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)(3)
AU-13	Monitoring for Information Disclosure	P0	Not Selected	Not Selected	Not Selected
AU-14	Session Audit	P0	Not Selected	Not Selected	Not Selected
AU-15	Alternate Audit Capability	P0	Not Selected	Not Selected	Not Selected
AU-16	Cross-Organizational Auditing	P0	Not Selected	Not Selected	Not Selected
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	System Interconnections	P1	CA-3	CA-3 (5)	CA-3 (5)
CA-4	Withdrawn	---	---	---	---
CA-5	Plan of Action and Milestones	P3	CA-5	CA-5	CA-5

Control Number	Control Name	Priority	Initial Control Baselines		
			Low	Moderate	High
CA-6	Security Authorization	P2	CA-6	CA-6	CA-6
CA-7	Continuous Monitoring	P2	CA-7	CA-7 (1)	CA-7 (1)
CA-8	Penetration Testing	P2	Not Selected	Not Selected	CA_8
CA-9	Internal System Connections	P2	CA-9	CA-9	CA-9
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)(7)	CM-2 (1)(2)(3)(7)
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	CM-6 (1)(2)
CM-7	Least Functionality	P1	CM-7	CM-7 (1)(2)(4)	CM-7 (1)(2)(5)
CM-8	Information System Component Inventory	P1	CM-8	CM-8 (1)(3)(5)	CM-8 (1)(2)(3)(4)(5)
CM-9	Configuration Management Plan	P1	Not Selected	CM-9	CM-9
CM-10	Software Usage Restrictions	P2	CM-10	CM-10	CM-10
CM-11	User-Installed Software	P1	CM-11	CM-11	CM-11
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)(3)(8)	CP-2 (1)(2)(3)(4)(5)(8)
CP-3	Contingency Training	P2	CP-3	CP-3	CP-3 (1)
CP-4	Contingency Plan Testing	P2	CP-4	CP-4 (1)	CP-4 (1)(2)
CP-5	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)	CP-7 (1)(2)(3)(4)
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)(5)
CP-10	Information System Recovery and Reconstitution	P1	CP-10	CP-10 (2)	CP-10 (2)(4)
CP-11	Alternate Communications Protocols	P0	Not Selected	Not Selected	Not Selected

Control Number	Control Name	Priority	Initial Control Baselines		
			Low	Moderate	High
CP-12	Safe Mode	P0	Not Selected	Not Selected	Not Selected
CP-13	Alternative Security Mechanisms	P0	Not Selected	Not Selected	Not Selected
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)(12)	IA-2 (1)(2)(3)(8)(11)(12)	IA-2 (1)(2)(3)(4)(8)(9)(11)(12)
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)(11)	IA-5 (1)(2)(3)(11)	IA-5 (1)(2)(3)(11)
IA-6	Authenticator Feedback	P2	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 (1)(2)(3)(4)	IA-8 (1)(2)(3)(4)	IA-8 (1)(2)(3)(4)
IA-9	Service Identification and Authentication	P0	Not Selected	Not Selected	Not Selected
IA-10	Adaptive Identification and Authentication	P0	Not Selected	Not Selected	Not Selected
IA-11	Re-authentication	P0	Not Selected	Not Selected	Not Selected
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	P2	Not Selected	IR-3 (2)	IR-3 (2)
IR-4	Incident Handling	P1	IR-4	IR-4 (1)	IR-4 (1)(4)
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	P2	IR-7	IR-7 (1)	IR-7 (1)
IR-8	Incident Response Plan	P1	IR-8	IR-8	IR-8
IR-9	Information Spillage Response	P0	Not Selected	Not Selected	Not Selected
IR-10	Integrated Information Security Analysis Team	P0	Not Selected	Not Selected	Not Selected
Maintenance					
MA-1	System Maintenance Policy and Procedures	P1	MA-1	MA-1	MA-1

Control Number	Control Name	Priority	Initial Control Baselines		
			Low	Moderate	High
MA-2	Controlled Maintenance	P2	MA-2	MA-2	MA-2 (2)
MA-3	Maintenance Tools	P3	Not Selected	MA-3 (1)(2)	MA-3 (1)(2)(3)
MA-4	Non-Local Maintenance	P2	MA-4	MA-4 (2)	MA-4 (2)(3)
MA-5	Maintenance Personnel	P2	MA-5	MA-5	MA-5 (1)
MA-6	Timely Maintenance	P2	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	MP-2
MP-3	Media Marking	P2	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 (4)	MP-5 (4)
MP-6	Media Sanitization	P1	MP-6	MP-6	MP-6 (1)(2)(3)
MP-7	Media Use	P1	MP-7	MP-7 (1)	MP-7 (1)
MP-8	Media Downgrading	P0	Not Selected	Not Selected	Not Selected
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	P2	Not Selected	PE-5	PE-5
PE-6	Monitoring Physical Access	P1	PE-6	PE-6 (1)	PE-6 (1)(4)
PE-7	Withdrawn	--	--	--	--
PE-8	Visitor Access Records	P3	PE-8	PE-8	PE-8 (1)
PE-9	Power Equipment and 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 (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	P2	PE-16	PE-16	PE-16

Control Number	Control Name	Priority	Initial Control Baselines		
			Low	Moderate	High
PE-17	Alternate Work Site	P2	Not Selected	PE-17	PE-17
PE-18	Location of Information System Components	P3	Not Selected	Not Selected	PE-18
PE-19	Information Leakage	P0	Not Selected	Not Selected	Not Selected
PE-20	Asset Monitoring and Tracking	P0	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 (3)	PL-2 (3)
PL-3	Withdrawn	---	---	---	---
PL-4	Rules of Behavior	P2	PL-4	PL-4 (1)	PL-4 (1)
PL-5	Withdrawn	---	---	---	---
PL-6	Withdrawn	---	---	---	---
PL-7	Security Concept of Operations	P0	Not Selected	Not Selected	Not Selected
PL-8	Information Security Architecture	P1	Not Selected	PL-8	PL-8
PL-9	Central Management	P0	Not Selected	Not Selected	Not Selected
Program Management					
PM-1	Information Security Program Plan	P1	**Deployed VA-wide. Supporting information security program. Not associated with security control baselines. Independent of any system impact level.**		
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			
PM-12	Insider Threat Program	P1			
PM-13	Information Security Workforce	P1			
PM-14	Testing, Training, and Monitoring	P1			

Control Number	Control Name	Priority	Initial Control Baselines		
			Low	Moderate	High
PM-15	Contacts with Security Groups and Associations	P3			
PM-16	Threat Awareness Program	P1			
Personnel Security					
PS-1	Personnel Security Policy and Procedures	P1	PS-1	PS-1	PS-1
PS-2	Position Risk Designation	P1	PS-2	PS-2	PS-2
PS-3	Personnel Screening	P1	PS-3	PS-3	PS-3
PS-4	Personnel Termination	P1	PS-4	PS-4	PS-4 (2)
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	Withdrawn	---	---	---	---
RA-5	Vulnerability Scanning	P1	RA-5	RA-5 (1)(2)(5)	RA-5 (1)(2)(4) (5)
RA-6	Technical Surveillance Countermeasures Survey	P0	Not Selected	Not Selected	Not Selected
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	System Development Life Cycle	P1	SA-3	SA-3	SA-3
SA-4	Acquisition Process	P1	SA-4 (10)	SA-4 (1)(2)(9)(10)	SA-4 (1)(2)(9)(10)
SA-5	Information System Documentation	P2	SA-5	SA-5	SA-5
SA-6	Withdrawn	--	--	--	--
SA-7	Withdrawn	--	--	--	--
SA-8	Security Engineering Principles	P1	Not Selected	SA-8	SA-8
SA-9	External Information System Services	P1	SA-9	SA-9 (2)	SA-9 (2)

Control Number	Control Name	Priority	Initial Control Baselines		
			Low	Moderate	High
SA-10	Developer Configuration Management	P1	Not Selected	SA-10	SA-10
SA-11	Developer Security Testing and Evaluation	P1	Not Selected	SA-11	SA-11
SA-12	Supply Chain Protection	P1	Not Selected	Not Selected	SA-12
SA-13	Trustworthiness	P0	Not Selected	Not Selected	Not Selected
SA-14	Criticality Analysis	P0	Not Selected	Not Selected	Not Selected
SA-15	Development Process, Standards, and Tools	P2	Not Selected	Not Selected	SA-15
SA-16	Developer-Provided Training	P2	Not Selected	Not Selected	SA-16
SA-17	Developer Security Architecture and Design	P1	Not Selected	Not Selected	SA-17
SA-18	Tamper Resistance and Detection	P0	Not Selected	Not Selected	Not Selected
SA-19	Component Authenticity	P0	Not Selected	Not Selected	Not Selected
SA-20	Customized Development of Critical Components	P0	Not Selected	Not Selected	Not Selected
SA-21	Developer Screening	P0	Not Selected	Not Selected	Not Selected
SA-22	Unsupported System Components	P0	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 Availability	P0	Not Selected	Not Selected	Not Selected
SC-7	Boundary Protection	P1	SC-7	SC-7 (3)(4) (5)(7)	SC-7 (3)(4) (5) (7)(8)(18)(21)
SC-8	Transmission Confidentiality and Integrity	P1	Not Selected	SC-8 (1)	SC-8 (1)
SC-9	Withdrawn	--	--	--	--
SC-10	Network Disconnect	P2	Not Selected	SC-10	SC-10
SC-11	Trusted Path	P0	Not Selected	Not Selected	Not Selected
SC-12	Cryptographic Key Establishment and Management	P1	SC-12	SC-12	SC-12 (1)
SC-13	Cryptographic Protection	P1	SC-13	SC-13	SC-13

Control Number	Control Name	Priority	Initial Control Baselines		
			Low	Moderate	High
SC-14	Withdrawn)	--	--	--	--
SC-15	Collaborative Computing Devices	P1	SC-15	SC-15	SC-15
SC-16	Transmission of Security Attributes	P0	Not Selected	Not Selected	Not Selected
SC-17	Public Key Infrastructure Certificates	P1	Not Selected	SC-17	SC-17
SC-18	Mobile Code	P2	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	SC-20	SC-20
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	P1	SC-21	SC-21	SC-21
SC-22	Architecture and Provisioning for Name/Address Resolution Service	P1	SC-22	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	P0	Not Selected	Not Selected	Not Selected
SC-26	Honeypots	P0	Not Selected	Not Selected	Not Selected
SC-27	Platform-Independent Applications	P0	Not Selected	Not Selected	Not Selected
SC-28	Protection of Information at Rest	P1	Not Selected	SC-28	SC-28
SC-29	Heterogeneity	P0	Not Selected	Not Selected	Not Selected
SC-30	Concealment and Misdirection	P0	Not Selected	Not Selected	Not Selected
SC-31	Covert Channel Analysis	P0	Not Selected	Not Selected	Not Selected
SC-32	Information System Partitioning	P0	Not Selected	Not Selected	Not Selected
SC-33	Withdrawn	--	--	--	--
SC-34	Non-Modifiable Executable Programs	P0	Not Selected	Not Selected	Not Selected
SC-35	Honeyclients	P0	Not Selected	Not Selected	Not Selected
SC-36	Distributed Processing and Storage	P0	Not Selected	Not Selected	Not Selected
SC-37	Out-of-Band Channels	P0	Not Selected	Not Selected	Not Selected
SC-38	Operations Security	P0	Not Selected	Not Selected	Not Selected
SC-39	Process Isolation	P1	SC-39	SC-39	SC-39
SC-40	Wireless Link Protection	P0	Not Selected	Not Selected	Not Selected
SC-41	Port and I/O Device Access	P0	Not Selected	Not Selected	Not Selected

Control Number	Control Name	Priority	Initial Control Baselines		
			Low	Moderate	High
SC-42	Sensor Capability and Data	P0	Not Selected	Not Selected	Not Selected
SC-43	Usage Restrictions	P0	Not Selected	Not Selected	Not Selected
SC-44	Detonation Chambers	P0	Not Selected	Not Selected	Not Selected
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)	SI-3 (1)(2)
SI-4	Information System Monitoring	P1	SI-4	SI-4 (2)(4)(5)	SI-4 (2)(4)(5)
SI-5	Security Alerts, Advisories, and Directives	P1	SI-5	SI-5	SI-5 (1)
SI-6	Security Function Verification	P1	Not Selected	Not Selected	SI-6
SI-7	Software, Firmware, and Information Integrity	P1	Not Selected	SI-7 (1)(7)	SI-7 (1)(2)(5)(7)(14)
SI-8	Spam Protection	P2	Not Selected	SI-8 (1)(2)	SI-8 (1)(2)
SI-9	Withdrawn	--	--	--	--
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	Information Handling and Retention	P2	SI-12	SI-12	SI-12
SI-13	Predictable Failure Prevention	P0	Not Selected	Not Selected	Not Selected
SI-14	Non-Persistence	P0	Not Selected	Not Selected	Not Selected
SI-15	Information Output Filtering	P0	Not Selected	Not Selected	Not Selected
SI-16	Memory Protection	P1	Not Selected	SI-16	SI-16
SI-17	Fail-Safe Procedures	P0	Not Selected	Not Selected	Not Selected

4. SECURITY CONTROLS

The control tables located within each family in this next section are based on the current version of NIST SP 800-53 and provide specific controls outlined in Table 2: 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 (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Develops, documents, and disseminates to defined personnel or roles (See Attachment 2): 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the access control policy and associated access controls; and b. Reviews and updates the current: 1. Access control policy (See Attachment 2); and 2. Access control procedures (See Attachment 2).	X	X	X
Baseline allocation summary	AC-1	AC-1	AC-1

VA OI&T in this Appendix has outlined VA's system security controls based on the current version of NIST 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.

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

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Information System Owner, local CIO, or designee will**:** a. Identify and select types of information system accounts to support VA missions/business functions (See Attachment 2); b. Assign account managers for information system accounts; c. Establish conditions for group and role membership; d. Specify authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; e. Require approvals by designated organizational officials/positions for requests to create information system accounts (See Attachment 2); f. Create, enable, modify, disable, and remove information system accounts in accordance with VA procedures or conditions (See Attachment 2); g. Monitor the use of information system accounts; h. Notify account managers: 1. When accounts are no longer required; 2. When users are terminated or transferred; and 3. When individual information system usage or need-to-know changes. i. Authorize access to the information system based on: 1. A valid access authorization; 2. Intended system usage; and 3. Other attributes as required by VA or associated missions/business functions; j. Review accounts for compliance with account management requirements (See Attachment 2); and k. Establish a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.	X	X	X
(1) *Automated System Account Management:* OI&T employs automated mechanisms to support the management of information system accounts.	Not Selected	X	X
(2) *Removal of Temporary/Emergency Accounts:* OI&T ensures information systems automatically remove or disable temporary and emergency accounts after use is no longer required (See Attachment 2).	Not Selected	X	X
(3) *Disable Inactive Accounts:* OI&T ensures information systems automatically disable inactive accounts (See Attachment 2).	Not Selected	X	X
(4) *Automated Audit Actions:* OI&T employs automated mechanisms to audit account creation, modification, enabling, disabling, and removal actions and notifies	Not Selected	X	X

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
designated organizational officials/positions (See Attachment 3).			
(5) *Inactivity Logout:* VA requires that users log out when a time period of expected inactivity has occurred or describes when to log out (See Attachment 2).	Not Selected	Not Selected	X
(11) *Usage Conditions:* The information system enforces circumstances and/or usage conditions for information system accounts (See Attachment 3).	Not Selected	Not Selected	X
(12) *Account Monitoring/Atypical Usage*: OI&T monitors information system accounts for atypical use and reports atypical usage of information system accounts to designated organizational officials/positions (See Attachment 3).	Not Selected	Not Selected	X
(13) *Disable Accounts for High-Risk Individuals:* OI&T disables accounts of users posing a significant risk within a defined time period of discovery of the risk (See Attachment 2).	Not Selected	Not Selected	X
Baseline allocation summary	AC-2	AC-2 (1)(2)(3)(4)	AC-2 (1)(2)(3) (4)(5) (11) (12)(13)

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

(a) The Information System Owner, 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. 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.

(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 OI&T. Responsibility and authorization for the creation or modification of application menus and system access within the systems will be under the control of the Information System Owner, local CIO, or designee.

(d) The decision to provide access to the system is the responsibility of the Information System Owner. For hosted systems, the Information System Owner in conjunction with the Information Owner makes the decision to provide access.

(e) The ISO will perform regular audits of requests for VA systems access by users to ensure 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 and privacy awareness training, signed ROB, and background screening requirements).

(f) 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 email.

(g) Requests for access to remote systems must be approved by the user's supervisor and submitted to the ISO for processing.

(h) Requests for access by contractors will be submitted to the ISO from the CO or the COR to the ISO to verify the requirements to access VA's systems (security and privacy awareness training, signed ROB, and background screening requirements) have been met. Once the ISO has completed verification, the ISO will pass the request to the Information System Owner for further approval and processing. The CO or COR ensures the requests include the user's name, service, phone number, mail code and purpose of the access.

(i) In the event that temporary access is required (e.g., 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.

(j) 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.

(k) Account management is a process whereby the Information System Owner, local CIO, or designee manages and maintains system accounts throughout their life cycle. Local account management SOP(s) include:

1. Identification of account types (e.g.,. 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 time frames 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 time frame for the review and auditing of accounts (e.g., 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 information and system resources in accordance with applicable VA access control policies.	X	X	X
Baseline allocation summary	AC-3	AC-3	AC-3

OI&T 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 validated. Additional guidance is available in the current version of NIST SP 800-53.

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

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on information flow control policies (See Attachment 2).	Not Selected	X	X
Baseline allocation summary	Not Selected	AC-4	AC-4

(a) 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.

(b) Transferring information between information systems representing different security domains with different security policies introduces risk that such transfers violate one or more domain security policies. In such situations, Information Owners/Stewards provide guidance at designated policy enforcement points between interconnected systems.

(c) VA considers mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes, for example: (i) prohibiting information transfers between interconnected systems (i.e., allowing access only); (ii) employing hardware mechanisms to enforce one-way information flows; and (iii) implementing trustworthy regarding mechanisms to reassign security attributes and security labels.

(d) 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.

(e) 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
OI&T separates duties of individuals; documents separation of duties of individuals; and defines information system access authorizations to support separation of duties (See Attachment 3).	Not Selected	X	X
Baseline allocation summary	Not Selected	AC-5	AC-5

(a) Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Examples of separation of duties include: (i) dividing mission functions and information system support functions among different individuals/roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, network security); and (iii) ensuring security personnel administering access control functions do not administer audit functions.

(b) Users requiring elevated privileges to VA systems (privileged users) will follow OI&T's approved process. OI&T will employ automated mechanisms to manage this process. The requirements and approved process document is available on OIS' 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, a user with access rights or permissions that allows the user to access system control, monitoring, or administration functions on the IT system is considered a privileged user. 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 by appropriate senior management officials. OI&T 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) OI&T will conduct a quarterly review of elevated privilege accounts to determine whether elevated privileges are still required.

(j) 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.

(k) Some examples of the separation of duties 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 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
OI&T 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) *Authorize Access to Security Functions*: OI&T explicitly authorizes access to security functions and security-relevant information (See Attachment 3).	Not Selected	X	X

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
(1) *Non-Privileged Access for Non-Security Functions:* OI&T 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 (See Attachment 3).	Not Selected	X	X
(3) *Network Access to Privileged Commands:* OI&T authorizes network access to privileged commands only for compelling operational needs and documents the rationale for such access in the security plan for the information system (See Attachment 3).	Not Selected	Not Selected	X
(5) *Privileged Accounts:* OI&T restricts privileged accounts on the information system to designated officials/positions (See Attachment 2).	Not Selected	X	X
(9) *Auditing Use of Privileged Functions:* The information system audits execution of privileged functions.	Not Selected	X	X
(10) *Prohibit Non-Privileged Users from Executing Privileged Functions:* The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.	Not Selected	X	X
Baseline allocation summary	Not Selected	AC-6 (1)(2)(5) (9)(10)	AC-6 (1)(2)(3)(5) (9)(10)

(a) OI&T employs least privilege for specific duties and information systems. The concept of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required VA mission/business functions. OI&T considers the creation of additional processes, roles, and information system accounts as necessary to achieve least privilege. OI&T also applies least privilege to the development, implementation, and operation of VA information systems.

(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**.

(c) OI&T will audit the use of privileged functions as auditing is a key method for detecting behavior associated with insider threat and advanced persistent threat.

(7) AC-7: Unsuccessful Logon Attempts (P2)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system: a. Enforces a limit of consecutive invalid logon attempts by a user during a specified time period (See Attachment 3); and b. Automatically takes action when the maximum number of unsuccessful attempts is exceeded (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 regardless of whether the logon occurs via a local or network connection.

(c) Locked accounts with privileged access (e.g., 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
The information system: a. Displays to users a 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, directives, policies, regulations, standards, and guidance and states that (See Attachment 2): 1. Users are accessing a U.S. Government information system; 2. Information system usage may be monitored, recorded, and subject to audit; 3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and 4. Use of the information system indicates consent to monitoring and recording; b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and c. For publicly accessible systems: 1. Displays system use information conditions, before granting further access (See Attachment 2); 2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and 3. Includes a description of the authorized uses of the system.	X	X	X
Baseline allocation summary	AC-8	AC-8	AC-8

(a) The Information System Owner, local CIO, or designee will coordinate with the system managers, and other OI&T 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 notifications are used only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

(c) The Information System Owner, local CIO, or designee 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 (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system notifies the user, upon successful logon (access) to the system, 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 applicable to logons to information systems via human user interfaces and logons to systems that occur in other types of architectures (e.g., service-oriented architectures).

(b) VA does not require, at this time, application of **AC-9: Previous Logon (Access) Notification**. OI&T 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 (P3)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system limits the number of concurrent sessions for each account and/or account type 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 the Information System Owner, local CIO, or designee 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: a. Prevents further access to the system by initiating a session lock after a period of inactivity or upon receiving a request from a user (See Attachment 3); and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.	Not Selected	X	X
(1) *Pattern-Hiding Displays:* The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.	Not Selected	X	X
Baseline allocation summary	Not Selected	AC-11 (1)	AC-11 (1)

(a) A session lock is not a substitute for logging out of the information system when OI&T requires users to logout at the end of the workday.

(b) Publicly viewable images can include static or dynamic images, for example, patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen, with the additional caveat that none of the images convey sensitive information.

(12) **AC-12: Session Termination (P2)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system automatically terminates a user session after defined conditions or trigger events requiring session disconnect (See Attachment 3).	Not Selected	X	X
Baseline allocation summary	Not Selected	AC-12	AC-12

This control addresses the termination of user-initiated logical sessions in contrast to **SC-10: Network Disconnect** which addresses the termination of network connections that are associated with communications sessions (i.e., network disconnect). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses a VA information system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions. Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events requiring automatic session termination can include, for example, VA-defined periods of user inactivity, targeted responses to certain types of incidents, time-of-day restrictions on information system use.

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

Incorporated into **AC-2: Account Management** and **AU-6: Audit Review, Analysis, and Reporting**.

(14) **AC-14: Permitted Actions Without Identification or Authentication (P3)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Information System Owner: a. Identifies user actions that can be performed on the information system without identification or authentication consistent with VA missions/business functions (See Attachment 3); and b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication.	X	X	X
(1) [Withdrawn: Incorporated into AC-14]	---	---	---
Baseline allocation summary	AC-14	AC-14	AC-14

(a) This control addresses situations where an Information System Owner determines that no identification and authentication is required.

(b) Information System Owners may allow a limited number of user actions without identification and authentication including, for example, service accounts, site-to-site VPN accounts, training accounts in a test system, accessing public Web sites or other publicly accessible Federal information systems, using mobile phones to receive calls, or receiving a facsimile (fax).

(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 CIO 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 (e.g., 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 Information System Owner, local CIO, or designee. 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**

Incorporated into **MP-3: Media Marking** control.

(16) **AC-16: Security Attributes (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Provides the means to associate defined types of security attributes with information in storage, in process, and in transmission; b. Ensures that the security attribute associations are made and retained with the information; c. Establishes the permitted security attributes for information systems; and d. Determines the permitted values or ranges for each of the established security attributes.	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**. OI&T, 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
OI&T: a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorizes remote access to the information system prior to allowing such connections.	X	X	X
(1) *Automated Monitoring/Control:* The information system monitors and controls remote access methods.	Not Selected	X	X
(2) *Protection of Confidentiality/Integrity Using Encryption:* The information implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	Not Selected	X	X
(3) *Managed Access Control Points:* The information system routes all remote accesses through managed network access control points (See Attachment 2).	Not Selected	X	X
(4) *Privileged Commands/Access:* OI&T: a. Authorizes the execution of privileged commands and access to security-relevant information via remote access only for defined needs (See Attachment 3); and b. Documents the rationale for such access in the security plan for the information system.	Not Selected	X	X
(5) [Withdrawn: Incorporated into SI-4]	---	---	---
(7) [Withdrawn: Incorporated into AC-3 (10)]	---	---	---

(8) [Withdrawn: Incorporated into CM-7]	---	---	---
Baseline allocation summary	AC-17	AC-17 (1)(2)(3)(4)	AC-17 (1)(2)(3)(4)

(a) Remote access is 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). Remote access methods include, for example, dial-up, broadband, and wireless.

(b) The use of VPNs does not technically make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate security controls may provide sufficient assurance to VA that it can effectively treat such connections as internal networks. Still, VPN connections traverse external networks and the VPN does not enhance the availability of remote connections.

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

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

(e) Users can access VA systems from their residence or while they are on travel status using approved VA GFE or external information systems 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) Only VA-approved methods and technologies may be used to connect external systems to VA's network.

(g) VA prohibits access to VA's internal network from countries that pose a significant security risk unless prior authorization has been granted. Access from a restricted country for legitimate VA business purposes must be documented in a risk-based decision and be approved by the user's VA supervisor, ISO, local CIO, and/or Information System Owner.

(h) 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 Information System Owner, local CIO, or designee 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 OI&T 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.

(i) Users may transport, transmit, download, or store VA sensitive information on VA-owned or approved storage devices/media that are taken outside of VA facilities only when their VA supervisor, and local ISO, PO, and Information System Owner, local CIO, or designee approves it or it is documented and approved within a VA contract or agreement. The ISO and Information System Owner, local CIO, or designee will review and authorize the mechanisms for using, processing, transporting, transmitting, downloading, or storing VA sensitive data outside of VA owned or managed facilities. 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.

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

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

(l) 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.

(m) 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.

(n) 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.

(o) OI&T 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.

(p) 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 approval of a higher level official or supervisor within the user's facility. The request will then be reviewed and approved by the Information System Owner, local CIO, or designee. 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.

(q) New users (those who do not have a current VA network account) who request remote access must complete VA-approved security and privacy 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.

(r) Requests for remote access by contractors will be submitted to the ISO by the CO or the COR or VA 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. The request will then be reviewed and approved by the Information System Owner, local CIO, or designee. 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 OIS Portal.

(s) 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.

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

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

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Establishes usage restrictions, configurations/connection requirements, and implementation guidance for wireless access; and b. Authorizes wireless access to the information system prior to allowing such connections.	X	X	X
(1) *Authentication and Encryption:* The information system protects wireless access to the system using authentication of users and/or devices and FIPS 140-2 (or its successor) validated encryption (See Attachment 3).	Not Selected	X	X
(2) [Withdrawn: Incorporated into SI-4]	---	---	---
(4) *Restrict Configuration by Users:* OI&T identifies and explicitly authorizes users to independently configure wireless networking capabilities.	Not Selected	Not Selected	X

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
(5) *Antennas/Transmission Power Levels:* OI&T selects radio antennas and calibrates transmission power levels to reduce the probability that usable signals can be received outside of VA-controlled boundaries.	Not Selected	Not Selected	X
Baseline allocation summary	AC-18	AC-18 (1)	AC-18 (1)(4) (5)

(a) Wireless technologies include, for example, microwave, satellite, packet radio (ultra-high frequency/very high frequency), 802.11x, and Bluetooth.

(b) Actions that may be taken by Operating Units to limit unauthorized use of wireless communications outside of VA-controlled boundaries include:

1. Reducing the power of the wireless transmission so that the transmissions are less likely to emit a signal that can be used by adversaries outside of the physical perimeter of the facility;

2. Employing measures such as Transient Electromagnetic Pulse Standard Pulse Standard (TEMPEST) to control wireless emanations; and

3. Using directional/beam forming antennas that reduce the likelihood that unintended receivers will be able to intercept signals.

(c) Prior to taking such actions, OI&T can conduct periodic wireless surveys to understand the radio frequency profile of VA information systems as well as other systems that may be operating in the area.

(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 OI&T.

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

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for VA-controlled mobile devices; and b. Authorizes the connection of mobile devices to VA information systems.	X	X	X
(1) [Withdrawn: Incorporated into MP-7]	---	---	---

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
(2) [Withdrawn: Incorporated into MP-7]	---	---	---
(3) [Withdrawn: Incorporated into MP-7]	---	---	---
(5) *Full-Device/Container-Based Encryption:* OI&T employs full-device encryption or container encryption to protect the confidentiality and integrity of information on mobile devices (See Attachment 2).	Not Selected	X	X
Baseline allocation summary	AC-19	AC-19 (5)	AC-19 (5)

(a) A mobile device is a computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable data storage; and (iv) includes a self-contained power source.

(b) Mobile devices may also include voice communication capabilities, on-board sensors that allow the device to capture (e.g., photograph, video, record, or determine location) information, and/or built-in features for synchronizing local data with remote locations. Examples include smartphones, E-readers, and tablets. In addition, other portable computing and communications devices with information storage capability, such as smartphones, digital cameras, and audio recording devices, will be subject to the same requirements as mobile devices. Portable storage devices are addressed in (e) below.

(c) Mobile devices are typically associated with a single individual and the device is usually in close proximity to the individual; however, the degree of proximity can vary depending upon the form factor/size of the device. The processing, storage, and transmission capability of the mobile device may be comparable to or merely a subset of desktop systems, depending upon the nature and intended use of the device.

(d) All mobile devices that store/transmit VA data must be GFE, and must be included in VA's Technical Reference Model (TRM). All applications developed and used must store and transmit data using a FIPS 140-2 (or its successor) validated application (or the application data resides in a container-based encryption solution), and must be listed in VA's TRM. FIPS 140-2 is required for data at rest and data in transit when it contains PII/PHI/sensitive information. There are two methods for this. Either the device itself must provide full-device encryption for all storage and have a protected connection back to VA or the application must be "wrapped" by a FIPS 140-2 validated solution. This would protect the information on a device that does not have data protected any other way. The storage and data in transit must be protected with FIPS 140-2 (or its successor) validated encryption.

(e) Portable storage devices are information system components that can be inserted into and removed from an information system, and that is used to store data or information (e.g., text, video, audio, and/or image data). Examples include floppy disks, CDs/DVDs, USB flash drives, external hard disk drives, and flash memory cards or drives that contain non-volatile memory.

(f) The Information System Owner, local CIO, or designee and supervisors must authorize the use of portable storage, mobile, and wireless devices within their Operating Unit prior to their implementation. The Information System Owner, local CIO, or designee will make the determination based on current VA policy and OI&T SOPs and guidance. See AC-20 (j) for use of personally-owned devices.

(g) All VA employees must have documented permission from their supervisor to store VA sensitive information on a mobile or portable storage device. The ISO and Information System Owner, local CIO, or designee must approve and document that the mobile or portable storage device to be used meets VA's security requirements.

(h) 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.

(i) Portable storage devices should be tested and approved by the TRM Workgroup and must use FIPS 140-2 (or its successor) validated encryption in FIPS mode per the validated security policy found on the NIST CMVP website. If critical security parameters (CSP) are stored on the device then Security Level 3 is required to detect and address tampering. The Information System Owner, local CIO, or designee and ISO may accept the risk of using Security Level 1 or Security Level 2, if other mitigating controls, such as permanently installed physical security measures, are in place prohibiting access to the device. If no CSPs are stored on the device, all sensitive data is encrypted, and decryption keys are not attachable or storable on the device, Security Level 1 or Security Level 2 is sufficient.

(j) Similarly, portable 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 OI&T management for applicable VA-approved tools for encrypting CDs/DVDs. 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 below 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.

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

(l) Non-VA personnel (e.g., contractors, business partners) must furnish their own FIPS 140-2 (or its successor) validated USB flash drives that conform to the published listing of VA-approved USB flash drives. Further, permission must be obtained from a designated VA supervisor and Information System Owner, local CIO, or designee before they can be utilized within the Department.

(m) 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 Medical Device Laptop or Biomedical Engineering Service Laptop to be used as required, Biomedical Engineering staff and VISN Biomedical Engineer (or VISN Biomedical Engineering Point of Contact) must create a Risk Based Decision (RBD) Memo to document the mitigating actions taken to protect the data. This RBD memo will be reviewed and approved by the Chief Biomedical Engineer, Facility Information Security Officer, and Medical Center Director. Once completed the RBD will be forwarded to the Office of Healthcare Technology Management (HTM), Health Information Security Division (HIS), and DAS for OIS, for review and approval. Approved laptop RBDs will be documented and maintained by HTM with a copy provided to HISD and the local ISO. Any laptops other than Medical Device Laptops or Biomedical Engineering Service Laptops that cannot be encrypted must have documented local ISO and CIO approval, as well the DAS for OIS.

(n) Portable storage 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).

(o) Mobile, portable storage, and wireless devices used for the processing and storage of VA information will follow VA policy regarding system hardware and electronic media sanitization and disposal.

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

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T 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: a. Access the VA information system from the external information systems; and b. Process, store, and transmit VA-owned information using the external information systems.	X	X	X
(1) *Limits on Authorized Use:* OI&T permits authorized individuals to use an external information system to access VA's information systems or to process, store, or transmit VA information only when OI&T: a. Verifies the implementation of required security controls on the external system as specified in the VA information security policy and security plan; or b. Retains approved information system connection or processing agreements with the organization hosting the external information system.	Not Selected	X	X
(2) *Portable Storage Devices:* OI&T restricts or prohibits the use of VA-controlled portable storage devices by authorized individuals on external information systems (See Attachment 2).	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 information. These individuals have completed the security requirements for access to VA systems or VA 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, smartphones, tablets, or PDAs);

2. Privately-owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, shopping malls, 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 documents (e.g., other Federal agency). The DAS for Information Security or designee will review these documents. Other VA developed and approved processes for verification will be 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 information must be documented in a MOU/ISA, contract or other agreement (e.g., Data Use Agreement) as specified in the procedures or templates provided for each of these types of agreements. See VA Directive 6513, *Secure External Connections,* VA Handbook 6500.6, *Contract Security*, and VHA Handbook 1080.01, *Data Use Agreements* for VHA Data Use Agreements. 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 Information System Owners, local CIOs, or designees 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) Information System owners, local CIOs, or designees 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) External information systems 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) may not be used on-site at a VA facility to directly connect to VA's network. Use of personally-owned information systems on-site to perform assigned official duties must be approved by the Information System Owner, local CIO, or designee.

(21) **AC-21: Information Sharing (P2)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
VA: a. 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 information-sharing circumstances where user discretion is required (See Attachment 2); and b. Employs automated mechanisms or manual processes to assist users in making information-sharing/collaboration decisions (See Attachment 2).	Not Selected	X	X
Baseline allocation summary	Not Selected	AC-21	AC-21

This control applies to information that may be restricted in some manner (e.g., privileged medical information, contract-sensitive information, proprietary information, PII, classified information related to special access programs or compartments) based on some formal or administrative determination. Depending on the particular information-sharing circumstances, sharing partners may be defined at the individual, group, or organizational level. Information may be defined by content, type, security category, or special access program/compartment.

(22) **AC-22: Publicly Accessible Content (P3)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
VA: a. Designates individuals authorized to post information onto a publicly accessible VA information system; b. Trains authorized individuals to ensure that publicly accessible information does not contain non-public information; c. Reviews the proposed content of information prior to posting onto the publicly accessible VA information system to ensure that non-public information is not included; and d. Reviews the content on the publicly accessible VA information system for non-public information and removes such information, if discovered (See Attachment 3).	X	X	X
Baseline allocation summary	AC-22	AC-22	AC-22

In accordance with Federal laws, Executive Orders, directives, policies, regulations, standards, or guidance the general public is not authorized access to non-public information (e.g.,

information protected under the Privacy Act and proprietary information). This control addresses information systems that are controlled by VA and accessible to the general public, typically without identification or authentication.

(23) **AC-23: Data Mining Protection (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
VA employs data mining prevention and detection techniques for data storage objects to adequately detect and protect against data mining.	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-23: Data Mining Protection**. OI&T, may, at their discretion, elect to ensure that information systems appropriately support and maintain data mining protection.

(24) **AC-24: Access Control Decisions (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
VA establishes procedures to ensure access control decisions are applied to each access request prior to access enforcement.	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-24: Access Control Decisions**. OI&T, may, at their discretion, elect to ensure that information systems appropriately support and maintain access control decisions.

(25) **AC-25: Reference Monitor (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system implements a reference monitor for access control policies that is tamperproof, always invoked, and small enough to be subject to analysis and testing, the completeness of which can be assured.	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-25: Reference Monitor**. OI&T, may, at their discretion, elect to ensure that information systems appropriately support and maintain a reference monitor.

b. Awareness and Training (AT)

(1) AT-1: Security Awareness and Training Policy and Procedures (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Develops, documents, and disseminates to defined personnel or roles (See Attachment 2): 1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and b. Reviews and updates the current: 1. Security awareness and training policy (See Attachment 2); and 2. Security awareness and training procedures (See Attachment 2).	X	X	X
Baseline allocation summary	AT-1	AT-1	AT-1

VA OI&T 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.

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

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T provides basic security awareness training to all information system users (including managers, senior executives, and contractors): a. As part of initial training for new users; b. When required by information system changes; and c. At a defined frequency thereafter (See Attachment 2).	X	X	X
(2) *Insider Threat:* OI&T includes security awareness training on recognizing and reporting potential indicators of insider threat.	Not Selected	X	X
Baseline allocation summary	AT-2	AT-2 (2)	AT-2 (2)

(a) VA requires that in addition to users of VA information systems outlined above, users of VA information must also complete VA-approved security and privacy awareness training annually (within a 365 day period from the date of the last completion of VA's approved security and privacy awareness training). Users of VA information systems or VA information will receive VA-approved security and privacy awareness training as part of initial training for new users, when required by system changes, and annually thereafter.

(b) VA determines the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and information systems. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security.

(c) Failure to complete VA-approved security and privacy awareness training may result in suspension or termination of access. Lack of access may lead to personnel action if access is required for fulfillment of position responsibilities. To prevent disruption of VA mission/business processes, VA facilities will develop procedures to ensure the prompt restoration of access upon completion of the security and privacy awareness training and in emergency situations.

(d) VA OI&T management has approved security and privacy awareness training reciprocity for other Federal agency employees. OI&T management will accept annual FISMA compliant training provided to other Federal government agency employees by their own agency in lieu of VA's approved security and privacy awareness training. Employees of other Federal agencies are required to sign the VA ROB prior to being provided access to VA's information systems or VA sensitive information.

(e) If, however, the other Federal government agency employee makes and/or causes an unauthorized disclosure, this employee will be required to complete VA's security and privacy awareness training, including re-signing the VA ROB, in addition to the annual privacy and information security training already received by the employee at his/her own agency, as part of incident remediation measures. Access will be suspended until the training has been completed and certification of completion has been submitted to the VA requesting official. Refer to the OI&T Training Reciprocity SOP for further information regarding incident remediation.

(3) **AT-3: Role-Based Security Training (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T provides role-based security training to personnel with assigned security roles and responsibilities: a. Before authorizing access to the information system or performing assigned duties; b. When required by information system changes; and c. At a defined frequency thereafter (See Attachment 2).	X	X	X
Baseline allocation summary	AT-3	AT-3	AT-3

(a) Information Technology Workforce Development (ITWD) has developed IT competency modeling for the OI&T workforce. Information Assurance is a core competency across all of the OI&T competency models (which include the mandatory VA security and privacy awareness and Rules of Behavior course for all VA employees and ongoing training through such security-focused initiatives 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, and Database Administrators) competency profiles and role-based training for "those with significant responsibilities" is incorporated.

(b) ITWD has developed additional Information Security Role-Based training for other positions within the Department which is available in the Talent Management System (TMS). Training shall be assigned to personnel based on Manager/Supervisor/COR discretion as the cyber security duties of the position change.

(4) AT-4: Security Training Records (P3)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
VA and OI&T: a. Document and monitor individual information system security training activities including basic security awareness training and specific information system security training; and b. Retain individual training records for a defined time period (See Attachment 2).	X	X	X
Baseline allocation summary	AT-4	AT-4	AT-4

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

Incorporated into **PM-15: Contacts with Security Groups and Associations** control.

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

(1) **AU-1: Audit and Accountability Policy and Procedures (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Develops, documents, and disseminates to defined personnel or roles (See Attachment 2): 1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and b. Reviews and updates the current: 1. Audit and accountability policy (See Attachment 2); and 2. Audit and accountability procedures (See Attachment 2).	X	X	X
Baseline allocation summary	AU-1	AU-1	AU-1

VA OI&T 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.

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

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Determines that the information system must be capable of auditing events as defined by the Information System Owner (See Attachment 3); b. 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; c. 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	X	X	X

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
d. Determines which events are to be audited within the information system including the frequency for each event (See Attachment 3).			
(3) *Reviews and Updates:* OI&T reviews and updates the audited events (See Attachment 3).	Not Selected	X	X
(4) [Withdrawn: Incorporated into AC-6(9)]	---	---	---
Baseline allocation summary	AU-2	AU-2 (3)	AU-2 (3)

(a) OI&T 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.

(b) OI&T shall include auditable events that are required by applicable Federal laws, Executive Orders, directives, policies, regulations, and standards.

(c) The list of events to be audited must be reviewed periodically, as necessary, to ensure that it is still sufficient and that there is still a need to audit the events.

(3) **AU-3: Content of Audit Records (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.	X	X	X
(1) *Additional Audit Information:* The information system generates audit records containing additional, more detailed information (See Attachment 3).	Not Selected	X	X
(2) *Centralized Management of Planned Audit Record Content:* The information system provides centralized management and configuration of the content to be captured in 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 Information System Owner allocates audit record storage capacity in accordance with audit record storage requirements (See Attachment 3).	X	X	X
Baseline allocation summary	AU-4	AU-4	AU-4

The Information System Owner considers the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity. Allocating sufficient audit storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of auditing capability.

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

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system: a. Alerts designated organizational officials/positions in the event of an audit processing failure (See Attachment 3); and b. Takes additional actions in the event of an audit processing failure (See Attachment 3):	X	X	X
(1) *Audit Storage Capacity:* The information system provides a warning to designated organizational officials/positions within a time period when allocated audit record storage volume reaches a percentage of repository maximum audit record storage capacity (See Attachment 3).	Not Selected	Not Selected	X
(2) *Real-Time Alerts:* The information system provides an alert in a defined time period to designated organizational officials/positions/locations when defined audit failure events requiring real-time alerts occur (See Attachment 3).	Not Selected	Not Selected	X
Baseline allocation summary	AU-5	AU-5	AU-5 (1)(2)

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

(b) This control applies to each audit data storage capacity (i.e., distinct information where system components audit records are stored), the total audit storage capacity of OI&T (i.e., all audit data storage repositories combined), or both.

(c) Multiple audit data storage repositories distributed across multiple information system components may each have different storage volume capacities.

(d) Alerts provide OI&T with urgent messages. Real-time alerts provide these messages at IT speed (i.e., the time from event detection to alert occurs in seconds or less).

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

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T reviews and analyzes information system audit records for indications of inappropriate or unusual activity, and reports findings to designated organizational officials/positions (See Attachment 3).	X	X	X
(1) *Process Integration:* OI&T employs automated mechanisms to integrate audit review, analysis, and reporting processes to support VA's processes for investigation and response to suspicious activities.	Not Selected	X	X

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
(3) *Correlate Audit Repositories*: OI&T analyzes and correlates audit records across different repositories to gain VA-wide situational awareness.	Not Selected	X	X
(5) *Integration/Scanning and Monitoring Capabilities*: OI&T integrates analysis of audit records with analysis of (one or more): vulnerability scanning information; performance data; information system monitoring information; organization-defined data/information collected from other sources to further enhance the ability to identify inappropriate or unusual activity (See Attachment 3).	Not Selected	Not Selected	X
(6) *Correlation with Physical Monitoring:* OI&T correlates information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.	Not Selected	Not Selected	X
Baseline allocation summary	AU-6	AU-6 (1)(3)	AU-6 (1)(3)(5)(6)

(a) Audit review, analysis, and reporting covers information security-related auditing performed by OI&T including, for example, auditing that results from monitoring of account usage, remote access, wireless connectivity, mobile or portable storage device connection, configuration settings, system component inventory, use of maintenance tools and non-local maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the information system boundaries, use of mobile code, and use of Voice over Internet Protocol (VoIP).

(b) Integration/Scanning and Monitoring Capabilities does not require vulnerability scanning, the generation of performance data, or information system monitoring. Rather, it requires that the analysis of information being otherwise produced in these areas is integrated with the analysis of audit information.

(c) Correlation with Physical Monitoring will assist VA in identifying suspicious behavior and in producing supporting evidence to substantiate it.

(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 that: a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and b. Does not alter original content or time ordering of audit	Not Selected	X	X

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
records.			
(1) *Automatic Processing*: The information system provides the capability to process audit records for events of interest based on defined audit fields within audit records (See Attachment 3).	Not Selected	X	X
Baseline allocation summary	Not Selected	AU-7 (1)	AU-7 (1)

(a) Audit reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analysts. Audit reduction and report generation capabilities do not always emanate from the same information system or from the same OI&T entities conducting auditing activities. Audit reduction capability can include, for example, modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. The report generation capability provided by the information system can generate customizable reports.

(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: a. Uses internal system clocks to generate time stamps for audit records; and b. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets a defined granularity of time measurement (See Attachment 3).	X	X	X
(1) *Synchronization with Authoritative Time Source:* The information system: a. Compares the internal information system clocks with a defined authoritative time source (See Attachment 3); and b. Synchronizes the internal information system clocks to the authoritative time source when the time difference is greater than a defined time period (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
(2) *Audit Backup on Separate Physical Systems/Components:* The information system backs up audit records onto a physically different system or system component than the system or component being audited (See Attachment 3).	Not Selected	Not Selected	X
(3) *Cryptographic Protection:* The information system implements cryptographic mechanisms to protect the integrity of audit information and audit tools.	Not Selected	Not Selected	X
(4) A*ccess by Subset of Privileged Users:* OI&T authorizes access to management of audit functionality to only a subset of privileged users (See Attachment 3).	Not Selected	X	X
Baseline allocation summary	AU-9	AU-9 (4)	AU-9 (2)(3)(4)

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

(b) This control focuses on technical protection of audit information.

(c) Cryptographic mechanisms used for protecting the integrity of audit information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

(d) Individuals with privileged access to an information system and who are also the subject of an audit by that system, may affect the reliability of audit information by inhibiting audit activities or modifying audit records.

(e) *Access by Subset of Privileged Users*, requires that privileged access be further defined between audit-related privileges and other privileges, thus limiting the users with audit-related privileges.

(10) **AU-10: Non-Repudiation (P2)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed actions to be covered by non-repudiation (See Attachment 3).	Not Selected	Not Selected	X
Baseline allocation summary	Not Selected	Not Selected	AU-10

Types of individual actions covered by non-repudiation include, for example, creating information, sending and receiving messages, and approving information (e.g., indicating concurrence or signing a contract). 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 email, 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
OI&T retains audit records to provide support for after-the-fact investigations of security incidents and to meet regulatory and VA 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 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: a. Provides audit record generation capability for the auditable events defined in **AU-2: Auditable Events** at information system components (See Attachment 3); b. Allows designated organizational officials/positions to select which auditable events are to be audited by specific components of the information system (See Attachment 3); and c. Generates audit records for the events defined in **AU-2: Auditable Events** with the content as defined in **AU-3: Content of Audit Records**.	X	X	X
(1) *System-Wide/Time Correlated Audit Trail:* 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 (See Attachment 3).	Not Selected	Not Selected	X
(3) *Changes by Authorized Individuals:* The information system provides the capability for designated organizational officials/positions to change the auditing to be performed on information system components based on selectable event criteria within time thresholds (See Attachment 3).	Not Selected	Not Selected	X
Baseline allocation summary	AU-12	AU-12	AU-12 (1)(3)

(a) Audit records can be generated from many different information system components. The events audited are typically a subset 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 (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T monitors open source information and/or information sites 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**. OI&T may, at their discretion, elect to monitor for information disclosure.

(14) **AU-14: Session Audit (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system provides the capability for authorized users to select a user session to capture/record or view/hear.	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**. OI&T may, at their discretion, elect to conduct session audits.

(15) **AU-15: Alternate Audit Capability (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T provides an alternate audit capability in the event of a failure in primary audit capability that provides alternate audit functionality.	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-15: Alternate Audit Capability**. OI&T may, at their discretion, elect to alternate audit capabilities.

(16) **AU-16: Cross-Organizational Auditing (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T employs methods for coordinating audit information among external organizations when audit information is transmitted across VA boundaries.	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-16: Cross-Organizational Auditing**. OI&T may, at their discretion, elect to employ cross-organizational auditing.

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

(1) **CA-1: Security Assessment and Authorization Policies and Procedures (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Develops, documents, and disseminates to defined personnel or roles (See Attachment 2): 1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and b. Reviews and updates the current: 1. Security assessment and authorization policy (See Attachment 2); and 2. Security assessment and authorization procedures (See Attachment 2).	X	X	X
Baseline allocation summary	CA-1	CA-1	CA-1

VA OI&T in this Appendix has outlined VA's system security controls based on the current version of NIST 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.

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

NIST SP 800-53	(3) APPLICABILITY		
	LOW	**MODERATE**	**HIGH**
OI&T: a. Develops a security assessment plan that describes the scope of the assessment including: 1. Security controls and control enhancements under assessment; 2. Assessment procedures to be used to determine security control effectiveness; and 3. Assessment environment, assessment team, assessment roles and responsibilities. b. Assesses the security controls in the information system and its environment of operation to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the established security requirements (See Attachment 2); c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the SCA to designated organizational officials/positions (See Attachment 2).	X	X	X
(1) *Independent Assessors:* OI&T employs independent assessors or assessment teams with an organization-defined level of independence to conduct SCAs (See Attachment 2).	Not Selected	X	X
(2) *Specialized Assessments:* OI&T 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)

(a) VA Handbook 6500.3 contains additional information on the A&A process used by VA.

(b) Assessments may also check non-security functions to ensure that they do not contain security vulnerabilities.

(3) **CA-3: System Interconnections (P1)**

NIST SP 800-53	(4) APPLICABILITY		
	(5) LOW	(6) MODERATE	(7) HIGH

OI&T: a. Authorizes connections from the information system to other information systems through the use of ISAs; b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and c. Reviews and updates ISAs (See Attachment 2).	X	X	X
(5) *Restrictions on External Network Connections:* OI&T employs policy for allowing information systems to connect to external information systems (See Attachment 2).	Not Selected	X	X
Baseline allocation summary	CA-3	CA-3 (5)	CA-3 (5)

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

(b) The Information 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. The VA CIO is the AO for all VA systems. Rather than using an ISA, the interface characteristics between the interconnecting information systems are described in the security plans for the respective systems.

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

(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/ISA will be obtained prior to connection with other systems and/or sharing of the information. The Information System Owner, local CIO, or designee and the ISO, in coordination and agreement with the Enterprise Security Change Control Board, approve ISAs. MOU and ISA templates are available on the OIS portal.

(f) For contractor systems, the MOU/ISA, if required, are 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**

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
OI&T: a. 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 b. Updates existing POA&M 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 Information System Owner must track all POA&M activity within the VA-approved FISMA database and coordinate completion with appropriate VA parties.

(b) The 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, OI&T's OCS 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); and

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 (P2)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
VA: a. Assigns a senior-level executive or manager to the role of AO for the information system; b. Ensures that the AO authorizes the information system for processing before commencing operations; and c. 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 NIST SP 800-37. VA Handbook 6500.3 contains additional information on A&A within VA.

(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 (P2)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishing metrics to be monitored (See Attachment 2); b. Establishing frequencies for monitoring and for assessments supporting such monitoring (See Attachment 2); c. Ongoing SCAs in accordance with VA's continuous monitoring strategy; and d. Ongoing security status monitoring of organization-defined metrics in accordance with VA's continuous monitoring strategy; e. Correlation and analysis of security-related information generated by assessments and monitoring;	X	X	X

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
f. Response actions to address results of the analysis of security-related information; and g. Reporting the security status of VA and the information system to the designated organizational officials/positions (See Attachment 2).			
(1) *Independent Assessment:* OI&T employs assessors or assessment teams to monitor the security controls in the information system on an ongoing basis (See Attachment 2).	Not Selected	X	X
Baseline allocation summary	CA-7	CA-7 (1)	CA-7 (1)

(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 collects, stores, and continuously reports information on the Department's assessments using a VA-approved FISMA database.

(f) The tools and means of conducting self-assessments may include scans, and any other automated tool identified by OI&T that offers a defined value in ensuring security control compliance.

(8) **CA-8: Penetration Testing (P2)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T conducts penetration testing on information systems or system components (See Attachment 2).	Not Selected	Not Selected	X
Baseline allocation summary	Not Selected	Not Selected	CA-8

(a) A standard method for penetration testing includes, for example: (i) pretest analysis based on full knowledge of the target system; (ii) pretest identification of potential

vulnerabilities based on pretest analysis; and (iii) testing designed to determine exploitability of identified vulnerabilities.

(b) OI&T correlates the penetration testing rules of engagement with the tools, techniques, and procedures that are anticipated to be employed by adversaries carrying out attacks. OI&T risk assessments guide decisions on the level of independence required for personnel conducting penetration testing.

(9) **CA-9: Internal System Connections (P2)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Authorizes internal connections of information system components or classes of components to the information system (See Attachment 2); and b. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.	X	X	X
Baseline allocation summary	CA-9	CA-9	CA-9

(a) This control applies to connections between OI&T systems and (separate) constituent system components (i.e., intra-system connections) including, for example, system connections with mobile or portable storage devices, printers, copiers, fax machines, scanners, and sensors.

(b) Instead of authorizing each individual internal connection, OI&T can authorize internal connections for a class of components with common characteristics and/or configurations, for example, all digital printers, scanners, and copiers with a specified processing, storage, and transmission capability or all smartphones with a specific baseline configuration.

e. Configuration Management (CM)

(1) CM-1: Configuration Management Policy and Procedures (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Develops, documents, and disseminates to defined personnel or roles (See Attachment 2): 1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and b. Reviews and updates the current: 1. Configuration management policy (See Attachment 2); and 2. Configuration management procedures (See Attachment 2).	X	X	X
Baseline allocation summary	CM-1	CM-1	CM-1

VA OI&T in this Appendix has outlined VA's system security controls based on the current version of NIST 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.

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

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	X	X	X
(1) *Reviews and Updates:* The Information 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) *Automation Support for Accuracy/Currency:* OI&T employs automated mechanisms to maintain an up-to-	Not Selected	Not Selected	X

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
date, complete, accurate, and readily available baseline configuration of the information system.			
(3) *Retention of Previous Configurations:* OI&T retains previous versions of baseline configurations of the information system to support rollback (See Attachment 3).	Not Selected	X	X
(4) [Withdrawn: Incorporated into CM-7]	---	---	---
(5) [Withdrawn: Incorporated into CM-7]	---	---	---
(7) *Configure Systems, Components, or Devices for High-Risk Areas:* OI&T: a. Issues information systems, system components, or devices with organization-defined configurations to individuals traveling to locations that OI&T deems to be of a significant risk (See Attachment 2); and b. Applies security safeguards to the devices when the individuals return (See Attachment 2).	Not Selected	X	X
Baseline allocation summary	CM-2	CM-2 (1)(3)(7)	CM-2 (1)(2)(3)(7)

(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) OI&T will develop, implement, and approve system security baseline configurations for all VA platforms and systems leveraging existing standards and best practices, where available, and tailored specifically for the VA environment. All standard, non-standard, custom-developed, and single instance platforms and applications are required to have an established baseline configuration from which to measure compliance and to assist OCS and VA with determining the overall security posture of the system. Baselines must adhere to standards set by FDCC, USGCB, and DISA STIG. In cases where standards, guidance, or best practices do not exist to assist with developing a secure baseline configuration, Service Delivery and Engineering will collaborate with OIS to develop, test, and implement an agreed-upon baseline.

(c) For systems that cannot meet the approved system security baseline configuration because of specific mission requirements, an OIS RBD is required. (See the Policy Section on the OCS Portal for information on the OIS RBD process.)

(d) Maintaining the baseline configuration involves creating new baselines as the information system changes over time. Changes to approved system security baseline configurations will be managed using a centralized change management process.

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

(f) OI&T will monitor VA's approved USGCB configuration on applicable VA systems regularly using a NIST validated Security Content Automation Protocol tool.

(g) Automated mechanisms employed for maintaining baseline configurations may include hardware and software inventory tools, configuration management tools, and network management tools. Such tools can be deployed or allocated as common controls, at the information system level, or at the operating system or component level (e.g., on workstations, servers, network components, mobile devices) and can be used to track operating system version numbers on operating system applications, types of software installed, and current patch levels.

(h) For all local VA systems located at a VA facility, the local CIO will establish standards, based on Federal requirements and VA security policies, for operating the system at the VA facility. The standards will be documented and agreed to by the local CIO and the business owner of the system. The local CIO will enforce compliance with the established standards and will remove non-compliant systems from use at a VA facility. The DAS for OIS and Deputy CIO for Service Delivery and Engineering must approve local systems that cannot meet this requirement.

(i) When it is known that information systems, system components, or devices (e.g., computers, mobile or portable storage devices) will be located in high-risk areas, additional security controls shall be implemented to counter the greater threat in such areas coupled with the lack of physical security relative to OI&T-controlled areas.

(j) For VA staff required to travel outside the US for VA business, OI&T must provide them the necessary mobile or portable storage 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;

4. Are encrypted with FIPS 140-2 (or its successor) validated encryption; and

5. Are assessed by OI&T for any anomalies.

(k) No VA mobile or portable storage devices may be taken outside of the US except those provided by OI&T specifically for the purposes of travel outside of the US.

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

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Determines the types of changes to the information system that are configuration-controlled; b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses; c. Documents configuration change decisions associated with the information system; d. Implements approved configuration-controlled changes to the system; e. Retains records of configuration-controlled changes to the information system (See Attachment 2); f. Audits and reviews activities associated with configuration-controlled changes to the information system; and g. Coordinates and provides oversight for configuration change control activities through configuration change control element (e.g., committee, board) that convenes on assigned schedule (See Attachment 2).	Not Selected	X	X
(1) *Automated Document/Notification/Prohibition of Changes:* OI&T employs automated mechanisms to: a. Document proposed changes to the information system; b. Notify designated approval authorities of proposed changes to the information system and request change approval (See Attachment 2); c. Highlight proposed changes to the information system that have not been approved or disapproved (See Attachment 3); d. Prohibit changes to the information system until designated approvals are received; e. Document all changes to the information system; and f. Notify designated organization officials when approved changes to the information system are completed (See Attachment 3).	Not Selected	Not Selected	X
(2) *Test/Validate/Document Changes:* OI&T 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 baseline configurations for components and configuration items of information systems, changes to the configuration settings for IT products (e.g., operating systems, applications, firewalls, routers, and mobile devices), unscheduled/unauthorized changes, and changes to remediate vulnerabilities. VA will follow VA Directive 6004, *Configuration, Change, and Release Management Programs*.

(b) All IT systems and components will be covered by a chartered or authorized local Change Control Board (CCB) or national CCB. If a system does not require a local board, such as if it is the exclusive responsibility of a regional, national, or enterprise board, then this must be clearly documented in the SSP and the Continuity of Operations Plan (COOP), if applicable.

(c) OI&T will employ a change control process to ensure change requests are reviewed, documented and tested through a formal CCB. The local or system-level CCB will consist of the Information System Owner, local CIO, or designee and other specified individuals as needed that have collective responsibility and authority to review and approve changes to the information system. No IT systems and components, including hardware, software, databases, networking devices, or unique, one-of-a-kind system shall be modified unless approved by the local CCB.

(d) The change management process must include security impact analysis, user impact analysis, testing, and post-implementation follow-up.

(e) The CCB shall retain and review records of all proposed changes that will ultimately affect users, systems, infrastructure, MOU/ISAs, partner connections and the like.

(f) The CCB shall determine if any proposed change affects the overall security of the system. The Information System Owner, with assistance from the ISO and PO, will determine if the proposed change is a change requiring reauthorization.

(g) If any changes are made without the explicit written approval from the CCB, a roll back process will be enacted immediately. The executive sponsor shall communicate with the respective management team to mentor on up to a formal written warning.

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

(i) 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.

(j) 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.

(k) 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.

(l) 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 (P2)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T analyzes changes to the information system to determine potential security impacts prior to change implementation.	X	X	X
(1) *Separate Test Environments:* OI&T analyzes changes to the information system in a separate test environment before implementation 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
OI&T defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.	Not Selected	X	X
(1) *Automated Access Enforcement/Auditing:* The information system enforces access restrictions and supports auditing of the enforcement actions.	Not Selected	Not Selected	X
(2) *Review System Changes:* The Information System Owner reviews information system changes and circumstances to determine whether unauthorized changes have occurred (See Attachment 3).	Not Selected	Not Selected	X
(3) *Signed Components:* The information system prevents the installation of software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by OI&T (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 OI&T 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
OI&T: a. Establishes and documents configuration settings for IT products employed within the information system using security configuration checklists that reflect the most restrictive mode consistent with operational requirements (See Attachment 2); b. Implements the configuration settings; c. Identifies, documents, and approves any deviations from established configuration settings for information system components based on operational requirements (See Attachment 2); and d. Monitors and controls changes to the configuration settings in accordance with VA policies and procedures (See Attachment 2).	X	X	X
(1) *Automated Central Management/Application/Verification:* OI&T employs automated mechanisms to centrally manage, apply and verify configuration settings for information system components (See Attachment 3).	Not Selected	Not Selected	X
(2) *Respond to Unauthorized Changes:* OI&T employs security safeguards to respond to unauthorized changes to VA-defined configuration settings (See Attachment 3).	Not Selected	Not Selected	X
(3) [Withdrawn: Incorporated into SI-7]	---	---	---
Baseline allocation summary	CM-6	CM-6	CM-6 (1)(2)

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture and/or functionality of the system. IT products for which security-related configuration settings can be defined include, for example, mainframe computers, servers (e.g., database, email, authentication, web, proxy, file, domain name), workstations, input/output devices (e.g., scanners, copiers, and printers), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications. Security-related parameters are those parameters impacting the security state of the information system including parameters required to satisfy 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, services, and remote connections.

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

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Information System Owner configures the information system to provide only essential capabilities and prohibits or restricts the use of other identified functions, ports, protocols, and/or services (See Attachment 3).	X	X	X
(1) *Periodic Review:* The Information System Owner: a. Reviews the information system to identify unnecessary and/or non-secure functions, ports, protocols, and services (See Attachment 3); and b. Disables functions, ports, protocols, and services within the information system deemed to be unnecessary and/or non-secure (See Attachment 3).	Not Selected	X	X
(2) *Prevent Program Execution:* The Information System Owner prevents program execution in accordance with one or more of the following specifications: VA policies regarding software usage and restrictions and/or rules authorizing the terms and conditions of software program usage (See Attachment 3).	Not Selected	X	X
(4) *Unauthorized Software/Blacklisting:* The Information System Owner: a. Identifies software programs not authorized to execute on the information system (See Attachment 2); b. Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system; and c. Reviews and updates the list of unauthorized software programs (See Attachment 2).	Not Selected	X	Not Selected
(5) *Authorized Software/Whitelisting:* The Information System Owner: a. Identifies software programs authorized to execute on the information system and reviews and updates the list of authorized software programs (See Attachment 2); b. Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and c. Reviews and updates the list of authorized software programs (See Attachment 2).	Not Selected	Not Selected	X
Baseline allocation summary	CM-7	CM-7 (1)(2)(4)	CM-7 (1)(2)(5)

Where feasible, OI&T limits component functionality to a single function per device (e.g., email 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., VoIP, Instant Messaging, auto-execute, file sharing).

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

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Develops and documents an inventory of information system components that: 1. Accurately reflects the current information system; 2. Includes all components within the authorization boundary of the information system; 3. Is at the level of granularity deemed necessary for tracking and reporting; and 4. Includes information necessary for effective information system component accountability (See Attachment 3); b. Reviews and updates the information system component inventory (See Attachment 2).	X	X	X
(1) *Updates During Installations/Removals:* OI&T updates the inventory of information system components as an integral part of component installations, removals, and information system updates.	Not Selected	X	X
(2) *Automated Maintenance:* OI&T 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) *Automated Unauthorized Component Detection:* The Information System Owner: a. Employs automated mechanisms to detect the presence of unauthorized hardware, software, and firmware components within the information system (See Attachment 3); and b. Takes the following actions when unauthorized components are detected (one or more): disables network access by such components; isolates components; notifies designated organizational officials/positions (See Attachment 3).	Not Selected	X	X
(4) *Accountability Information:* OI&T includes in the information system component inventory information, a means for identifying individuals responsible/accountable for administering those components (See Attachment 3).	Not Selected	Not Selected	X
(5) *No Duplicate Accounting of Components:* OI&T verifies that all components within the authorization boundary of the information system are not duplicated in other information system component inventories.	Not Selected	X	X
Baseline allocation summary	CM-8	CM-8 (1)(3)(5)	CM-8 (1)(2)(3) (4)(5)

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

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T develops, documents, and implements a configuration management plan for the information system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Establishes a process for identifying configuration items throughout the SDLC and a process for managing the configuration of the configuration items; c. Defines the configuration items for the information system and places configuration items under configuration management; and d. Protects the configuration management plan from unauthorized disclosure and modification.	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 will conduct a security impact analysis prior to the implementation of any changes to the system.

(10) CM-10: Software Usage Restrictions (P2)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Uses software and associated documentation in accordance with contract agreements and copyright laws; b. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.	X	X	X
Baseline allocation summary	CM-10	CM-10	CM-10

(11) CM-11: User-Installed Software (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Establishes policies governing the installation of software by users (See Attachment 2); b. Enforces software installation policies through defined methods (See Attachment 2); and c. Monitors policy compliance (See Attachment 2).	X	X	X
Baseline allocation summary	CM-11	CM-11	CM-11

To maintain control over the types of software installed, OI&T identifies permitted and prohibited actions regarding software installation. Only those authorized by OI&T may install software. Permitted software installations may include, for example, updates and security patches to existing software and downloading applications from VA-approved “app stores.” Prohibited software installations may include, for example, software with unknown or suspect pedigrees or software that VA considers potentially malicious.

f. Contingency Planning (CP)

(1) CP-1: Contingency Planning Policy and Procedures (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Develops, documents, and disseminates to defined personnel or roles (See Attachment 2): 1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and b. Reviews and updates the current: 1. Contingency planning policy (See Attachment 2); and 2. Contingency planning procedures (See Attachment 2).	X	X	X
Baseline allocation summary	CP-1	CP-1	CP-1

VA OI&T in this Appendix has outlined VA's system security controls based on the current version of NIST 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.

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

NIST SP 800-53	APPLICABILITY		
	(3) LOW	(4) MODERATE	(5) HIGH
The Information System Owner: a. Develops a contingency plan for the information system that: 1. Identifies essential missions and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; 5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and 6. Is reviewed and approved by designated organizational officials (See Attachment 2); b. Distributes copies of the contingency plan (See Attachment 3); c. Coordinates contingency planning activities with incident handling activities; d. Reviews the contingency plan for the information system (See Attachment 2); e. Updates the contingency plan to address changes to VA, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; f. Communicates contingency plan changes (See Attachment 3); and g. Protects the contingency plan from unauthorized disclosure and modification.	(6) X	(7) X	(8) X
(1) *Coordinate with Related Plans:* The Information System Owner coordinates contingency plan development with organizational elements responsible for related plans.	Not Selected	X	X
(2) *Capacity Planning:* The Information 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) *Resume Essential Missions/Business Functions:* The Information System Owner plans for the resumption of essential missions and business functions after contingency plan activation (See Attachment 3).	Not Selected	X	X

NIST SP 800-53	APPLICABILITY		
	(3) LOW	(4) MODERATE	(5) HIGH
(4) *Resume all Missions/Business Functions:* The Information System Owner plans for the resumption of all missions and business functions within a defined time period of contingency plan activation (See Attachment 3).	Not Selected	Not Selected	X
(5) *Continue Essential Missions/Business Functions:* The Information System Owner plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites.	Not Selected	Not Selected	X
(8) *Identify Critical Assets:* The Information System Owner identifies critical information system assets supporting essential missions and business functions.	Not Selected	X	X
Baseline allocation summary	CP-2	CP-2 (1)(3)(8)	CP-2 (1)(2)(3) (4)(5)(8)

(a) Contingency planning for information systems is part of an overall Operating Unit program for achieving continuity of operations for mission/business functions. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. The effectiveness of contingency planning is maximized by considering such planning throughout the phases of the SDLC. Performing contingency planning on hardware, software, and firmware development can be an effective means of achieving information system resiliency. Contingency plans reflect the degree of restoration required for VA information systems since not all systems may need to fully recover to achieve the level of continuity of operations desired.

(b) 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 and/or 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, orderly/graceful degradation, information system shutdown, fall back to a manual mode, alternate information flows, and operating in a mode that is reserved for when the system is under attack. By closely coordinating contingency planning with incident handling activities, OI&T can ensure that the necessary contingency planning activities are in place and activated in the event of a security incident.

(c) Capacity planning is needed because different types of threats (e.g., natural disasters, targeted cyber attacks) can result in a reduction of the available processing, telecommunications, and support services originally intended to support VA mission/business functions. VA may need to anticipate degraded operations during contingency operations and factor such degradation into capacity planning.

(d) The time period for resumption of essential missions/business functions may be dependent on the severity/extent of disruptions to the information system and the information system's supporting infrastructure.

(e) OI&T identifies critical information system assets so that additional safeguards and countermeasures can be employed (above and beyond those safeguards and countermeasures routinely implemented) to help ensure that VA mission/business functions can continue to be conducted during contingency operations. In addition, the identification of critical information assets facilitates the prioritization of VA resources. Critical information system assets include technical and operational resources. Technical aspects include, for example, IT services, information system components, IT products, and mechanisms. Operational aspects include, for example, procedures (manually executed operations) and personnel (individuals operating technical safeguards and/or executing manual procedures). VA program protection plans can provide assistance in identifying critical assets.

(f) Information 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. Contingency planning is coordinated with incident handling to ensure that the necessary contingency activities are in place and can be activated in the event of a security incident. VA identifies critical information system assets to help ensure that VA missions and business functions can continue to be conducted during contingency operations.

(g) See VA Handbook 6500.8, *Information System Contingency Planning*, for more information and details.

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

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit provides contingency training to information system users consistent with assigned roles and responsibilities within a defined time period of assuming a contingency role or responsibility; when required by information system changes; and thereafter (See Attachment 2).	X	X	X
(1) *Simulated Events:* 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)

Contingency training provided by OI&T is linked to the assigned roles and responsibilities of VA personnel to ensure that the appropriate content and level of detail is included in such training. For example, regular users may only need to know when and where to report for duty during contingency operations and if normal duties are affected; system administrators may require additional training on how to set up information systems at alternate processing and storage sites; and managers/senior leaders may receive more specific training on how to conduct mission-essential functions in designated off-site locations and how to establish communications with other governmental entities for purposes of coordination on contingency-related activities. Training for contingency roles/responsibilities reflects the specific continuity requirements in the contingency plan.

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

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Tests the contingency plan for the information system using OI&T-defined tests to determine the effectiveness of the plan and VA's readiness to execute the plan (See Attachment 3); b. Reviews the contingency plan test results; and c. Initiates corrective actions, if needed.	X	X	X
(1) *Coordinate with Related Plans:* OI&T coordinates contingency plan testing with organizational elements responsible for related plans.	Not Selected	X	X
(2) *Alternate Processing Site:* OI&T tests the contingency plan at the alternate processing site: a. To familiarize contingency personnel with the facility and available resources; and b. To evaluate the capabilities of the alternate processing site to support contingency operations.	Not Selected	Not Selected	X
Baseline allocation summary	CP-4	CP-4 (1)	CP-4 (1)(2)

There are several methods for testing contingency plans to identify potential weaknesses (e.g., walk-through/tabletop, checklists, parallel or full interrupt simulations, and comprehensive exercises). Contingency plan testing includes 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**

Incorporated into **CP-2: Contingency Plan** control.

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

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and b. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.	Not Selected	X	X
(1) *Separation from Primary Site:* OI&T identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.	Not Selected	X	X
(2) *Recovery Time/Point Objectives:* OI&T configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.	Not Selected	Not Selected	X
(3) *Accessibility:* OI&T 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) An alternate storage site maintains duplicate copies of information and data in the event that the primary storage site is not available.

(b) Items covered by alternate storage site agreements include, for example, environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and coordination of delivery/retrieval backup media.

(c) Alternate storage sites reflect the requirements in contingency plans so that VA can maintain essential missions/business functions despite disruption, compromise, or failure in VA information systems.

(d) Area-wide disruptions refer to those types of disruptions that are broad in geographic scope (e.g., hurricane, regional power outage) with such determinations made by OI&T based on organizational assessments of risk.

(e) Explicit mitigation actions include, for example, duplicating backup information at other alternate storage sites if access problems occur at originally designated alternate sites; or, planning for physical access to retrieve backup information if electronic accessibility to the alternate site is disrupted.

(f) 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.

(g) OI&T will store securely system and application documentation and an up-to-date hard copy of the contingency plans at the alternate storage location.

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

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of defined information system operations for essential missions and business functions when the primary processing capabilities are unavailable (See Attachment 3); b. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for resumption; and c. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.	Not Selected	X	X
(1) *Separation from Primary Site:* OI&T identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.	Not Selected	X	X
(2) *Accessibility:* OI&T 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) *Priority-of-Service:* OI&T develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives).	Not Selected	X	X
(4) *Preparation for Use:* OI&T prepares the alternate processing site so that the site is ready to be used as the operational site supporting essential missions and business functions.	Not Selected	Not Selected	X
(5) [Withdrawn: Incorporated into CP-7]	---	---	---
Baseline allocation summary	Not Selected	CP-7 (1)(2)(3)	CP-7 (1)(2)(3)(4)

(a) Alternate processing sites are sites that are geographically distinct from primary processing sites. An alternate processing site provides processing capability in the event that the primary processing site is not available.

(b) Threats that affect the alternate processing sites are typically defined in the organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber attacks, and errors of omission/commission. OI&T determines what is considered a sufficient degree of separation between primary and alternate processing sites based on the types of threats that are of concern. For hostile cyber attacks the degree of separation between sites is less relevant.

(c) Priority-of-service agreements refer to negotiated agreements with service providers that ensure that VA receives priority treatment consistent with VA's availability requirements and the availability of information resources at the alternate processing site.

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

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T establishes alternate telecommunications services including necessary agreements to permit the resumption of defined information system operations for essential missions and business functions when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites (See Attachment 3).	Not Selected	X	X
(1) *Priority-of-Service Provisions:* OI&T: a. Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the organizational availability requirements (including recovery time objectives); and b. 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) *Single Points of Failure:* OI&T obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.	Not Selected	X	X
(3) *Separation of Primary/Alternate Providers:* OI&T obtains alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.	Not Selected	Not Selected	X
(4) *Provider Contingency Plan:* OI&T: a. Requires primary and alternate telecommunications service providers to have contingency plans;	Not Selected	Not Selected	X

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
b. Reviews provider contingency plans to ensure that the plans meet OI&T contingency requirements; and c. Obtains evidence of contingency testing/training by providers (See Attachment 2).			
Baseline allocation summary	Not Selected	CP-8 (1)(2)	CP-8 (1)(2)(3)(4)

(a) This control applies to telecommunications services (data and voice) for primary and alternate processing and storage sites. Alternate telecommunications services reflect the continuity requirements in contingency plans to maintain essential missions/business functions despite the loss of primary telecommunications services.

(b) OI&T may specify different time periods for primary/alternate sites.

(c) Alternate telecommunications services include, for example, additional organizational or commercial ground-based circuits/lines or satellites in lieu of ground-based communications.

(d) OI&T considers factors such as availability, quality of service, and access when entering into alternate telecommunications agreements.

(e) OI&T seeks to reduce common susceptibilities by, for example, minimizing shared infrastructure among telecommunications service providers and achieving sufficient geographic services.

(f) OI&T may consider using a single service provider in situations where the service provider can provide alternate telecommunications services meeting the separation needs addressed in the risk assessment.

(g) Reviews of provider contingency plans consider the proprietary nature of such plans. In some situations, a summary of provider contingency plans may be sufficient evidence for OI&T to satisfy the review requirement. Telecommunications service providers may also participate in ongoing disaster recovery exercises in coordination with the Department of Homeland Security, state, and local governments. OI&T may use these types of activities to satisfy evidentiary requirements related to service provider contingency plan reviews, testing, and training.

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

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Conducts backups of user-level information contained in the information system consistent with recovery time and recovery point objectives (See Attachment 3);	X	X	X

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
b. Conducts backups of system-level information contained in the information system consistent with recovery time and recovery point objectives (See Attachment 3); c. Conducts backups of information system documentation including security-related documentation consistent with recovery time and recovery point objectives (See Attachment 3); and d. Protects the confidentiality, integrity, and availability of backup information at storage locations.			
(1) *Testing for Reliability/Integrity:* OI&T tests backup information to verify media reliability and information integrity (See Attachment 3).	Not Selected	X	X
(2) *Test Restoration Using Sampling:* OI&T 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) *Separate Storage for Critical Information:* OI&T stores backup copies of critical information system software and other security-related information in a separate facility or in a fire-rated container that is not co-located with the operational system (See Attachment 3).	Not Selected	Not Selected	X
(5) *Transfer to Alternate Storage Site:* OI&T transfers information system backup information to the alternate storage site at a frequency and transfer rate consistent with the recovery time and recovery point objectives (See Attachment 3).	Not Selected	Not Selected	X
Baseline allocation summary	CP-9	CP-9 (1)	CP-9 (1)(2)(3)(5)

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

(b) Critical information system software includes, for example, operating systems, cryptographic key management systems, and intrusion detection/prevention systems. Security-related information includes, for example, organizational inventories of hardware, software, and firmware components.

(c) The Information System Owner in conjunction with the Information Owner defines the system and user-level information to be backed up.

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

(e) OI&T 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.

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

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

(h) The Operating Unit ensures that a mobile device or portable storage device does not contain the only copy of VA information. A backup 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 Information 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) *Transaction Recovery:* The information system implements transaction recovery for systems that are transaction-based.	Not Selected	X	X
(3) [Withdrawn: Addressed through tailoring procedures]			
(4) *Restore Within Time Period:* OI&T provides the capability to restore information system components from configuration-controlled and integrity-protected information representing a known, operational state for the components (See Attachment 3).	Not Selected	Not Selected	X
Baseline allocation summary	CP-10	CP-10 (2)	CP-10 (2)(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 a fully operational state. Recovery and reconstitution operations reflect mission and business priorities, recovery point/time and reconstitution objectives, and established metrics consistent with contingency plan requirements. 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, reestablishment of continuous monitoring activities, a potential information system reauthorization and the activities to prepare the system against future disruption, compromise, or failure. Recovery and reconstitution capabilities employed by the Operating Unit can include both automated mechanisms and manual procedures.

(11) **CP-11: Alternate Communications Protocols (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system provides the capability to employ alternative communications protocols in support of maintaining continuity of operations.	Not Selected	Not Selected	Not Selected
Baseline allocation summary	Not Selected	Not Selected	Not Selected

VA does not require, at this time, application of **CP-11: Alternate Communications Protocols**. OI&T may, at their discretion and the system's capability, elect to provide capability to employ alternate communications protocols.

(12) **CP-12: Safe Mode (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system, when certain conditions are detected, enters a safe mode of operation with defined restrictions of safe mode operation.	Not Selected	Not Selected	Not Selected
Baseline allocation summary	Not Selected	Not Selected	Not Selected

VA does not require, at this time, application of **CP-12: Safe Mode**. OI&T may, at their discretion and the system's capability, elect to provide a safe mode of operation.

(13) **CP-13: Alternative Security Mechanisms (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T employs alternative or supplemental security mechanisms for satisfying security functions when the primary means of implementing the security function is unavailable or compromised.	Not Selected	Not Selected	Not Selected
Baseline allocation summary	Not Selected	Not Selected	Not Selected

VA does not require, at this time, application of **CP-13: Alternative Security Mechanisms.** OI&T may, at their discretion and the system's capability, elect to employ alternative security mechanisms.

g. Identification and Authentication (IA)

(1) IA-1: Identification and Authentication Policy and Procedures (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Develops, documents, and disseminates to defined personnel or roles (See Attachment 2): 1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and b. Reviews and updates the current: 1. Identification and authentication policy (See Attachment 2); and 2. Identification and authentication procedures (See Attachment 2).	X	X	X
Baseline allocation summary	IA-1	IA-1	IA-1

(a) VA OI&T in this Appendix has outlined VA's system security controls based on the current version of NIST 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.

(b) User identification and authentication must be consistent with:

1. Homeland Security Presidential Directive (HSPD) 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*;

2. OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*;

3. FIPS 140-2 (or its successor);

4. FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*;

5. NIST SP 800-63, *Electronic Authentication Guideline*;

6. NIST SP 800-73, *Interfaces for Personal Identity Verification (4 parts): Part 1: End Point PIV Card Application Namespace, Data Model and Representation; Part 2: PIV Card Application Interface; Part 3: PIV Client Application Programming Interface; and Part 4: The PIV Transitional Data Model and Interfaces*;

7. NIST SP 800-76, *Biometric Specification for Personal Identity Verification*;

8. NIST SP 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification;* and

9. 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) *Network Access to Privileged Accounts:* The information system implements multifactor authentication for network access to privileged accounts.	X	X	X
(2) *Network Access to Non-Privileged Accounts*: The information system implements multifactor authentication for network access to non-privileged accounts.	Not Selected	X	X
(3) *Local Access to Privileged Accounts:* The information system implements multifactor authentication for local access to privileged accounts.	Not Selected	X	X
(4) *Local Access to Non-Privileged Accounts:* The information system implements multifactor authentication for local access to non-privileged accounts.	Not Selected	Not Selected	X
(8) *Network Access to Privileged Accounts – Replay-Resistant:* The Information System Owner implements replay-resistant authentication mechanisms for network access to privileged accounts.	Not Selected	X	X
(9) *Network Access to Non-Privileged Accounts- Replay-Resistant:* The Information System Owner implements replay-resistant authentication mechanisms for network access to non-privileged accounts.	Not Selected	Not Selected	X
(11) *Remote Access – Separate Device:* The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets the strength of mechanism requirements (See Attachment 2).	Not Selected	X	X
(12) *Acceptance of PIV Credentials*: The information system accepts and electronically verifies PIV credentials.	X	X	X
Baseline allocation summary	IA-2	IA-2	IA-2

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
	(1)(12)	(1)(2)(3)(8) (11)(12)	(1)(2)(3) (4)(8)(9) (11)(12)

(a) OI&T may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

(b) 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**.

(c) 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**.

(d) Multifactor authentication requires the use of two or more different factors to achieve authentication. The factors are defined as: (i) something you know (e.g., password, personal identification number); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as PIV. In addition to identifying and authenticating users at the information system level (i.e., at logon), OI&T also employs identification and authentication mechanisms at the application level, when necessary, to provide increased information security.

(e) 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)**.

(f) Remote access users who cannot use multifactor authentication for remote access must request an OIS RBD. (See the Policy Section on the OCS Portal for information on the OIS RBD process.)

(g) 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.

(h) Acceptance of PIV Credentials applies when OI&T implements multifactor authentication for logical access control systems and PACS.

(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

(a) 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 OI&T. 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 OI&T approved authentication solution (e.g., Institute of Electrical and Electronics Engineers, 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.

(b) All internal servers will use FIPS 140-2 (or its successor) validated server certificates for inter-server and server-to-user communications.

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

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T manages information system identifiers by: a. Receiving authorization from designated organizational officials/positions to assign an individual, group, role, or device identifier (See Attachment 3); b. Selecting an identifier that identifies an individual, group, role, or device; c. Assigning the identifier to the intended individual, group, role, or device; d. Preventing reuse of identifiers (See Attachment 3); and e. Disabling the identifier after a time period of inactivity (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. When the user identifier is the name of an information system account associated with an individual, 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). Preventing reuse of identifiers implies preventing the assignment of previously used individual, group, role, or device identifiers to different individuals, groups, roles, or devices.

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

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T manages information system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator; b. Establishing initial authenticator content for authenticators defined by OI&T; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; e. Changing default content of authenticators prior to information system installation; f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; g. Changing/refreshing authenticators (See Attachment 2); h. Protecting authenticator content from unauthorized disclosure and modification;	X	X	X

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and j. Changing authenticators for group/role accounts when membership to those accounts changes.			
(1) *Password-Based Authentication:* The information system, for password-based authentication: a. Enforces VA minimum password complexity (See Attachment 2); b. Enforces at least a number of changed characters when new passwords are created (See Attachment 2); c. Stores and transmits only cryptographically-protected representations of passwords; d. Enforces password minimum and maximum lifetime restrictions (See Attachment 2); e. Prohibits reuse of a password (See Attachment 2); and f. Allows the use of a temporary password for system logons with an immediate change to a permanent password.	X	X	X
(2) *PKI-Based Authentication:* The information system, for PKI-based authentication: a. Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information; b. Enforces authorized access to the corresponding private key; c. Maps the authenticated identity to the account of the individual or group; and d. Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.	Not Selected	X	X
(3) *In-Person or Trusted Third-Party Registration:* The Operating Unit requires the registration process to receive defined types of authenticators be conducted by a designated person or trusted third party before a designated registration authority with authorization by a designated organizational official/position (See Attachment 2).	Not Selected	X	X
(11) *Hardware Token-Based Authentication:* The information system, for hardware token-based authentication, employs mechanisms that satisfy specific token quality requirements (See Attachment 2).	X	X	X
Baseline allocation summary	IA-5 (1)(11)	IA-5 (1)(2)(3)(11)	IA-5 (1)(2)(3)(11)

(a) Individual 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. 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 the verification stage of biometric authentication. Specific actions that can be taken to safeguard user authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing individual authenticators with others, and reporting lost, stolen, 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) Cryptographically-protected passwords include, for example, encrypted versions of passwords and one-way cryptographic hashes of passwords.

(d) Password lifetime restrictions do not apply to temporary passwords.

(e) To mitigate certain brute force attacks against passwords, the Operating Unit may consider salting passwords.

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

(g) Authenticators (passwords) must be protected to prevent unauthorized use. 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 reuse, or be configured to bypass authentication mechanisms. For example, Internet browsers must not be enabled to save passwords for reuse. 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 unencrypted email 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 noncompliance with VA requirements; or

d. On direction 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 (P2)

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. For some types of information systems or system components, for example, desktops/notebooks with relatively large monitors, the threat (often referred to as shoulder surfing) may be significant. For other types of systems or components, for example, mobile devices with 2 to 4 inch screens, this threat may be less significant, and may need to be balanced against the increased likelihood of typographic input errors due to the small keyboards. Therefore, the means for obscuring the authenticator feedback is selected accordingly.

(7) IA-7:Cryptographic Module Authentication (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system implements 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

Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role.

(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
(1) *Acceptance of PIV Credentials from Other Agencies:* The information system accepts and electronically verifies PIV credentials from other Federal agencies.	X	X	X

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
(2) *Acceptance of Third-Party Credentials:* The information system accepts only Federal Identity, Credential, and Access Management (FICAM)-approved third-party credentials.	X	X	X
(3) *Use of FICAM-Approved Products:* OI&T employs only FICAM-approved information system components in defined information systems to accept third-party credentials (See Attachment 2).	X	X	X
(4) *Use of FICAM-Issued Profiles:* The information system conforms to FICAM-issued profiles.	X	X	X
Baseline allocation summary	IA-8 (1)(2)(3)(4)	IA-8 (1)(2)(3)(4)	IA-8 (1)(2)(3)(4)

(a) 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)**.

(b) Acceptance of PIV Credentials from Other Agencies applies to logical access control systems and PACS.

(c) OMB Memorandum 11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12-Policy for a Common Identification Standard for Federal Employees and Contractors*, requires Federal agencies to continue implementing the requirements specified in HSPD-12 to enable agency-wide use of PIV credentials.

(d) Third-party credentials are those credentials issued by non-Federal government entities approved by the FICAM Trust Framework Solutions initiative. Approved third party credentials meet or exceed the set of minimum Federal government-wide technical, security, privacy, and VA maturity requirements.

(e) Acceptance of Third-Party Credentials and Use of FICAM-Approved Products typically apply to information systems that are accessible to the general public, for example, public-facing Web sites.

(f) Use of FICAM-Issued Profiles addresses open identity management standards. To ensure that these standards are viable, robust, reliable, sustainable (e.g., available in commercial IT products), and interoperable as documented, the U.S. Government assesses and scopes identity management standards and technology implementations against applicable Federal legislation, directives, policies, and requirements. The result is FICAM-issued implementation profiles of approved protocols (e.g., FICAM authentication protocols such as Security Assertion Markup Language 2.0 and OpenID 2.0, as well as other protocols such as the FICAM Backend Attribute Exchange).

(9) **IA-9: Service Identification and Authentication (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T identifies and authenticates information system services using security safeguards.	Not Selected	Not Selected	Not Selected
Baseline allocation summary	Not Selected	Not Selected	Not Selected

VA does not require, at this time, application of **IA-9: Service Identification and Authentication.** OI&T may, at their discretion and the system's capability, elect to employ service identification and authentication.

(10) **IA-10: Adaptive Identification and Authentication (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T requires that individuals accessing the information system employ supplemental authentication techniques or mechanisms under specific defined circumstances or situations.	Not Selected	Not Selected	Not Selected
Baseline allocation summary	Not Selected	Not Selected	Not Selected

VA does not require, at this time, application of **IA-10: Adaptive Identification and Authentication.** OI&T may, at their discretion and the system's capability, elect to adaptive identification and authentication.

(11) **IA-11: Re-Authentication (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T requires users and devices to re-authenticate when defined circumstances or situations require re-authentication.	Not Selected	Not Selected	Not Selected
Baseline allocation summary	Not Selected	Not Selected	Not Selected

VA does not require, at this time, application of **IA-11: Re-Authentication.** OI&T may, at their discretion and the system's capability, elect to employ re-authentication.

h. **Incident Response (IR)**

(1) **IR-1: Incident Response Policy and Procedures (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Develops, documents, and disseminates to defined personnel or roles (See Attachment 2): 1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and b. Reviews and updates the current: 1. Incident response policy (See Attachment 2); and 2. Incident response procedures (See Attachment 2).	X	X	X
Baseline allocation summary	IR-1	IR-1	IR-1

(a) VA OI&T in this Appendix has outlined VA's system security controls based on the current version of NIST 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.

(b) For additional information regarding incident response see VA Handbook 6500.2.

(2) **IR-2: Incident Response Training (P2)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T provides incident response training to information system users consistent with assigned roles and responsibilities: a. Within a defined time period of assuming an incident response role or responsibility (See Attachment 2); b. When required by information system changes; and c. For a defined frequency thereafter (See Attachment 2).	X	X	X

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
(1) *Simulated Events:* OI&T incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.	Not Selected	Not Selected	X
(2) *Automated Training Environments:* OI&T employs automated mechanisms to provide a more thorough and realistic incident response training environment.	Not Selected	Not Selected	X
Baseline allocation summary	IR-2	IR-2	IR-2 (1)(2)

(a) Incident response training is linked to the assigned roles and responsibilities of VA personnel to ensure that the appropriate content and level of detail is included in such training. For example, regular users may only need to know who to call or how to recognize an incident on the information system; system administrators may require additional training on how to handle/remediate incidents; and incident responders may receive more specific training on forensics, reporting, system recovery, and restoration. Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources.

(b) Role-based security incident response training will be incorporated with IT competency modeling. See **AT-3: Role-Based Security Training**.

(3) **IR-3: Incident Response Testing (P2)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T tests the incident response capability for the information system at a defined frequency using specified tests to determine the incident response effectiveness and documents the results (See Attachment 2).	Not Selected	X	X
(2) *Coordination with Related Plans*: OI&T coordinates incident response testing with VA elements responsible for related plans.	Not Selected	X	X
Baseline allocation summary	Not Selected	IR-3 (2)	IR-3 (2)

(a) VA tests incident response capabilities to determine the overall effectiveness of the capabilities and to identify potential weaknesses or deficiencies. Incident response testing includes, for example, the use of checklists, walk-through or tabletop exercises, simulations (parallel/full interrupt), and comprehensive exercises. Incident response testing can also include a determination of the effects on VA operations (e.g., reduction in mission capabilities), assets, and individuals due to incident response.

(b) Organizational plans related to incident response testing include, for example, Business Continuity Plans, Contingency Plans, Disaster Recovery Plans, COOPs, Crisis Communications Plans, Critical Infrastructure Plans, and Occupant Emergency Plans.

(c) All tests are documented in the SSP.

(d) 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
OI&T: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. 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) *Automated Incident Handling Processes:* OI&T employs automated mechanisms to support the incident handling process.	Not Selected	X	X
(4) *Information Correlation:* OI&T correlates incident information and individual incident responses to achieve a VA-wide perspective on incident awareness and response.	Not Selected	Not Selected	X
Baseline allocation summary	IR-4	IR-4 (1)	IR-4 (1)(4)

(a) VA considers incident response as part of the definition, design, and development of mission/business processes and information systems.

(b) Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, user/administrator reports, and reported supply chain events.

(c) Effective incident handling capability includes coordination among many organizational entities including, for example, mission/business owners, Information System Owners, the AO, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive (function).

(d) Automated mechanisms supporting incident handling processes include, for example, online incident management systems.

(e) Sometimes the nature of a threat event, for example, a hostile cyber attack, is such that it can only be observed by bringing together information from different sources including various reports and reporting procedures established by VA.

(f) When a system requires remediation due to an incident, VA-NSOC will develop remediation instructions to reduce risk of continued compromise, reinfection, or proliferation of malicious activity. The instructions will include timelines in which remediation activities must be completed. Information System Owners must implement the remediation requirements and meet the remediation timelines established by VA-NSOC. Information System Owners, working with their ISOs, should immediately submit an RBD to VA-NSOC for DAS for OIS approval if they cannot implement the remediation or meet the required remediation timeline.

(g) VA will establish performance metrics to measure the effectiveness of incident response activities.

(h) VA-NSOC will establish standard remediation timelines based on remediation action required.

(i) Incidents must be remediated in a timely fashion to reduce the exposure of VA data to potential security threats.

(5) **IR-5: Incident Monitoring (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	**MODERATE**	**HIGH**
OI&T tracks and documents information system security incidents.	X	X	X
• *Automated Tracking/Data Collection/Analysis:* OI&T 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)

OI&T employs VA-approved tools for tracking and documenting information system 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 OI&T: a. Require personnel to report suspected security/privacy incidents immediately upon suspicion to their ISO, PO, and supervisor (See Attachment 2); and b. Report security/privacy incident information (See Attachment 2).	X	X	X
(1) *Automated Reporting:* OI&T 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. Suspected security incidents include, for example, the receipt of suspicious email communications that can potentially contain malicious code. The types of security incidents reported, the content and timeliness of the reports, and the list of designated reporting authorities reflect applicable Federal laws, Executive Orders, directives, 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) Any VA staff member who witnesses a case of egregious waste of government resources or outright fraud must comply with 38 C.F.R. § 1.201, *Employee's Duty to Report* and 38 C.F.R. § 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 via email 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.

(7) **IR-7: Incident Response Assistance (P2)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit and OI&T 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) *Automation Support for Availability of Information/Support:* OI&T 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 OI&T 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 email at VA-NSOC@va.gov).

(8) **IR-8: Incident Response Plan (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit and OI&T: a. Develop an incident response plan that: 1. Provides OI&T with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and	X	X	X

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
8. Is reviewed and approved by designated organizational personnel or roles (See Attachment 2); b. 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); c. Review the incident response plan (See Attachment 3); d. Update the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; e. 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); and f. Protect the incident response plan from unauthorized disclosure and modification.			
Baseline allocation summary	IR-8	IR-8	IR-8

(9) IR-9: Information Spillage Response (P0)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit and OI&T respond to information spills by: a. Identifying the specific information involved in the information system contamination; b. Alerting designated individuals or roles of the information spill using a method of communication not associated with the spill; c. Isolating the contaminated information system or system component; d. Eradicating the information from the contaminated information system or component; e. Identifying other information systems or system components that may have been subsequently contaminated; and f. Performing other actions.	Not Selected	Not Selected	Not Selected
Baseline allocation summary	Not Selected	Not Selected	Not Selected

VA does not require, at this time, application of **IR-9: Information Spillage Response.** OI&T may, at their discretion and the system's capability, elect to employ an information spillage response.

(10) **IR-10: Integrated Information Security Analysis Team (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit and OI&T establish an integrated team of forensic/malware analysts, tool developers, and real-time operations personnel.	Not Selected	Not Selected	Not Selected
Baseline allocation summary	Not Selected	Not Selected	Not Selected

VA does not require, at this time, application of **IR-10: Integrated Information Security Analysis Team.** OI&T may, at their discretion and the system's capability, elect to employ an integrated information security analysis team.

i. **Maintenance (MA)**

(1) **MA-1 System Maintenance Policy and Procedures (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Develops, documents, and disseminates to defined personnel or roles (See Attachment 2): 1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and b. Reviews and updates the current: 1. System maintenance policy (See Attachment 2); and 2. System maintenance procedures (See Attachment 2).	X	X	X
Baseline allocation summary	MA-1	MA-1	MA-1

VA OI&T in this Appendix has outlined VA's system security controls based on the current version of NIST 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.

(2) MA-2: Controlled Maintenance (P2)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. 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; b. Approves and monitors all maintenance activities, whether performed on-site or remotely and whether the equipment is serviced on-site or removed to another location; c. Requires that defined personnel or roles explicitly approve the removal of the information system or system components from VA facilities for off-site maintenance or repairs (See Attachment 2); d. Sanitizes equipment to remove all information from associated media prior to removal from VA facilities for off-site maintenance or repairs; e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions: and f. Includes maintenance-related information in VA maintenance records (See Attachment 3).	X	X	X
(1) [Withdrawn: Incorporated into MA-2]	---	---	---
(2) *Automated Maintenance Activities:* OI&T: a. Employs automated mechanisms to schedule, conduct, and document maintenance and repairs; and b. Produces up-to-date, accurate, and complete records of all maintenance and repair actions requested, scheduled, in process, and completed.	Not Selected	Not Selected	X
Baseline allocation summary	MA-2	MA-2	MA-2 (2)

This control addresses the information security aspects of the information system maintenance program and applies to all types of maintenance to any system component (including applications) conducted by any local or non-local entity (e.g., in-contract, warranty, in-house, software maintenance agreement). System maintenance also includes those components not directly associated with information processing and/or data/information retention such as scanners, copiers, and printers. Information necessary for creating effective maintenance records includes, for example: (i) date and time of maintenance; (ii) name of individuals or group performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; (v) information system components/equipment removed or replaced (including identification numbers, if applicable).

(3) MA-3: Maintenance Tools (P3)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T approves, controls, and monitors information system maintenance tools.	Not Selected	X	X
(1) *Inspect Tools:* OI&T inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.	Not Selected	X	X
(2) *Inspect Media:* OI&T checks media containing diagnostic and test programs for malicious code before the media are used in the information system.	Not Selected	X	X
(3) *Prevent Unauthorized Removal:* OI&T prevents the unauthorized removal of maintenance equipment containing VA information by: a. Verifying that there is no VA information contained on the equipment; b. Sanitizing or destroying the equipment; c. Retaining the equipment within the facility; or d. Obtaining an exemption from designated organizational personnel or roles explicitly authorizing removal of the equipment from the facility (See Attachment 2).	Not Selected	Not Selected	X
Baseline allocation summary	Not Selected	MA-3 (1)(2)	MA-3 (1)(2)(3)

(a) This control addresses the security-related issues associated with maintenance tools used specifically for diagnostic and repair actions on VA information systems.

(b) Maintenance tools can include hardware, software, and firmware items. Maintenance tools are potential vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and subsequently into VA information systems. Maintenance tools can include, for example, hardware/software diagnostic test equipment and hardware/software packet sniffers.

(c) This control does not cover hardware/software components that may support information system maintenance, yet are a part of the system, for example, the software implementing “ping,” “ls,” “ipconfig,” or the hardware and software implementing the monitoring port of an Ethernet switch.

(d) If, upon inspection of maintenance tools, OI&T determines that the tools have been modified in an improper/unauthorized manner, or contain malicious code, the incident is handled consistent with VA policies and procedures for incident handling.

(e) If, upon inspection of media containing maintenance diagnostic and test programs, OI&T determines that the media contain malicious code, the incident is handled consistent with VA policies and procedures for incident handling.

(4) **MA-4: Non-Local Maintenance (P2)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Approves and monitors non-local maintenance and diagnostic activities; b. 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; c. Employs strong authenticators in the establishment of non-local maintenance and diagnostic sessions; d. Maintains records for non-local maintenance and diagnostic activities; and e. Terminates session and network connections when non-local maintenance is completed.	X	X	X
(2) Document Non-Local Maintenance: OI&T documents, in the security plan for the information system, the policies and procedures for establishment and use of non-local maintenance and diagnostic connections.	Not Selected	X	X
(3) Compare Security/Sanitization: OI&T: a. Requires that non-local maintenance and diagnostic services be performed from an information system that implements a security capability comparable to the capability implemented on the system being serviced; or b. 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) before reconnecting the component to the information system.	Not Selected	Not Selected	X
Baseline allocation summary	MA-4	MA-4 (2)	MA-4 (2)(3)

(a) 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. Authentication techniques used in the establishment of non-local maintenance and diagnostic sessions reflect the network access requirements in **IA-2: Identification and Authentication (Organizational Users)**. Typically, strong authentication requires authenticators that are resistant to replay attacks and employ multifactor authentication. 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.

(b) Comparable security capability on information systems, diagnostic tools, and equipment providing maintenance services implies that the implemented security controls on those systems, tools, and equipment are at least as comprehensive as the controls on the information system being serviced.

(5) **MA-5: Maintenance Personnel (P2)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel; b. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and c. Designates VA personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.	X	X	X
(1) *Individuals Without Appropriate Access:* OI&T: a. Implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements: 1. Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved VA personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; 2. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearance or formal access approvals, all volatile information storage components within the information system are sanitized and all non-volatile storage media are removed or physically disconnected from the system and secured; and b. Develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system.	Not Selected	Not Selected	X
Baseline allocation summary	MA-5	MA-5	MA-5 (1)

(a) This control applies to individuals performing hardware or software maintenance on VA information systems, while **PE-2: Physical Access Authorizations** addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems (e.g., custodial staff, physical plant maintenance personnel).

(b) OI&T may issue temporary credentials to individuals based on an assessment of risk, when required to conduct maintenance activities with little or no notice. Examples of individuals, not previously identified as authorized maintenance personnel, that may require temporary credentials for privileged access to VA's systems, are IT manufacturers, vendors, systems integrators, and consultants. Temporary credentials must be issued and documented by the Information System Owner, local CIO, or designee for either one-time use or for a very limited period of time.

(c) Individuals Without Appropriate Access denies maintenance personnel who lack appropriate security clearances or are not U.S. citizens, visual and electronic access to any classified information, controlled unclassified information, or VA sensitive information contained on VA information systems. Procedures for the use of maintenance personnel can be documented in the security plan for the information system.

(6) **MA-6: Timely Maintenance (P2)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Information System Owner obtains maintenance support and/or spare parts for information system 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

OI&T specifies those information system components that result in increased risk to VA operations, assets, individuals, other organizations or the Nation when the functionality provided by those components is not operational.

j. Media Protection (MP)

(1) MP-1: Media Protection Policy and Procedures (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Develops, documents, and disseminates to defined personnel or roles (See Attachment 2): 1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and b. Reviews and updates the current: 1. Media protection policy (See Attachment 2); and 2. Media protection procedures (See Attachment 2).	X	X	X
Baseline allocation summary	MP-1	MP-1	MP-1

VA OI&T in this Appendix has outlined VA's system security controls based on the current version of NIST 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.

(2) MP-2: Media Access (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Information System Owner restricts access to information in printed form or on digital media to a defined list of authorized individuals (See below and See Attachment 3).	X	X	X
(1) [Withdrawn: Incorporated into MP-4 (2)]	---	---	---
Baseline allocation summary	MP-2	MP-2	MP-2

(a) The use of VA information system media within the Operating Unit must first be authorized by the Information System Owner, local CIO, or designee. 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 and portable storage 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 (P2)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and b. Exempts specific types of information system media or hardware 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 security marking refers to the application/use of human-readable security attributes.

(b) Marking of information system media reflects applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

(4) **MP-4: Media Storage (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Physically controls and securely stores types of digital and non-digital media within controlled areas (See Attachment 3); and b. 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, portable storage 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, portable storage 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) Controlled areas are areas for which the Operating Unit provides sufficient physical and procedural safeguards to meet the requirements established for protecting information and/or information systems (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: a. Protects and controls information system media during transport outside of controlled areas using security safeguards (See Attachment 3); b. Maintains accountability for information system media during transport outside of controlled areas; c. Documents activities associated with the transport of information system media; and d. Restricts the activities associated with the transport of information system media to authorized personnel.	Not Selected	X	X
(2) [Withdrawn: Incorporated into MP-5]	---	---	---
(3) *Cryptographic Protection:* The information system implements 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 (4)	MP-5 (4)

(a) Physical and technical security safeguards are commensurate with the security category or classification of the information residing on the media. Safeguards to protect media during transport include, for example, locked containers and cryptography.

(b) Activities associated with transport include the actual transport as well as those activities such as releasing media for transport and ensuring that media enters the appropriate transport processes.

(c) For the actual transport, authorized transport and courier personnel may include individuals from outside VA (e.g., U.S. Postal Service or a commercial transport or delivery service).

(d) Maintaining accountability of media during transport includes, for example, restricting transport activities to authorized personnel, and tracking and/or obtaining explicit records of

transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering.

(e) This control also applies to mobile or portable storage devices with information storage capability that is transported outside of controlled areas. See **AC-19: Access Control for Mobile Devices** regarding requirements for protecting mobile and portable storage devices.

(6) **MP-6: Media Sanitization (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit and OI&T: a. Sanitize information system media prior to disposal, release out of VA control, or release for reuse using defined sanitization techniques and procedures in accordance with applicable Federal and VA standards and policies (See Attachment 2); and b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.	X	X	X
(1) *Review/Approve/Track/Document/Verify:* The Operating Unit and OI&T reviews, approves, tracks, documents, and verifies media sanitization and disposal actions.	Not Selected	Not Selected	X
(2) *Equipment Testing:* OI&T tests sanitization equipment and procedures to verify that the intended sanitization is being achieved (See Attachment 2).	Not Selected	Not Selected	X
(3) *Non-Destructive Techniques:* OI&T applies non-destructive sanitization techniques to portable storage devices prior to connecting such devices to the information system under the identified circumstances (See Attachment 2).	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 VA or external 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) Hard drives that are encrypted with FIPS 140-2 (or its successor) validated encryption do not require pre-sanitization prior to leaving VA control; they may be shipped to the authorized destruction vendor without further processing.

(c) 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.

(d) 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.

(e) Operating Units refer to the current version of NIST 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.

(7) **MP-7: Media Use (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit restricts the use of specific types of information system media on information systems or system components using security safeguards (See Attachment 2).	X	X	X
(1) *Prohibit Use Without Owner:* OI&T prohibits the use of portable storage devices in VA information systems when such devices have no identifiable owner.	Not Selected	X	X
Baseline allocation summary	MP-7	MP-7 (1)	MP-7 (1)

This control also applies to mobile or portable storage devices with information storage capability. In contrast to **MP-2: Media Access**, which restricts user access to media, this control restricts the use of certain types of media on information systems, for example, restricting/prohibiting the use of flash drives or external hard disk drives.

(8) **MP-8: Media Downgrading (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Establishes an information system media downgrading process that includes employing downgrading mechanisms with strength and integrity; b. Ensures that the information system media downgrading process is commensurate with the security category and/or classification level of the information to be removed and the access authorizations of the potential recipients of the downgraded information; c. Identifies information system media requiring downgrading; and d. Downgrades the identified information system media using the established process.	Not Selected	Not Selected	Not Selected
Baseline allocation summary	Not Selected	Not Selected	Not Selected

VA does not require, at this time, application of **MP-8: Media Downgrading.** OI&T may, at their discretion and the system's capability, elect to employ media downgrading.

k. Physical and Environmental Protection (PE)

(1) PE-1: Physical and Environmental Protection Policy and Procedures (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Develops, documents, and disseminates to defined personnel or roles (See Attachment 2): 1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and b. Reviews and updates the current: 1. Physical and environmental protection policy (See Attachment 2); and 2. Physical and environmental protection procedures (See Attachment 2).	X	X	X
Baseline allocation summary	PE-1	PE-1	PE-1

VA OI&T in this Appendix has outlined VA's system security controls based on the current version of NIST 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. 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
OI&T: a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides; b. Issues authorization credentials for facility access; c. Reviews the access list detailing authorized facility access by individuals (See Attachment 3); and	X	X	X

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
d. Removes individuals from the facility access list when access is no longer required.			
Baseline allocation summary	PE-2	PE-2	PE-2

(a) This control applies to VA employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors.

(b) Authorization credentials include, for example, badges, identification cards, and smart cards. OI&T determines the strength of authorization credentials needed (including level of forge-proof badges, smart cards, or ID cards) consistent with Federal standards, policies, and procedures. This control only applies to areas within facilities that have not been designated as publicly accessible.

(c) The Information 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: a. Enforces physical access authorizations at entry/exit points to the facility where the information system resides (See Attachment 3) by: 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress/egress to the facility using PACS/devices and/or guards (See Attachment 3); b. Maintains physical access audit logs for entry/exit points (See Attachment 3); c. Provides security safeguards to control access to areas within the facility officially designated as publicly accessible (See Attachment 2); d. Escorts visitors and monitors visitor activity under defined circumstances requiring visitor escorts and monitoring (See Attachment 2); e. Secures keys, combinations, and other physical access devices. f. Inventories physical access devices (See Attachment 2); and g. Changes combinations and keys as specified in the security plan and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated (See Attachment 3).	X	X	X

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
(1) *Information System Access:* The Operating Unit enforces physical access authorizations to the information system in addition to the physical access controls for the facility at physical spaces containing one or more components of the information system (See Attachment 3).	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 facility guards needed including, for example, professional physical security staff or other personnel such as administrative staff or information system users. Physical access devices include, for example, keys, locks, combinations, and card readers. Safeguards for publicly accessible areas within VA facilities include, for example, cameras, monitoring guards, and isolating selected information systems and/or system components in secured areas.

(b) FICAM provides implementation guidance for identity, credential, and access management capabilities for PACS.

(c) Audit logs can be procedural (e.g., a written log of individuals accessing the facility and when such access occurred), automated (e.g., capturing ID provided by a PIV card), or some combination thereof.

(d) Components of VA information systems (e.g., workstations, terminals) may be located in areas designated as publicly accessible with access to such devices being safeguarded.

(e) Keys will be controlled in accordance with the current version of VA Handbook 0730.

(f) The requirement for independent physical access authorizations for high-impact systems provides additional physical security for those areas within facilities where there is a 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 VA facilities using security safeguards (See Attachment 3).	Not Selected	X	X
Baseline allocation summary	Not Selected	PE-4	PE-4

(a) Physical security safeguards applied to information system distribution and transmission lines help to prevent accidental damage, disruption, and physical tampering. In

addition, physical safeguards may be necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions.

(b) Security safeguards to control physical access to system distribution and transmission lines include, for example:

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 (P2)**

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

(a) Controlling physical access to output devices includes, for example, placing output devices in locked rooms or other secured areas and allowing access to authorized individuals only, and placing output devices in locations that can be monitored by VA personnel.

(b) Monitors (viewing), printers, copiers, scanners, fax machines, 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: a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents; b. Reviews physical access logs at a defined frequency and upon occurrence of defined events or potential indications of events (See Attachment 3); and c. Coordinates results of reviews and investigations with VA's incident response capability.	X	X	X
(1) *Intrusion Alarms/Surveillance Equipment:* The Operating Unit monitors physical intrusion alarms and surveillance equipment.	Not Selected	X	X

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
(4) *Monitoring Physical Access to Information Systems:* OI&T monitors physical access to the information system in addition to the physical access monitoring of the facility as physical spaces containing one or more components of the information system (See Attachment 3).	Not Selected	Not Selected	X
Baseline allocation summary	PE-6	PE-6 (1)	PE-6 (1)(4)

(a) 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.

(b) Suspicious physical access activities include, for example: (i) access outside of normal work hours; (ii) repeated access to areas not normally accessed; (iii) access for unusual lengths of time; and (iv) out-of-sequence access.

(c) Monitoring Physical Access to Information Systems provides additional monitoring for those areas within facilities where there is a concentration of information system components (e.g., server rooms, media storage areas, communication centers).

(7) **PE-7: Visitor Control**

Incorporated into **PE-2: Physical Access Authorizations** and **PE-3: Physical Access Control** controls.

(8) **PE-8: Visitor Access Records (P3)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Maintains visitor access records to the facility where the information system resides (See Attachment 2); and b. Reviews visitor access records (See Attachment 3).	X	X	X
(1) *Automated Records Maintenance/Review:* OI&T employs automated mechanisms to facilitate the maintenance and review of visitor access records.	Not Selected	Not Selected	X
(2) [Withdrawn: Incorporated into PE-2]	---	---	---
Baseline allocation summary	PE-8	PE-8	PE-8 (1)

(a) Visitor access records will include, but are not limited to:

1. Name and 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 and organization of person visited.

(b) Visitor access records are not required for publicly accessible areas.

(c) Operating Units will use a validation/redundancy procedure to ensure that access logs are reviewed as required.

(9) **PE-9: Power Equipment and 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

OI&T determines the types of protection necessary for power equipment and cabling employed at different locations both internal and external to VA facilities and environments of operation. This includes, for example, generators and power cabling outside of buildings, internal cabling and uninterruptable power sources within an office or data center, and power sources for self-contained entities such as vehicles and satellites.

(10) **PE-10: Emergency Shutoff (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit: a. Provides the capability of shutting off power to the information system or individual system components in emergency situations; b. Places emergency shutoff switches or devices in locations to facilitate safe and easy access for personnel (See Attachment 3); and c. Protects emergency power shutoff capability from unauthorized activation.	Not Selected	X	X
Baseline allocation summary	Not Selected	PE-10	PE-10

This control applies primarily to facilities containing concentrations of information system resources including, 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 and/or transition of the information system to long-term alternate power in the event of a primary power source loss (See Attachment 3).	Not Selected	X	X
(1) *Long-Term Alternate Power Supply – Minimal Operational Capability:* 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)

Operating Units can provide long-term alternate power supply, for example, by the use of secondary commercial power supply or other external power supply. Long-term alternate power supplies for the information system can be either manually or automatically activated.

(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 applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms.

(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) *Detection Devices/Systems:* The Operating Unit employs fire detection devices/systems for the information system that activate automatically and notify designated organizational	Not Selected	Not Selected	X

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
officials/positions and emergency responders in the event of a fire (See Attachment 3).			
(2) *Suppression Devices/Systems:* The Operating Unit employs fire suppression devices/systems for the information system that provide automatic notification of any activation to designated organizational officials/positions and emergency responders (See Attachment 3).	Not Selected	Not Selected	X
(3) *Automatic Fire Suppression:* 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 (3)	PE-13 (1)(2)(3)

(a) Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.

(b) This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms.

(14) **PE-14: Temperature and Humidity Controls (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit: a. Maintains temperature and humidity levels within the facility where the information system resides at acceptable levels (See Attachment 3); and b. Monitors temperature and humidity levels (See Attachment 3).	X	X	X
Baseline allocation summary	PE-14	PE-14	PE-14

This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms.

(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 or isolation valves that are accessible, working properly, and known to key personnel.	X	X	X
(1) *Automation Support:* The Operating Unit employs mechanisms to detect the presence of water in the vicinity of the information system and alerts designated organizational officials/positions (See Attachment 3).	Not Selected	Not Selected	X
Baseline allocation summary	PE-15	PE-15	PE-15 (1)

This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern, without affecting all of VA

(16) **PE-16: Delivery and Removal (P2)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit authorizes, monitors, and controls types of information system components 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 7002-1, *Logistics Management Procedures*.

(17) **PE-17: Alternate Work Site (P2)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit: a. Employs security controls at alternate work sites (See Attachment 3); b. Assesses, as feasible, the effectiveness of security controls at alternate work sites; and c. 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) While commonly distinct from alternative processing sites, alternate work sites may provide readily available alternate locations as part of contingency operations.

(c) Operating Units may define different sets of security controls and policies for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites.

(d) This control supports the contingency planning activities of VA and the Federal Telework initiative. 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 (P3)**

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 (See Attachment 3).	Not Selected	Not Selected	X
Baseline allocation summary	Not Selected	Not Selected	PE-18

(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 other forms of incoming electromagnetic radiation.

(b) VA and Operating Unit 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 information systems and therefore increase the potential for unauthorized access to VA communications (e.g., through the use of wireless sniffers or microphones).

(19) **PE-19: Information Leakage (P0)**

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**. OI&T may, at their discretion, elect to protect against information leakage.

(20) **PE-20: Asset Monitoring and Tracking (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit: a. Employs asset location technologies to track and monitor the location and movement of assets within controlled areas; and b. Ensures that asset location technologies are employed in accordance with applicable Federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.	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-20: Asset Monitoring and Tracking**. OI&T may, at their discretion, elect to employ asset monitoring and tracking.

I. Planning (PL)

(1) PL-1: Security Planning Policy and Procedures (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Develops, documents, and disseminates to defined personnel or roles (See Attachment 2): 1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and b. Reviews and updates the current: 1. Security planning policy (See Attachment 2); and 2. Security planning procedures (See Attachment 2).	X	X	X
Baseline allocation summary	PL-1	PL-1	PL-1

VA OI&T 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.

(2) PL-2: System Security Plan (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Information System Owner: a. Develops a security plan for the information system that: 1. Is consistent with VA's EA; 2. Explicitly defines the authorization boundary for the system; 3. Describes the operational context of the information system in terms of missions and business processes; 4. Provides the security categorization of the information system including supporting rationale; 5. Describes the operational environment for the information system and relationships with or connections to other information systems; 6. Provides an overview of the security requirements for	X	X	X

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
the system; 7. Identifies any relevant overlays, if applicable; 8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and 9. Is reviewed and approved by the AO or designee prior to plan implementation; b. Distributes copies of the security plan and communicates subsequent changes to the plan to designated organizational officials/positions (See Attachment 3); c. Reviews the security plan for the information system (See Attachment 2); d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or SCAs; and e. Protects the security plan from unauthorized disclosure and modification.			
(3) *Plan/Coordinate with Other Organizational Entities:* The Information System Owner plans and coordinates security-related activities affecting the information system with designated individuals or groups before conducting such activities in order to reduce the impact on other organizational entities (See Attachment 3).	Not Selected	X	X
Baseline allocation summary	PL-2	PL-2 (3)	PL-2 (3)

Every VA information system must be included/covered by an SSP that is compliant with guidance in the current versions of NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, and NIST 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**

Incorporated into **PL-2: System Security Plan** control.

(4) **PL-4: Rules of Behavior (P2)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
VA: a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; b. Receives a signed acknowledgment from such individuals indicating that they have read, understand, and agree to abide by the ROB, before authorizing access to information and the information system; c. Reviews and updates the ROB (See Attachment 2); and d. Requires individuals who have signed a previous version of the ROB to read and re-sign when the ROB are revised/updated.	X	X	X
(1) *Social Media and Networking Restrictions:* OI&T includes in the ROB, explicit restrictions on the use of social media/networking sites and posting VA information on public Web sites.	Not Selected	X	X
Baseline allocation summary	PL-4	PL-4 (1)	PL-4 (1)

(a) The VA National ROB must be signed annually by all VA users of VA information systems or VA 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 acceptable 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 electronic security and privacy awareness training. Other Federal Government Agency users, who complete security and privacy awareness training through their agency, will be required to sign the VA National ROB.

(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**

This control will be incorporated into policy created by Office of Privacy and Records Management.

(6) **PL-6: Security-Related Activity Planning**

Incorporated into **PL-2: System Security Plan** control.

(7) **PL-7: Security Concept of Operations (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit: a. Develops a security Concept of Operations for the information system containing at a minimum, how VA intends to operate the system from the perspective of information security; and b. Reviews and updates the Concept of Operations.	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 **PL-7: Security Concept of Operations**. OI&T may, at their discretion, elect to employ security concept of operations.

(8) **PL-8: Information Security Architecture (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit: a. Develops an information security architecture for the information system that: 1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of VA information; 2. Describes how the information security architecture is integrated into and supports the EA; and 3. Describes any information security assumptions about, and dependencies on, external services; b. Reviews and updates the information security architecture to reflect updates in the EA (See Attachment 2); and c. Ensures that the planned information security architecture changes are reflected in the security plan, the security Concept of Operations, and VA procurements/acquisitions.	Not Selected	X	X
Baseline allocation summary	Not Selected	PL-8	PL-8

(a) This control addresses actions taken by VA in the design and development of information systems. The information security architecture at the individual information system level is consistent with and complements the more global, VA-wide information security architecture described in **PM-7: Enterprise Architecture** that is integral to and developed as part of the EA. The information security architecture includes an architectural description, the

placement/allocation of security functionality (including security controls), security-related information for external interfaces, information being exchanged across the interfaces, and the protection mechanisms associated with each interface. In addition, the security architecture can include other important security-related information, for example, user roles and access privileges assigned to each role, unique security requirements, the types of information processed, stored, and transmitted by the information system, restoration priorities of information and information system services, and any other specific protection needs.

(b) There are going to be key dependencies on external information services and service providers. Describing such dependencies in the information security architecture is important to developing a comprehensive mission/business protection strategy. Establishing, developing, documenting, and maintaining under configuration control, a baseline configuration for VA information systems is critical to implementing and maintaining effective information security architecture. The development of the information security architecture is coordinated with the SAOP/CPO to ensure that security controls needed to support privacy requirements are identified and effectively implemented.

(c) This control primarily helps ensure VA develops an information security architecture for the information system, and that the security architecture is integrated with or tightly coupled to the EA through the VA-wide information security architecture.

(9) **PL-9: Central Management (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit centrally manages defined security controls and related processes.	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 **PL-9: Central Management**. OI&T may, at their discretion, elect to employ central management.

m. **Program Management (PM)**

(1) **PM-1: Information Security Program Plan (P1)** (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 VA's Program Management controls.

(b) VA OI&T 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. Include the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;

3. Reflect coordination among VA entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical);

4. Are approved by OI&T 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;

(c) The documents are reviewed continuously and updated according to VA records management requirements;

(d) The program is updated to address organizational changes and problems identified during plan implementation or subsequent reviews; and

(e) The program and associated details are protected from unauthorized disclosure and modification.

(f) 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 must be reviewed and updated on an annual basis. Local SOPs should be created, as needed.

(2) **PM-2: Senior Information Security Officer (CISO) (P1)** (See Attachment 1)

VA CIO has appointed a CISO with the mission and resources to coordinate, develop, implement, and maintain a VA-wide information security program.

(3) **PM-3: Information Security Resources (P1)** (See Attachment 1)

VA OI&T 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 (P1)** (See Attachment 1)

(a) VA OI&T has implemented a standardized process for ensuring that POA&Ms for the security program and the associated VA information systems: (i) are developed and

maintained; (ii) document the remedial information security actions to adequately respond to risk to VA operations and assets, individuals, other organizations, and the Nation; and (iii) are reported in accordance with OMB FISMA reporting requirements.

(b) VA OI&T reviews POA&Ms for consistency with the VA risk management strategy and VA-wide priorities for risk response actions.

(c) A POA&M is based on findings from SCAs, security impact analysis, continuous monitoring, and risk management activities.

(5) **PM-5: Information System Inventory (P1)** (See Attachment 1)

OI&T 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. Service Delivery and Engineering 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 (P1)** (See Attachment 1)

VA OI&T 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) (P1)** (See Attachment 1)

OI&T'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 (P1)** (See Attachment 1)

VA OI&T 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 (P1)** (See Attachment 1)

VA OI&T 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. VA implements the risk management strategy consistently across the organization and reviews and updates the strategy as required to address VA changes.

(10) PM-10: Security Authorization Process (P1) (See Attachment 1)

OI&T has developed a security authorization process to manage and control VA information system security posture. See VA Handbook 6500.3.

(11) **PM-11: Mission/Business Process Definition (P1)** (See Attachment 1)

VA OI&T 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 achievable protection needs are obtained. OI&T works closely with VHA, VBA, and NCA to determine their missions and their security requirements and needs and to ensure they are involved in evaluating the impact of security controls on mission and business processes.

(12) **PM-12: Insider Threat Program (P1)** (See Attachment 1)

(a) VA OI&T has an insider threat program that includes a cross-discipline insider threat incident handling team.

(b) The cross-discipline insider threat incident handling team includes representation from major departments across VA and meets on a regular basis to discuss the current level of organizational preparedness in addressing insider threat. The insider threat program includes controls to detect malicious insider activity and the correlation of both technical and nontechnical information. Human resources records are especially important in this effort, as there is compelling evidence to show that some types of insider crimes are often preceded by nontechnical behaviors in the workplace (e.g., ongoing patterns of disgruntled behavior and conflicts with coworkers and other colleagues). These precursors can better inform and guide organizational officials in more focused, targeted monitoring efforts. The participation of a legal team is important to ensure that all monitoring activities are performed in accordance with appropriate legislation, directives, regulations, policies, standards, and guidelines.

(13) **PM-13: Information Security Workforce (P1)** (See Attachment 1)

(a) VA OI&T has an information security workforce development and improvement program.

(b) The VA information security workforce development and improvement program includes, for example: (i) defining the knowledge and skill levels needed to perform information security duties and tasks; (ii) developing role-based training programs for individuals assigned information security roles and responsibilities; and (iii) providing standards for measuring and building individual qualifications for incumbents and applicants for information security-related positions. The VA workforce program also includes associated information security career paths to encourage: (i) information security professionals to advance in the field and fill positions with greater responsibility; and (ii) VA to fill information security-related positions with qualified personnel. Information security workforce development and improvement programs focus on developing and institutionalizing core information security capabilities of selected personnel needed to protect VA operations, assets, and individuals.

(14) **PM-14: Testing, Training, and Monitoring (P1)** (See Attachment 1)

(a) VA OI&T implements a process for ensuring that VA plans for conducting security testing, training, and monitoring activities associated with VA information systems:

1. Are developed and maintained;

2. Continue to be executed in a timely manner; and

(b) VA OI&T reviews testing, training, and monitoring plans for consistency with VA risk management strategy and VA-wide priorities for risk response actions.

(c) With the importance of continuous monitoring programs, the implementation of information security across the three tiers of the risk management hierarchy, and the widespread use of common controls, VA coordinates and consolidates the testing and monitoring activities that are routinely conducted as part of ongoing VA assessments supporting a variety of security controls. Security training activities, while typically focused on individual information systems and specific roles, also necessitate coordination across all VA elements. Testing, training, and monitoring plans and activities are informed by current threat and vulnerability assessments.

(15) **PM-15: Contacts With Security Groups and Associations (P3)** (See Attachment 1)

(a) VA OI&T establishes and institutionalizes contact with selected groups and associations within the security community:

1. To facilitate ongoing security education and training for VA personnel;

2. To maintain currency with recommended security practices, techniques, and technologies; and

3. To share current security-related information including threats, vulnerabilities, and incidents.

(b) Ongoing contact with security groups and associations is of paramount importance in an environment of rapidly changing technologies and threats. Security groups and associations include, for example, special interest groups, forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations. VA selects groups and associations based on VA missions/business functions. VA shares threat, vulnerability, and incident information consistent with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

(16) **PM-16: Threat Awareness Program (P1)** (See Attachment 1)

(a) VA OI&T has a threat awareness program that includes a cross-VA information-sharing capability.

(b) Because of the constantly changing and increasing sophistication of adversaries, especially the advanced persistent threat, adversaries are more likely to successfully breach or compromise VA information systems. VA will share threat information as one technique to address this concern. This includes, for example, sharing threat events (i.e., tactics, techniques, and procedures) that VA has experienced, mitigations that VA has found are effective against certain types of threats, or threat intelligence (i.e., indications and warnings about threats that are likely to occur). Threat information sharing may be bilateral (e.g., government-commercial cooperatives, government-government cooperatives), or multilateral (e.g., VA taking part in threat-sharing consortia). Threat information may be highly sensitive requiring special agreements and protection, or less sensitive and freely shared.

n. **Personnel Security (PS)**

(1) **PS-1: Personnel Security Policy and Procedures (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Develops, documents, and disseminates to defined personnel or roles (See Attachment 2): 1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and b. Reviews and updates the current: 1. Personnel security policy (See Attachment 2); and 2. Personnel security procedures (See Attachment 2).	X	X	X
Baseline allocation summary	PS-1	PS-1	PS-1

VA OI&T in this Appendix has outlined VA's system security controls based on the current version of NIST 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.

(2) **PS-2: Position Risk Designation (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
VA: a. Assigns a risk designation to all VA positions; b. Establishes screening criteria for individuals filling those positions; and c. Reviews and updates position risk designations consistent with policy and procedures as required (See Attachment 2).	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: a. Screens individuals prior to authorizing access to the information system; and b. Rescreens individuals according to policy and procedures required (See Attachment 2).	X	X	X
Baseline allocation summary	PS-3	PS-3	PS-3

(a) VA requires that all personnel be subject to a successfully adjudicated 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 Human Resources personnel will ensure that screening is conducted for Federal employees and all other appointed workforce members.

(d) Compensated Work Therapy workers are considered patients and VA is unable to perform a background screening. Therefore, they are not permitted to access VA information systems or VA sensitive information.

(e) 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.

(f) Background Investigations: The level of background investigation 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 background investigations are contained in VA Directive and Handbook 0710.

(g) 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 (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit, upon termination of individual employment: a. Disables information system access (See Attachment 2); b. Terminates/revokes any authenticators/credentials associated with the individual; c. Conducts exit interviews that include a discussion of information security topics (See Attachment 3); d. Retrieves all security-related VA information system-related property; e. Retains access to VA information and information systems formerly controlled by the terminated individual; and f. Notifies designated organizational officials/positions within a defined time period (See Attachment 3).	X	X	X
(2) *Automated Notification:* The Operating Unit employs automated mechanisms to notify designated organizational officials/positions upon termination of an individual (See Attachment 3).	Not Selected	Not Selected	X
Baseline allocation summary	PS-4	PS-4	PS-4 (2)

(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.

(c) Human Resources may perform exit interviews on behalf of the Operating Unit.

(d) Automated mechanisms can be used to send automatic alerts or notifications to specific VA personnel or roles (e.g., management personnel, supervisors, personnel security officers, ISOs, system administrators, or IT administrators) when individuals are terminated. Such automatic alerts or notifications can be conveyed in a variety of ways, including, for example, via telephone, email, text message, or Web sites.

(5) **PS-5: Personnel Transfer (P2)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Operating Unit: a. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within VA; b. Initiates transfer or reassignment actions promptly (See Attachment 3); c. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and d. Notifies designated organizational officials/positions within a defined time period (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 Human Resources 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
The Operating Unit: a. Develops and documents access agreements for VA information systems; b. Reviews and updates the access agreements (See Attachment 2); c. Ensures that individuals requiring access to VA information and information systems: 1. Sign appropriate access agreements prior to being granted access; and 2. Re-sign access agreements to maintain access to VA information systems when access agreements have been updated or at a defined frequency (See Attachment 2).	X	X	X
Baseline allocation summary	PS-6	PS-6	PS-6

(a) Access agreements include, for example, nondisclosure agreements, acceptable use agreements, ROBs, and conflict-of-interest agreements (See **PL-4: Rules of Behavior** for VA's ROB requirements).

(b) VA's current approved 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: a. Establishes personnel security requirements including security roles and responsibilities for third-party providers; b. Requires third-party providers to comply with personnel security policies and procedures established by VA; c. Documents personnel security requirements; d. Requires third-party providers to notify designated organizational officials/positions of any personnel transfers or terminations of third-party personnel who possess VA credentials and/or badges, or who have information system privileges (See Attachment 2); and e. Monitors provider compliance.	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 personnel security 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: a. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and b. Notifies designated organizational officials/positions when a formal employee sanctions process is implemented, identifying the individual sanctioned and the reason for the sanction (See Attachment 2).	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 Human Resources 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 Human Resources, 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.

o. Risk Assessment (RA)

(1) RA-1: Risk Assessment Policy And Procedures (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Develops, documents, and disseminates to defined personnel or roles (See Attachment 2): 1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and b. Reviews and updates the current: 1. Risk assessment policy (See Attachment 2); and 2. Risk assessment procedures (See Attachment 2).	X	X	X
Baseline allocation summary	RA-1	RA-1	RA-1

VA OI&T in this Appendix has outlined VA's system security controls based on the current version of NIST 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.

(2) RA-2: Security Categorization (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Information System Owner: a. Categorizes information and the information system in accordance with applicable Federal laws, Executive Orders, policies, regulations, standards, and guidance; b. Documents the security categorization results (including	X	X	X

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
supporting rationale) in the security plan for the information system; and c. Ensures that the security categorization decision is reviewed and approved by the AO or designee.			
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, NIST SP 800-60, and the results of the categorization must be documented in the SSP. The security categories describe the potential adverse impacts to VA operations and assets and individuals, if VA information and information systems are 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 NIST SP 800-37 and VA Directive 6500.

(3) **RA-3: Risk Assessment (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The Information System Owner: a. 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; b. Documents risk assessment results (See Attachment 2); c. Reviews risk assessment results (See Attachment 2); d. Disseminates risk assessment results to designated organizational officials/positions (See Attachment 3); and e. Updates the risk assessment at a defined 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	X	X	X

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
conditions that may impact the security state of the system (See Attachment 2).			
Baseline allocation summary	RA-3	RA-3	RA-3

VA Information System Owners will perform system risk assessments using VA OI&T approved methodologies.

(4) **RA-4: Risk Assessment Update**

Incorporated into **RA-3: Risk Assessment** control.

(5) **RA-5: Vulnerability Scanning (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Scans for vulnerabilities in the information system and hosted applications at a defined frequency and/or randomly and when new vulnerabilities potentially affecting the system/applications are identified and reported (See Attachment 3); b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact. c. Analyzes vulnerability scan reports and results from SCAs; d. Remediates legitimate vulnerabilities in accordance with an organizational assessment of risk (See Attachment 2); and e. Shares information obtained from the vulnerability scanning process and SCAs with designated organizational officials/positions to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies) (See Attachment 3).	X	X	X
(1) *Update Tool Capability:* OI&T employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.	Not Selected	X	X
(2) *Update by Frequency/Prior to New Scan/When Identified:* OI&T updates the information system vulnerabilities scanned at a defined frequency, prior to a new scan, or when new vulnerabilities are identified and reported (See Attachment 3).	Not Selected	X	X
(4) *Discoverable Information:* OI&T determines what information is discoverable by adversaries and subsequently takes corrective actions (See Attachment 3).	Not Selected	Not Selected	X

NIST SP 800-53	APPLICABILITY		
	LOW	**MODERATE**	**HIGH**
(5) *Privileged Access:* The information system implements privileged access authorization to identified information system components for selected vulnerability scanning activities (See Attachment 3).	Not Selected	X	X
(7) [Withdrawn: Incorporated into CM-8]	---	---	---
Baseline allocation summary	RA-5	RA-5 (1)(2)(5)	RA-5 (1)(2)(4)(5)

(a) Security categorization of information systems guides the frequency and comprehensiveness of vulnerability scans.

(b) OI&T determines the required vulnerability scanning for all information system components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked.

(c) Vulnerability scanning includes, for example, scanning for patch levels, 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 control mechanisms.

(d) 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.

(e) 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).

(f) 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.

(g) Information System Owners, system managers, and other OI&T 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), and Internet Information Services).

(h) The vulnerabilities to be scanned need to be readily updated as new vulnerabilities are discovered, announced, and scanning methods developed. This updating process helps to

ensure that potential vulnerabilities in the information system are identified and addressed as quickly as possible.

(i) In certain situations, the nature of the vulnerability scanning may be more intrusive or the information system component that is the subject of the scanning may contain highly sensitive information. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and also protects the sensitive nature of such scanning.

(j) The Operating Unit implements patch and vulnerability management in accordance with the **SI-2: Flaw Mediation**, control outlined in this Handbook.

(6) RA-6: Technical Surveillance Countermeasures Survey (P0)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T employs a technical surveillance countermeasures survey at specified locations when events or indicators occur.	Not Selected	Not Selected	Not Selected
Baseline allocation summary	Not Selected	Not Selected	Not Selected

VA does not require, at this time, application of **RA-6: Technical Surveillance Countermeasures Survey.** OI&T may, at their discretion and the system's capability, elect to employ a technical surveillance countermeasures survey.

p. System and Services Acquisition (SA)

(1) SA-1: System and Services Acquisition Policy and Procedures (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Develops, documents, and disseminates to defined personnel or roles (See Attachment 2): 1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and b. Reviews and updates the current: 1. System and services acquisition policy (See Attachment 2); and 2. System and services acquisition procedures (See Attachment 2).	X	X	X
Baseline allocation summary	SA-1	SA-1	SA-1

(a) VA OI&T in this Appendix has outlined VA's system security controls based on the current version of NIST 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.

(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
OI&T management: a. Determines information security requirements for the information system or information system service in mission/business process planning; b. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and c. 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 NIST 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: System Development Life Cycle (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Manages the information system using a defined SDLC that incorporates information security considerations (See Attachment 2); b. Defines and documents information security roles and responsibilities throughout the SDLC; c. Identifies individuals having information security roles and responsibilities; and d. Integrates VA information security risk management process into SDLC activities.	X	X	X
Baseline allocation summary	SA-3	SA-3	SA-3

(a) All 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 an authority to operate (ATO). Systems that cannot provide such recovery/decryption capabilities must be reviewed by the OIG, then subsequently agreed to by the VA CIO prior to system development and 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: Acquisition Process (P1)**

NIST SP 800-53	**APPLICABILITY**		
	(5) LOW	(6) MODERATE	(7) HIGH
The Operating Unit includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and VA mission/business needs: a. Security functional requirements; b. Security strength requirements; c. Security assurance requirements; d. Security-related documentation requirements; e. Requirements for protecting security-related documentation; f. Description of the information system developmental environment and environment in which the system is intended to operate; and g. Acceptance criteria.	X	X	X
(1) *Functional Properties of Security Controls:* The Operating Unit requires the developer of the	Not Selected	X	X

NIST SP 800-53	APPLICABILITY		
information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.			
(2) *Design/Implementation Information for Security Controls:* The Operating Unit requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; at a defined level of detail (See Attachment 3).	Not Selected	X	X
(4) [Withdrawn: Incorporated into CM-8 (9)]	---	---	---
(9) *Functions/Ports/Protocols/Services In Use*: The organization requires the developer of the information system, system component, or information system service to identify early in the SDLC, the functions, ports, protocols, and services intended for organizational use.		X	X
(10) *Use of Approved PIV Products:* The Operating Unit employs only IT products on the FIPS 201-approved products list for PIV capability implemented within VA information systems.	X	X	X
(8) Baseline allocation summary	SA-4 (10)	SA-4 (1)(2)(9)(10)	SA-4 (1)(2)(9)(10)

(a) Security functional requirements include security capabilities, security functions, and security mechanisms. Security strength requirements associated with such capabilities, functions and mechanisms include degree of correctness, completeness, resistance to direct attack, and resistance to tampering or bypass.

(b) Security assurance requirements include: (i) development processes, procedures, practices, and methodologies; and (ii) evidence from development and assessment activities providing grounds for confidence that the required security functionality has been implemented and the required security strength has been achieved. Security documentation requirements address phases of the SDLC.

(c) Security functionality, assurance, and documentation requirements are expressed in terms of security controls and control enhancements that have been selected through the tailoring process. The security control tailoring process includes, for example, the specification of parameter values through the use of assignment and selection statements and the specification of platform dependencies and implementation information.

(d) Requirements in acquisition documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented.

(e) The identification of functions, ports, protocols, and services early in the SDLC (e.g., during the initial requirements definition and design phases) allows VA to influence the design of the information system, information system component, or information system service. This early involvement in the life cycle helps VA to avoid or minimize the use of functions, ports, protocols, or services that pose unnecessarily high risks and to understand the trade-offs involved in blocking specific ports, protocols, or services (or when requiring information system service providers to do so). Early identification of functions, ports, protocols, and services avoids costly retrofitting of security controls after the information system, system component, or information system service has been implemented.

(f) Additional contract security policy and procedures are outlined in VA Handbook 6500.6.

(5) **SA-5: Information System Documentation (P2)**

NIST SP 800-53	(6) APPLICABILITY		
	LOW	**MODERATE**	**HIGH**
The Operating Unit: a. Obtains administrator documentation for the information system, system component, or information system service that describes: 1. Secure configuration, installation, and operation of the system, component, or service; 2. Effective use and maintenance of security functions/mechanisms; and 3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions. b. Obtains user documentation for the information system, system components, or information system service that describes: 1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms; 2. Methods for user interaction which enables individuals to use the system, component, or service in a more secure manner; and 3. User responsibilities in maintaining the security of the system, component, or service. c. Documents attempts to obtain information system,	(7)	(8) X	(9)

system component, or information system service documentation when such documentation is either unavailable or non-existent and takes defined actions in response (See Attachment 3); d. Protects documentation as required, in accordance with the risk management strategy; and e. Distributes documentation to designated organizational officials/positions (See Attachment 3).			
(1) [Withdrawn: Incorporated into SA-4 (1)]	---	---	---
(2) [Withdrawn: Incorporated into SA-4 (2)]	---	---	---
(3) [Withdrawn: Incorporated into SA-4 (2)]	---	---	---
Baseline allocation summary	SA-5	SA-5	SA-5

System documentation contains descriptions of the system hardware, software, policies, standards, procedures, and approvals related to the system life cycle and formalizes 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. Documentation that addresses information system vulnerabilities may require an increased level of protection. Secure operation of the information system, includes, for example, initially starting the system and resuming secure system operation after any lapse in system operation.

(6) **SA-6: Software Usage Restrictions**

Incorporated into **CM-10: Software Usage Restrictions** and **SI-7: Software, Firmware, and Information Integrity** controls.

(7) **SA-7: User-Installed Software**

Incorporated into **CM-11: User-Installed Software** and **SI-7: Software, Firmware, and Information Integrity** controls.

(8) SA-8: Security Engineering Principles (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T 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

OI&T designs and implements an information system using security engineering principles recommended by the current version of NIST 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
OI&T: a. Requires that providers of external information system services comply with VA information security requirements and employ security controls in accordance with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and guidance (See Attachment 2); b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and c. Employs defined processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis (See Attachment 2).	X	X	X
(2) *Identification of Functions/Ports/Protocols/Services:* OI&T requires providers of external information system services to identify the functions, ports, protocols, and other services required for the use of such services (See Attachment 3).	Not Selected	X	X
Baseline summary allocation	SA-9	SA-9 (2)	SA-9 (2)

(a) An external information system service is a service that is implemented outside of the authorization boundary of a VA information system. This includes services that are used by, but not part of, VA information systems. In VA these services are called Managed Services. FISMA and OMB policy require that external providers processing, storing, or transmitting Federal information or operating information systems on behalf of the Federal government ensure that such providers meet the same security requirements that Federal agencies are required to meet. VA establishes relationships with external service providers in a variety of ways including, for example, through joint ventures, business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, and supply chain exchanges. The responsibility for managing risks from the use of external information system services remains with the program office requesting the service. 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. The extent and nature of this chain of trust varies based on the relationships between VA and the external provider. 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 expectations of performance for security controls, describe measurable outcomes, and identify remedies and response requirements for identified instances 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
OI&T requires the developer of the information system, system component, or information system service to: a. Perform configuration management during system, component, or service (one or more): design; development; implementation; and/or operation (See Attachment 3); b. Document, manage, and control the integrity of changes to defined configuration items under configuration management (See Attachment 3); c. Implement only VA-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and	Not Selected	X	X

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
e. Track security flaws and flaw resolution within the system component, or service and report findings to authorized personnel (See Attachment 3).			
Baseline allocation summary	Not Selected	SA-10	SA-10

Safeguards include, for example, protecting from unauthorized modification or destruction, the master copies of all material used to generate security-relevant portions of the system hardware, software, and firmware. Maintaining the integrity of changes to the information system, information system component, or information system service requires configuration control throughout the SDLC to track authorized changes and prevent unauthorized changes. Configuration items that are placed under configuration management (if existence/use is required by other security controls) include: the formal model; the functional, high-level, and low-level design specifications; other design data; implementation documentation; source code and hardware schematics; the running version of the object code; tools for comparing new versions of security-relevant hardware descriptions and software/firmware source code with previous versions; and test fixtures and documentation. Depending on the mission/business needs of VA and the nature of the contractual relationships in place, developers may provide configuration management support during the operations and maintenance phase of the life cycle.

(11) **SA-11: Developer Security Testing and Evaluation (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T requires the developer of the information system, system component, or information system service to: a. Create and implement a security assessment plan; b. Perform one or more of the following: unit; integration; system; and/or regression testing/evaluation at a defined depth and coverage (See Attachment 3); c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation; d. Implement a verifiable flaw remediation process; and e. Correct flaws identified during security testing/evaluation.	Not Selected	X	X
Baseline allocation summary	Not Selected	SA-11	SA-11

(a) Developmental security testing and evaluation occurs at all post-design phases of the SDLC. Such testing/evaluation confirms that the required security controls are implemented correctly, operating as intended, enforcing the desired security policy, and meeting established security requirements. Security properties of information systems may be

affected by the interconnection of system components or changes to those components. These interconnections or changes (e.g., upgrading or replacing applications and operating systems) may adversely affect previously implemented security controls.

(b) Security assessment plans provide the specific activities that developers plan to carry out including the types of analyses, testing, evaluation, and reviews of software and firmware components, the degree of rigor to be applied, and the types of artifacts produced during those processes. Contracts specify the acceptance criteria for security assessment plans, flaw remediation processes, and the evidence that the plans and processes have been diligently applied. Methods for reviewing and protecting plans, evidence, and documentation are commensurate with the security category or classification level of the information system. Contracts will specify documentation protection requirements.

(c) 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 to the information system, system component, or information system service by employing security safeguards 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) Information systems (including system components that compose those systems) need to be protected throughout the SDLC (i.e., during design, development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement). Protection of VA information systems is accomplished through threat awareness, by the identification, management, and reduction of vulnerabilities at each phase of the life cycle and the use of complementary, mutually reinforcing strategies to respond to risk.

(b) VA will implement a standardized process to address supply chain risk with respect to information systems and system components, and to educate the acquisition workforce on threats, risks, and required security controls. VA uses the acquisition/procurement processes to require supply chain entities to implement necessary security safeguards to: (i) reduce the likelihood of unauthorized modifications at each stage in the supply chain; and (ii) protect information systems and information system components, prior to taking delivery of such systems/components.

(c) Security safeguards include, for example: (i) security controls for development systems, development facilities, and external connections to development systems; (ii) vetting development personnel; and (iii) use of tamper-evident packaging during shipping/warehousing. Methods for reviewing and protecting development plans, evidence, and documentation are commensurate with the security category or classification level of the information system.

(13) **SA-13: Trustworthiness (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Describes the trustworthiness required in the information system, system component, or information system service supporting its critical missions/business functions; and b. Implements an assurance overlay to achieve such trustworthiness.	Not Selected	Not Selected	Not Selected
Baseline allocation summary	Not Selected	Not Selected	Not Selected

VA does not require, at this time, application of **SA-13: Trustworthiness.** OI&T may, at their discretion, elect to implement this control.

(14) **SA-14: Criticality Analysis (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T identifies critical information system components and functions by performing a criticality analysis for information systems, information system components, or information system services at defined decision points in the SDLC.	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**. OI&T may, at their discretion, elect to implement this control.

(15) **SA-15: Development Process, Standards, and Tools (P2)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Requires the developer of the information system, system component, or information system service to follow a documented development process that: 1. Explicitly addresses security requirements;	Not Selected	Not Selected	X

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
2. Identifies the standards and tools used in the development process; 3. Documents the specific tool options and tool configurations used in the development process; and 4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development. b. Reviews the development process, standards, tools, and tool options/configurations to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy security requirements (See Attachment 2).			
Baseline allocation summary	Not Selected	Not Selected	SA-15

Development tools include, for example, programming languages and computer-aided design systems. Reviews of development processes can include, for example, the use of maturity models to determine the potential effectiveness of such processes. Maintaining the integrity of changes to tools and processes enables accurate supply chain risk assessment and mitigation, and requires robust configuration control throughout the life cycle (including design, development, transport, delivery, integration, and maintenance) to track authorized changes and prevent unauthorized changes.

(16) **SA-16: Developer-Provided Training (P2)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T requires the developer of the information system, system component, or information system service to provide training on the correct use and operation of the implemented security functions, controls, and/or mechanisms (See Attachment 2).	Not Selected	Not Selected	X
Baseline allocation summary	Not Selected	Not Selected	SA-16

This control applies to external and internal (in-house) developers. Training of personnel is an essential element to ensure the effectiveness of security controls implemented within VA information systems. Training options include, for example, classroom-style training, web-based/computer-based training, and hands-on training. VA can also request sufficient training materials from developers to conduct in-house training or offer self-training to VA personnel. OI&T determines the type of training necessary and may require different types of training for different security functions, controls, or mechanisms.

(17) **SA-17: Developer Security Architecture and Design (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that: a. Is consistent with and supportive of VA's security architecture which is established within and is an integrated part of VA's EA; b. Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and c. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.	Not Selected	Not Selected	X
Baseline allocation summary	Not Selected	Not Selected	SA-17

This control is primarily directed at external developers, although it could also be used for internal (in-house) development. In contrast, **PL-8: Information Security Architecture** is primarily directed at internal developers to help ensure that VA develops an information security architecture that is integrated or tightly coupled to the EA. This distinction is important if/when VA outsources the development of information systems, information system components, or information system services to external entities, and there is a requirement to demonstrate consistency with VA's EA and information security architecture.

(18) **SA-18: Tamper Resistance and Detection (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T implements a tamper protection program for the information system, system component, or information system service.	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-18: Tamper Resistance and Detection**. OI&T may, at their discretion, elect to implement this control.

(19) **SA-19: Component Authenticity (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Develops and implements anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the information system; and b. Reports counterfeit information system components to (one or more): source of counterfeit component; reporting organizations; designated personnel or roles.	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-19: Component Authenticity**. OI&T may, at their discretion, elect to implement this control.

(20) **SA-20: Customized Development of Critical Components (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T re-implements or custom develops critical 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-20: Customized Development of Critical Components**. OI&T may, at their discretion, elect to implement this control.

(21) **SA-21: Developer Screening (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T requires that the developer of the information system, system component, or information system service: a. Have appropriate access authorizations as determined by assigned official government duties; and b. Satisfy additional personnel screening criteria.	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-21: Developer Screening**. OI&T may, at their discretion, elect to implement this control.

(22) **SA-22: Unsupported System Components (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer; and b. Provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.	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-22: Unsupported System Components**. OI&T may, at their discretion, elect to implement this control.

q. **System and Communications Protection (SC)**

(1) **SC-1: System and Communications Protection Policy and Procedures (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Develops, documents, and disseminates to defined personnel or roles (See Attachment 2): 1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and b. Reviews and updates the current: 1. System and communications protection policy (See Attachment 2); and 2. System and communications protection procedures (See Attachment 2).	X	X	X
Baseline allocation summary	SC-1	SC-1	SC-1

VA OI&T in this Appendix has outlined VA's system security controls based on the current version of NIST 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.

(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. OI&T implements separation of system management-related functionality from user functionality by using different computers, different central processing units, different instances of operating systems, different network addresses, virtualization techniques, or combination of these 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. Separation of system and user functionality may include isolating administrative interfaces on different domains 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). Such isolation controls access to and protects the integrity of, the hardware, software, and firmware that perform those security functions.

Information systems implement code separation (i.e., separation of security functions from non-security functions) in a number of ways, including, for example, through the provision of the security kernels via processor rings or processor modes.

For non-kernel code, security function isolation is often achieved through file system protections that serve to protect the code on disk, and address space protections that protect executing code. Information systems restrict access to security functions through the use of access control mechanisms and by implementing least privilege capabilities.

While the ideal is for all code within the security function isolation boundary to only contain security-relevant code, it is sometimes necessary to include non-security functions within the isolation boundary as an exception.

(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

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 those resources have been released back to the information systems. The control of information in shared resources is also commonly referred to as object reuse and residual information protection. This control does not address:

(a) Information remanence, which refers to residual representation of data that has been nominally erased or removed;

(b) Covert channels (including storage and/or timing channels) where shared resources are manipulated to violate information flow restrictions; or

(c) Components within 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
OI&T, through VA-NSOC, ensures that the information system protects against or limits the effects of the types of DoS attacks by employing security safeguards (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 information system components on internal VA networks from being directly affected by DoS

attacks. Employing increased capacity and bandwidth combined with service redundancy may also reduce the susceptibility to DoS attacks.

(6) SC-6: Resource Availability (P0)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system protects the availability of resources by allocating resources by selecting (one or more): priority; quota; security safeguards.	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 Availability**. OI&T may, at their discretion, elect to limit the use of resources by priority.

(7) SC-7: Boundary Protection (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are separated from internal VA networks (See Attachment 3); and c. 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) [Withdrawn: Incorporated into SC-7]	---	---	---
(2) [Withdrawn: Incorporated into SC-7]	---	---	---
(3) *Access Points:* OI&T limits the number of external network connections to the information system.	Not Selected	X	X
(4) *External Telecommunications Services:* OI&T: a. Implements a managed interface for each external telecommunication service; b. Establishes a traffic flow policy for each managed interface; c. Protects the confidentiality and integrity of the information being transmitted across each interface; d. Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; e. Reviews exceptions to the traffic flow policy (See Attachment 2); and f. Removes exceptions that are no longer supported by an explicit mission/business need.	Not Selected	X	X
(5) *Deny by Default/Allow by Exception:* The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny-all, permit-by-exception).	Not Selected	X	X

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
(6) [Withdrawn: Incorporated into SC-7 (18)]	---	---	---
(7) *Prevent Split Tunneling for Remote Devices:* The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.	Not Selected	X	X
(8) *Route Traffic to Authenticated Proxy Servers:* The information system routes defined internal communications traffic to defined external networks through authenticated proxy servers within the managed interfaces (See Attachment 2).	Not Selected	Not Selected	X
(18) *Fail Safe*: The information system fails securely in the event of an operational failure of a boundary protection device.	Not Selected	Not Selected	X
(21) *Isolation of Information System Components:* OI&T employs boundary protection mechanisms to separate information system components supporting missions and/or business functions (See Attachment 3).	Not Selected	Not Selected	X
Baseline allocation summary	SC-7	SC-7 (3) (4)(5)(7)	SC-7 (3) (4)(5) (7)(8) (18)(21)

(a) Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks).

(b) Restricting or prohibiting interfaces within VA information systems includes, for example, restricting external web traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses.

(c) VA considers the 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 also include third-party provided access lines and other service elements. Such transmission services may represent sources of increased risk despite contract security provisions.

(d) Limiting the number of external network connections facilitates more comprehensive monitoring of inbound and outbound communications traffic. The Trusted Internet Connection (TIC) initiative is an example of limiting the number of external network connections.

(e) Deny by Default/Allow by Exception applies to both inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those connections which are essential and approved are allowed.

(f) Prevent Split Tunneling for Remote Devices is implemented within remote devices (e.g., notebook computers) through configuration settings to disable split tunneling in those devices and by preventing those configuration settings from being readily configurable by users. This control enhancement is implemented within the information system by the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device, and by prohibiting the connection if the remote device is using split tunneling. Split tunneling might be desirable by remote users to communicate with local information system resources such as printers/file servers. However, split tunneling would allow unauthorized external connections making the system more vulnerable to attack and to exfiltration of VA information. The use of VPNs for remote connections, when adequately provisioned with appropriate security controls, may provide VA with sufficient assurance that it can effectively treat these connections as non-remote connections from the confidentiality and integrity perspective. VPNs provide a means for allowing non-remote communications paths from remote devices. The use of an adequately provisioned VPN does not eliminate the need for preventing split tunneling.

(g) External networks are networks outside of VA control. A proxy server is a server (i.e., information system or application) that acts as an intermediary for clients requesting information system resources (e.g., files, connections, web pages, or services) from other organizational servers. Client requests established through an initial connection to the proxy server are evaluated to manage complexity and to provide additional protection by limiting direct connectivity. Web content filtering devices are one of the most common proxy servers providing access to the Internet.

(h) Fail secure is a condition achieved by employing information system mechanisms to ensure that in the event of operational failures of boundary protection devices at managed interfaces (e.g., routers, firewalls, guards, and application gateways residing on protected subnetworks commonly referred to as demilitarized zones), information systems do not enter into unsecure states where intended security properties no longer hold. Failures of boundary protection devices cannot lead to, or cause information external to the devices to enter the devices.

(i) Proxy servers support logging individual TCP sessions and blocking specific Uniform Resource Locators (URL), domain names, and IP addresses. Web proxies can be configured with VA-defined lists of authorized and unauthorized Web sites.

(j) OI&T can isolate information system components performing different missions and/or business functions. Such isolation limits unauthorized information flows among system components and also provides the opportunity to deploy greater levels of protection for selected components. Separating system components with boundary protection mechanisms provides the capability for increased protection of individual components and to more effectively control information flows between those components. This type of enhanced protection limits the potential harm from cyber attacks and errors. The degree of separation provided varies depending upon the mechanisms chosen.

(k) Boundary protection mechanisms include, for example, routers, gateways, and firewalls separating system components into physically separate networks or subnetworks, cross-domain devices separating subnetworks, virtualization techniques, and encrypting information flows among system components using distinct encryption keys.

(8) **SC-8: Transmission Confidentiality and Integrity (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system protects the confidentiality and/or integrity of transmitted information (See Attachment 3).	Not Selected	X	X
(1) *Cryptographic or Alternate Physical Protection:* The information system implements cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission unless otherwise protected by alternative physical safeguards (See Attachment 3).	Not Selected	X	X
Baseline allocation summary	Not Selected	SC-8 (1)	SC-8 (1)

(a) This control applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, fax machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification. Protecting the confidentiality and/or integrity of VA information can be accomplished by physical means (e.g., employing physical distribution systems) or by local means (e.g., employing encryption techniques). If an organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service (i.e., services which can be highly specialized to individual customer needs), it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality/integrity. In such situations, VA determines what types of confidentiality/integrity services are available in standard, commercial telecommunication service packages.

(b) Encrypting information for transmission protects information from unauthorized disclosure and modification. Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions which have common application in digital signatures, checksums, and message authentication codes. 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 email 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 email is not available. Email users must exercise common sense, good judgment, and propriety in the use of this government resource. Email 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 email messages. Such reviews will be handled in accordance with the Operating Unit's "Electronic Mail Review" SOP. The ISO and/or PO will provide concurrence for requests for removal of email messages when warranted.

2. Auto-forwarding of email messages to addresses outside the VA network is strictly prohibited.

3. When transmitting VA sensitive information, the VA email system will default to the most secure setting, to include non-repudiation, while providing maximum interoperability with other Federal agencies.

(e) 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 time frame. 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) See VA Directive 6609, *Mailing of Personally Identifiable and Sensitive Information*.

(9) **SC-9: Transmission Confidentiality**

Incorporated into **SC-8: Transmission Confidentiality and Integrity** control.

(10) **SC-10: Network Disconnect (P2)**

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.

(11) **SC-11: Trusted Path (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system establishes a trusted communications path between the user and the identified security functions of the system, (including authentication and re-authentication).	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**. OI&T 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
OI&T establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with requirements for the key generation, distribution, storage, access, and destruction (See Attachment 2).	X	X	X
(1) *Availability:* OI&T 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. VA defines key management requirements in accordance with applicable Federal laws, Executive Orders, directives, regulations, policies, standards, and guidance, specifying appropriate options, levels, and parameters. VA manages trust stores to ensure that only approved trust anchors are in such trust stores. This includes certificates with visibility external to VA information systems and certificates related to the internal operations of systems.

(13) **SC-13: Cryptographic Protection (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T requires that the information system implements cryptographic uses and type of cryptography required for each use in accordance with applicable Federal laws, Executive Orders, directives, policies, regulations, and standards (See Attachment 2).	X	X	X
Baseline allocation summary	SC-13	SC-13	SC-13

(a) When cryptography is required and employed within information systems, OI&T 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 transmission 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**

Incorporated into **AC-2: Account Management**, **AC-3: Access Enforcement**, **AC-5: Separation of Duties**, **AC-6: Least Privilege**, **SI-3: Malicious Code Protection**, **SI-4: Information System Monitoring**, **SI-5: Security Alerts, Advisories, and Directives**, **SI-7: Software, Firmware,** and **Information Integrity**, **SI-10: Information Input Validation controls**.

(15) **SC-15: Collaborative Computing Devices (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Prohibits remote activation of collaborative computing devices unless an exception is defined where remote activation is to be allowed (See Attachment 3); and b. 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 Information 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 (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system associates security attributes with information exchanged between information systems and between 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 **SC-16: Transmission of Security Attributes**. OI&T 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 public key certificates under an appropriate certificate policy or obtains public key certificates from an approved service provider (See Attachment 2).	Not Selected	X	X
Baseline allocation summary	Not Selected	SC-17	SC-17

For all certificates, VA manages information system trust stores to ensure only approved trust anchors are in the trust stores. This control addresses both certificates with visibility external to VA's information system and certificates related to the internal operations of systems, for example, application-specific time services.

(18) **SC-18: Mobile Code (P2)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Defines acceptable and unacceptable mobile code and mobile code technologies; b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and c. 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) OI&T and Operating Units implementing mobile code must ensure compliance with the current version of NIST SP 800-19, *Mobile Agent Security*, and NIST 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, PDAs and other personal handheld devices, information management systems, 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 and must be protected from malicious agents and hosts. NIST currently has a project in progress to evaluate security countermeasures to attacks from malicious mobile code.

(b) Decisions regarding the employment of mobile code within VA information systems are based on the potential for the code to cause damage to the systems 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 servers and mobile code downloaded and executed on individual workstations (e.g., smartphones). Mobile code policy and procedures address preventing the development, acquisition, or introduction of unacceptable mobile code within VA information systems.

(19) **SC-19: Voice Over Internet Protocol (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if used maliciously; and b. 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 Information System Owners implement protective measures consistent with the requirements in the current version of NIST 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
OI&T: a. Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and b. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.	X	X	X
(1) [Withdrawn: Incorporated into SC-20]	---	---	---
Baseline allocation summary	SC-20	SC-20	SC-20

(a) This control enables external clients, including, for example, remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. Information systems that provide name and address resolution services include, for example, domain name system servers. Additional artifacts include, for example, domain name system security digital signatures and cryptographic keys. Domain name system 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.

(b) An example of the means to indicate the security status of child zones includes, for example, the use of delegation signer resource records in the domain name system.

(c) The domain name system security controls reflect (and are referenced from) OMB Memorandum M-08-23, *Securing the Federal Government's Domain Name System Infrastructure*.

(21) **SC-21: Secure Name/Address Resolution Service (Recursive or Caching Resolver) (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system requests and authorizes the performance of data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.	X	X	X
Baseline allocation summary	SC-21	SC-21	SC-21

(a) Each client of name resolution services either performs this validation on its own, or has authenticated channels to trusted validation providers.

(b) Information systems that provide name and address resolution services for local clients include, for example, recursive resolving or caching domain name system servers.

(c) Domain name system client resolvers either perform validation of domain name system security signatures, or clients use authenticated channels to recursive resolvers that perform such validations.

(d) Information systems that use technologies other than the domain name server to map between host names, 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 VA are fault-tolerant and implement internal/external role separation.	X	X	X
Baseline allocation summary	SC-22	SC-22	SC-22

Information systems that provide name and address resolution services include, for example, domain name system servers. To eliminate single points of failure and to enhance redundancy, OI&T employs at least two authoritative domain name system servers; one configured as the primary server and the other configured as the secondary server. Additionally, OI&T typically deploys the servers in two geographically separated subnetworks (i.e., not located in the same physical facility). For role separation, domain name systems with an internal role, only process name and address resolution requests from within the organization (i.e., from internal clients). Domain name systems with an external role only process name and address resolution information requests from clients external to VA (i.e., on external networks including the Internet). VA specifies clients that can access authoritative domain name systems in a particular role (e.g., by address ranges, explicit lists).

(23) **SC-23: Session Authenticity (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system protects the authenticity of communications sessions.	Not Selected	X	X
Baseline allocation summary	Not Selected	SC-23	SC-23

This control addresses communications protection at the session, versus packet, level (e.g., sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of a communications 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.

(24) **SC-24: Fail in Known State (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system will fail to a known state for defined types of failures preserving system state information in failure (See Attachment 3).	Not Selected	Not Selected	X
Baseline allocation summary	Not Selected	Not Selected	SC-24

Failure in a known state can address security concerns in accordance with the mission/business needs of VA. Failure in a known secure state helps to prevent the loss of confidentiality, integrity, and availability of information in the event of a failure of VA's information systems or system components. Failure in a known safe state helps to 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 VA with less disruption of mission/business processes.

(25) **SC-25: Thin Nodes (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T employs information system components with 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**. OI&T may, at their discretion, elect to employ processing components that have minimal functionality and information storage.

(26) **SC-26: Honeypots (P0)**

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**. OI&T 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: Platform-Independent Applications (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system includes defined platform-independent applications.	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**. OI&T 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/or integrity of information at rest (See Attachment 2).	Not Selected	X	X
Baseline allocation summary	Not Selected	SC-28	SC-28

(a) This control addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems. System-related information requiring protection includes, for example, configurations or rule sets for firewalls, gateways, intrusion detection/prevention systems, filtering routers, and authenticator content.

(b) OI&T employs different mechanisms to achieve confidentiality and integrity protections including the use of cryptographic mechanisms and file scanning. Integrity protection can be achieved, for example, by implementing Write-Once-Read-Many technologies. OI&T also employs other security controls including; for example, secure offline storage in lieu of online storage when adequate protection of information at rest cannot otherwise be achieved and/or continuous monitoring to identify malicious code at rest.

(c) 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.

(d) 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.

(e) Database management systems used in VA will be encrypted using FIPS 140-2 (or its successor) validated encryption.

(29) **SC-29: Heterogeneity (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T employs a diverse set of information technologies for information system components 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**. OI&T may, at their discretion, elect to employ diverse information technologies.

(30) **SC-30: Concealment and Misdirection (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T employs concealment and misdirection techniques for information systems at defined time periods to confuse and mislead adversaries.	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: Concealment and Misdirection**. OI&T may, at their discretion, elect to employ virtualization techniques.

(31) **SC-31: Covert Channel Analysis (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	**MODERATE**	**HIGH**
OI&T: a. Performs a covert channel analysis to identify those aspects of communications within the information system that are potential avenues for covert storage; or timing channels; and b. Estimates the maximum bandwidth of those 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**. OI&T, may, at their discretion, elect to perform covert channel analysis.

(32) **SC-32: Information System Partitioning (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	**MODERATE**	**HIGH**
OI&T partitions the information system into information system components residing in separate physical domains or environments based on circumstances for physical separation of 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 **SC-32: Information System Partitioning**. OI&T, may, at their discretion, elect to perform information system partitioning.

(33) **SC-33: Transmission Preparation Integrity**

Incorporated into **SC-8: Transmission Confidentiality and Integrity** control.

(34) **SC-34: Non-Modifiable Executable Programs (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system at information system components: a. Loads and executes the operating environment from hardware-enforced, read-only media; and b. Loads and executes applications 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**. OI&T may, at their discretion, elect to use non-modifiable executable programs.

(35) **SC-35: Honeyclients (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system includes components that proactively seek to identify malicious Web sites and/or web-based malicious code.	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-35: Honeyclients**. OI&T may, at their discretion, elect to implement this control.

(36) **SC-36: Distributed Processing and Storage (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T distributes processing and storage across multiple physical locations.	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-36: Distributed Processing and Storage**. OI&T may, at their discretion, elect to implement this control.

(37) **SC-37: Out-of-Band Channels (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T employs out-of-band channels for the physical delivery of electronic transmission of information, information system components, or devices to designated individuals or 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 **SC-37: Out-of-Band Channels**. OI&T may, at their discretion, elect to implement this control.

(38) **SC-38: Operations Security (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T employs operations security safeguards to protect key VA information throughout the SDLC.	Not Selected	Not Selected	Not Selected
Baseline allocation summary	Not Selected	Not Selected	Not Selected

VA does not require, at this time, application of **SC-38: Operations Security**. OI&T may, at their discretion, elect to implement this control.

(39) **SC-39: Process Isolation (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system maintains a separate execution domain for each executing process.	X	X	X
Baseline allocation summary	SC-39	SC-39	SC-39

Information systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each information system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process. Maintaining separate execution domains for executing processes can be achieved, for example, by implementing separate address spaces.

(40) **SC-40: Wireless Link Protection (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system protects external and internal wireless links from types of signal parameter attacks or references to sources for 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 **SC-40: Wireless Link Protection**. OI&T may, at their discretion, elect to implement this control.

(41) **SC-41: Port and I/O Device Access (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T physically disables or removes connection ports or input/output devices on information systems or 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 **SC-41: Port and I/O Device Access**. OI&T may, at their discretion, elect to implement this control.

(42) **SC-42: Sensor Capability and Data (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system: a. Prohibits the remote activation of environmental sensing capabilities with exceptions where remote activation of sensors is allowed; and b. Provides an explicit indication of sensor use to designated class of users.	Not Selected	Not Selected	Not Selected
Baseline allocation summary	Not Selected	Not Selected	Not Selected

VA does not require, at this time, application of **SC-42: Sensor Capability and Data**. OI&T may, at their discretion, elect to implement this control.

(43) **SC-43: Usage Restrictions (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	**MODERATE**	**HIGH**
OI&T: a. Establishes usage restrictions and implementation guidance for information system components based on the potential to cause damage to the information system if used maliciously; and b. Authorizes, monitors, and controls the use of such components within 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 **SC-43: Usage Restrictions**. OI&T may, at their discretion, elect to implement this control.

(44) **SC-44: Detonation Chambers (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	**MODERATE**	**HIGH**
OI&T employs a detonation chamber capability within the information system, system component, or designated location.	Not Selected	Not Selected	Not Selected
Baseline allocation summary	Not Selected	Not Selected	Not Selected

VA does not require, at this time, application of **SC-44: Detonation Chambers**. OI&T may, at their discretion, elect to implement this control.

r. System and Information Integrity (SI)

(1) SI-1: System and Information Integrity Policy and Procedures (P1)

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Develops, documents, and disseminates to defined personnel or roles (See Attachment 2): 1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and b. Reviews and updates the current: 1. System and communications protection policy (See Attachment 2); and 2. System and communications protection procedures (See Attachment 2).	X	X	X
Baseline allocation summary	SI-1	SI-1	SI-1

VA OI&T in this Appendix has outlined VA's system security controls based on the current version of NIST 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.

(2) **SI-2: Flaw Remediation (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Identifies, reports, and corrects information system flaws; b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; c. Installs security-relevant software and firmware updates within a defined time period of the release of the updates (See Attachment 2); and d. Incorporates flaw remediation into the VA configuration management process.	X	X	X
(1) *Central Management:* OI&T centrally manages the flaw remediation process.	Not Selected	Not Selected	X
(2) *Automated Flaw Remediation Status:* OI&T employs automated mechanisms to determine the state of information system components with regard to flaw remediation (See Attachment 2).	Not Selected	X	X
Baseline allocation summary	SI-2	SI-2 (2)	SI-2 (1)(2)

(a) OI&T identifies information systems affected by announced software flaws including potential vulnerabilities resulting from those flaws, and reports this information to designated personnel with information security responsibilities. Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures. VA addresses flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. VA takes advantage of resources such as the Common Weakness Enumeration or Common Vulnerabilities and Exposures databases in remediating flaws discovered in VA information systems. By incorporating flaw remediation into ongoing configuration management processes, required/anticipated remediation actions can be tracked and verified. Flaw remediation actions that can be tracked and verified include, for example, whether VA follows US-CERT guidance and Information Assurance Vulnerability Alerts.

(b) VA has a Patch and Vulnerability Management Program managed by the PVT. The PVT operates under a charter approved by OI&T 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 NIST SP 800-40, *Creating a Patch and Vulnerability Management Program.*

(c) OI&T 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) OI&T management defines the scope of system patching responsibilities for the PVT. The PVT is responsible for standard system configurations that are managed by OI&T 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 Information 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. OI&T 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 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) OI&T continuously monitors for vulnerabilities and identifies available and required patches for VA systems.

(g) When patches are not available or cannot be applied because of their impact on availability, features, or functionality, OI&T will develop a short-term set of compensating controls and a long-term data and application migration plan to move to newer platforms, hardware, and/or technologies where patches can be applied and new security features can be enabled.

(h) OI&T continuously monitors for threat, vulnerability, and remediation related information and disseminates the information internally as needed.

(i) OI&T 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.

(j) OI&T 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.

(k) OI&T will follow a phased approach in implementing security patches. OI&T will start with testing and applying patches to standard desktop and server systems with a common platform build, followed by testing and applying patches to non-standard and one-off platform builds, and finally testing and applying patches to legacy and antiquated platforms, where possible.

(l) OI&T 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.

(m) OI&T ensures all appropriate documentation has been updated to reflect the patch prior to release.

(n) OI&T uses a VA-approved standard suite of automated patch management tools across the enterprise to expedite the distribution of patches to systems.

(o) OI&T deploys patches and remediation promptly and in accordance with PVT developed procedures.

(p) OI&T verifies that patches and remediations 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.

(q) 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 Information System Owners. The Information System Owner or administrator will assess the applicability of the information to his or her systems or applications.

(r) OI&T provides role-based training to OI&T staff and Administration System Owners involved in the patch and remediation effort, and to end users as appropriate.

(s) OI&T consistently measures the effectiveness of the Patch and Vulnerability Management Program and applies corrective actions, as necessary.

(t) OI&T assesses and mitigates the risks associated with deploying enterprise patch management tools.

(u) OI&T will approve standardized, secure configuration baseline for IT resources used within VA, whenever possible. See control **CM-2: Baseline Configuration** for requirements for developing, documenting and maintaining under configuration control a current baseline configuration of the information system.

(v) OI&T may provide additional guidance and expectations for identifying and remediating system flaws.

(3) **SI-3: Malicious Code Protection (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; b. Updates malicious code protection mechanisms whenever new releases are available in accordance with VA configuration management policy and procedures; c. Configures malicious code protection mechanisms to perform periodic scans of the information system and real-time scans of files from external sources at endpoint and/or network entry/exit points as the files are downloaded, opened, or executed in accordance with VA security policy and takes identified action in response to malicious code detection (See Attachment 2); and d. 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) *Central* Management: OI&T centrally manages malicious code protection mechanisms.	Not Selected	X	X
(2) *Automatic Updates:* The information system automatically updates malicious code protection mechanisms (including signature definitions).	Not Selected	X	X
(3) [Withdrawn: Incorporated into AC-6 (10)]	---	---	---
Baseline allocation summary	SI-3	SI-3 (1)(2)	SI-3 (1)(2)

(a) Information system entry and exit points include, for example, firewalls, email servers, web servers, proxy servers, remote access servers, workstations, notebook computers, and mobile devices.

(b) Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using steganography. Malicious code can be transported by different means including, for example, web accesses, email, email attachments, and portable storage devices. Malicious code insertions occur through the exploitation of information system vulnerabilities.

(c) Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code attacks. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf 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 cannot always detect such code. In these situations, VA relies instead on other safeguards including; 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. OI&T may determine that in response to the detection of malicious code, different actions may be warranted. For example, OI&T can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads, and/or actions in response to detection of maliciousness when attempting to open or execute files.

(d) Central management is the VA-wide management and implementation of malicious code protection mechanisms. Central management includes, planning, implementing, assessing, authorizing, and monitoring the VA-defined, centrally managed malicious code protection security controls.

(e) Malicious code protection mechanisms include, for example, signature definitions. Due to information system integrity and availability concerns, VA will give careful consideration to the methodology used to carry out automatic updates.

(4) **SI-4: Information System Monitoring (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with monitoring objectives (See Attachment 3); and 2. Unauthorized local, network, and remote connections. b. Identifies unauthorized use of the information system through techniques and methods (See Attachment 2); c. Deploys monitoring devices: 1. Strategically within the information system to collect VA-determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to VA; d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; e. 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	X	X	X

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
Nation based on law enforcement information, intelligence information, or other credible sources of information; f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable Federal laws, Executive Orders, directives, policies, or regulations; and g. Provides information system monitoring information to designated organizational officials/positions as needed and/or at a defined frequency (See Attachment 3).			
(2) *Automated Tools for Real-Time Analysis:* OI&T employs automated tools to support near real-time analysis of events.	Not Selected	X	X
(4) *Inbound and Outbound Communications Traffic:* The information system monitors inbound and outbound communications traffic for unusual or unauthorized activities or conditions (See Attachment 2).	Not Selected	X	X
(5) *System-Generated Alerts*: The information system alerts designated organizational officials/positions when indications of compromise or potential compromise occur (See Attachment 3).	Not Selected	X	X
(6) [Withdrawn: Incorporated into AC-6 (10)]	---	---	---
Baseline allocation summary	SI-4	SI-4 (2)(4)(5)	SI-4 (2)(4)(5)

(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 information system. OI&T can monitor information systems, for example, by observing audit activities in real-time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives may guide determination of events. Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, 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 objectives. An example of a specific type of transaction of interest to VA with regard to monitoring is HTTP traffic that bypasses organizational HTTP proxies. Output from system monitoring serves as input to continuous monitoring and incident response programs.

(b) Automated tools include, for example, host-based, network-based, transport-based, or storage-based event monitoring tools or Security Information and Event Management

technologies that provide real-time analysis of alerts and/or notifications generated by VA information systems.

(c) Unusual/unauthorized activities or conditions related to information system inbound and outbound communications include, for example, internal traffic that indicates the presence of malicious code within VA information systems or propagating among system components, the unauthorized exporting of information, or signaling to external information systems. Evidence of malicious code is used to identify potentially compromised information systems or information system components.

(d) Alerts may be generated from a variety of sources, including, 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. Alerts can be transmitted, for example, by telephone, email messages, or text messages. VA personnel on the notification list can include, for example, system administrators, mission/business owners, Information System Owners, or ISOs.

(5) **SI-5: Security Alerts, Advisories, and Directives (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Receives information system security alerts, advisories, and directives from external organizations on an ongoing basis (See Attachment 2); b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to select (one or more): designated organizational officials/positions; elements within VA; and/or external organizations as designated by the Information System Owner (See Attachment 3); and d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.	X	X	X
(1) *Automated Alerts and Advisories:* OI&T employs automated mechanisms to make security alert and advisory information available throughout VA.	Not Selected	Not Selected	X
Baseline allocation summary	SI-5	SI-5	SI-5 (1)

(a) 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 effects on VA operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner.

(b) The significant number of changes to VA information systems and the environments in which those systems operate requires the dissemination of security-related information to a variety of VA entities that have a direct interest in the success of VA missions and business functions. Based on the information provided by the security alerts and advisories, changes may be required at one or more of the three tiers related to the management of information security risk including the governance level, mission/business process/EA level, and the information system level.

(6) **SI-6: Security Function Verification (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system: a. Verifies the correct operation of security functions (See Attachment 3); b. Performs the verification at system transitional states, upon command by user with appropriate privilege, and/or at a defined frequency (See Attachment 3); c. Notifies designated organizational officials/positions of failed security verification tests (See Attachment 3); and d. Shuts the information system down, restarts the information system, and/or defines alternative actions when anomalies are discovered (See Attachment 3).	Not Selected	Not Selected	X
Baseline allocation summary	Not Selected	Not Selected	SI-6

Transitional states for information systems include, for example, system startup, restart, shutdown, and abort. Notifications provided by information systems include, for example, electronic alerts to system administrators, messages to local computer consoles, and/or hardware indications such as lights.

(7) **SI-7: Software, Firmware, and Information Integrity (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T employs integrity verification tools to detect unauthorized changes to software, firmware, and information (See Attachment 3).	Not Selected	X	X
(1) *Integrity Checks:* The information system performs an integrity check of software, firmware, and information at startup, at defined transitional states or security-relevant events and/or at a defined frequency (See Attachment 3).	Not Selected	X	X
(2) *Automated Notifications of Integrity Violations:* OI&T employs automated tools that provide notification to designated organizational officials/positions upon discovering discrepancies during integrity verification (See Attachment 3).	Not Selected	Not Selected	X

(5) *Automated Response to Integrity Violations:* The information system automatically shuts down, restarts, and/or implements security safeguards when integrity violations are discovered (See Attachment 3).	Not Selected	Not Selected	X
(7) *Integration of Detection and Response:* OI&T incorporates the detection of unauthorized security-relevant changes to the information system into VA incident response capability (See Attachment 3).	Not Selected	X	X
(14) *Binary or Machine Executable Code:* OI&T: a. Prohibits the use of binary or machine executable code from sources with limited or no warranty and without the provision of source code; and b. Provides exceptions to the source code requirement only for compelling mission/operational requirements and with the approval of the AO.	Not Selected	Not Selected	X
Baseline allocation summary	Not Selected	SI-7 (1)(7)	SI-7 (1)(2)(5) (7)(14)

(a) VA information must be protected from unauthorized changes.

(b) Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity (e.g., tampering). Software includes, for example, operating systems (with key internal components such as kernels, drivers), middleware, and applications. Firmware includes, for example, the Basic Input Output System. Information includes metadata such as security attributes associated with information. State-of-the-practice integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools can automatically monitor the integrity of information systems and hosted applications.

(c) Security-relevant events include, for example, the identification of a new threat to which VA information systems are susceptible, and the installation of new hardware, software, or firmware. Transitional states include, for example, system startup, restart, shutdown, and abort.

(d) The use of automated tools to report integrity violations and to notify OI&T personnel in a timely matter is an essential precursor to effective risk response. Personnel having an interest in integrity violations include, for example, mission/business owners, Information System Owners, systems administrators, software developers, systems integrators, and ISOs.

(e) OI&T may define different integrity-checking and anomaly responses: (i) by type of information (e.g., firmware, software, user data); (ii) by specific information (e.g., boot firmware, boot firmware for specific types of machines); or (iii) a combination of both. Automatic implementation of specific safeguards within VA information systems includes, for example, reversing the changes, halting the information system, or triggering audit alerts when unauthorized modifications to critical security files occur.

(f) Integration of Detection and Response helps to ensure that detected events are tracked, monitored, corrected, and available for historical purposes. Maintaining historical records is important both for being able to identify and discern adversary actions over an extended period of time and for possible legal actions. Security-relevant changes include, for example, unauthorized changes to established configuration settings or unauthorized elevation of information system privileges.

(g) Binary or Machine Executable Code applies to all sources of binary or machine executable code including, for example, commercial software/firmware and open source software. OI&T assesses software products without accompanying source code from sources with limited or no warranty for potential security impacts. The assessments address the fact that these types of software products may be very difficult to review, repair, or extend given that VA, in most cases, does not have access to the original source code and there may be no owners who could make such repairs on VA's behalf.

(8) **SI-8: Spam Protection (P2)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and b. Updates spam protection mechanisms when new releases are available in accordance with VA configuration management policy and procedures.	Not Selected	X	X
(1) *Central Management:* OI&T centrally manages spam protection mechanisms.	Not Selected	X	X
(2) *Automatic Updates:* The information system automatically updates spam protection mechanisms.	Not Selected	X	X
Baseline allocation summary	Not Selected	SI-8 (1)(2)	SI-8 (1)(2)

Information system entry and exit points include, for example, firewalls, email servers, web servers, proxy servers, remote access servers, workstations, mobile devices, and notebook/laptop computers. Spam can be transported by different means including, for example, email, email attachments, and web accesses. Spam protection mechanisms include, for example, signature definitions.

(9) **SI-9: Information Input Restrictions**

Incorporated into **AC-2: Account Management**, **AC-3: Access Enforcement**, **AC-5: Separation of Duties**, **AC-6: Least Privilege** controls.

(10) **SI-10: Information Input Validation (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system checks validity of information inputs (See Attachment 3).	Not Selected	X	X
Baseline allocation summary	Not Selected	SI-10	SI-10

OI&T establishes rules for checking valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, and acceptable values) to ensure that they are in place and to verify that inputs match specified definitions for format and content. Prescreening inputs prior to passing to interpreters prevents the content from being unintentionally interpreted as commands. Input validation helps to ensure accurate and correct inputs and prevent attacks such as cross-site scripting and a variety of injection attacks.

(11) **SI-11: Error Handling (P2)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system: a. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and b. Reveals error messages only to designated organizational officials/positions (See Attachment 3).	Not Selected	X	X
Baseline allocation summary	Not Selected	SI-11	SI-11

The structure and content of error messages are carefully considered by OI&T. The extent to which the information system is able to identify and handle error conditions is guided by OI&T operational procedural requirements.

(12) **SI-12: Information Handling and Retention (P2)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
VA handles and retains information within the information system and information output from the system in accordance with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	X	X	X
Baseline allocation summary	SI-12	SI-12	SI-12

Information handling and retention requirements cover the full life cycle of information, in some cases extending beyond the disposal of the information systems. NARA provides guidance on records retention.

(13) **SI-13: Predictable Failure Prevention (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T: a. Determines mean time to failure for information system components in specific environments of operation; and b. Provides substitute information system components and a means to exchange active and standby components at mean time failure substitution criteria.	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**. OI&T may, at their discretion, elect to ensure that information systems appropriately support and maintain the binding of security attributes and settings.

(14) **SI-14: Non-Persistence (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
OI&T implements non-persistent information system components and services that are initiated in a known state and terminated upon end of session of use and/or periodically at a defined frequency.	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-14: Non-Persistence**. OI&T may, at their discretion, elect to implement this control.

(15) **SI-15: Information Output Filtering (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system validates information output from software programs and/or applications to ensure that the information is consistent with the expected content.	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-15: Information Output Filtering**. OI&T may, at their discretion, elect to implement this control.

(16) **SI-16: Memory Protection (P1)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system implements security safeguards to protect its memory from unauthorized code execution (See Attachment 3).	Not Selected	X	X
Baseline allocation summary	Not Selected	SI-16	SI-16

Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can either be hardware-enforced or software-enforced with hardware providing the greater strength of mechanism.

(17) **SI-17: Fail-Safe Procedures (P0)**

NIST SP 800-53	APPLICABILITY		
	LOW	MODERATE	HIGH
The information system implements fail-safe procedures when failure conditions occur.	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-17: Fail-Safe Procedures**. OI&T may, at their discretion, elect to implement this control.

This page is intentionally blank for the purpose of printing front and back copies.

DEPARTMENT OF VETERANS AFFAIRS

VA INFORMATION PROTECTION

VA SYSTEM SECURITY CONTROLS

ATTACHMENT 1

OWNERS AND ORGANIZATION-DEFINED PARAMETERS (ODP)

COMMON CONTROLS

This attachment contains OI&T's Program Management Controls. Program Management Controls are considered common controls as they are applicable to all OI&T systems and are the responsibility of OI&T management for implementation and management. OI&T may identify additional controls as "common controls" based on the implementation responsibility of the controls (agency, region, facility). These are identified within the VA-approved FISMA database.

COMMON CONTROLS

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	Value (if required)	Owner
PM-1	H, M, L	**Program Management – Information Security Program Plan** OI&T: 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) Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance; (iii) Reflects coordination among organizational entities for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and (iv) Is approved by the Assistant Secretary for OI&T 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 VA-wide information security program plan [organization-defined frequency]; c. Updates the plan to address organizational changes and problems identified during plan implementation or SCAs; and d. Protects the information security program plan from unauthorized disclosure and modification.	Every 5 years per VA Directive 6330 and VA Handbook 6330, *Directives Management Procedures* VA Directive and Handbook 6500 as well as other 6500 series handbooks fulfill this control.	DAS for the Office of Information Security
PM-2	H, M, L	**Program Management – Senior Information Security Officer** OI&T appoints a CISO with the mission and resources to coordinate, develop, implement, and maintain a VA-wide information security program.	DAS for Information Security	Assistant Secretary for OI&T
PM-3	H, M, L	**Program Management – Information Security Resources** OI&T: 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.		OI&T Resource Management

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	Value (if required)	Owner
PM-4	H, M, L	**Program Management – Plan of Action and Milestones Process** OI&T: a. Implements a process for ensuring that POA&Ms for the security program and the associated VA information systems: (i) Are developed and maintained; (ii) Document the remedial information security actions to adequately respond to risk to VA operations and assets, individuals, other organizations, and the Nation; and (iii) Are reported in accordance with OMB FISMA reporting requirements. b. Reviews POA&Ms for consistency with VA risk management strategy and VA-wide priorities for risk response actions.	VA-approved FISMA database	OI&T OCS
PM-5	H, M, L	**Program Management – Information System Inventory** OI&T develops and maintains an inventory of its information systems.	OI&T Information System Inventory	OI&T Service Delivery and Engineering OI&T OCS
PM-6	H, M, L	**Program Management – Information Security Measures of Performance** OI&T develops, monitors, and reports on the results of information security measures of performance.		OI&T Information Security Office
PM-7	H, M, L	**Program Management – Enterprise Architecture** OI&T develops EA with consideration for information security and the resulting risk to VA operations and assets, individuals, other organizations, and the Nation.		OI&T Architecture, Strategy, and Design
PM-8	H, M, L	**Program Management – Critical Infrastructure Plan** OI&T addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.		OI&T Service Delivery and Engineering OI&T Business Continuity
PM-9	H, M, L	**Program Management – Risk Management Strategy** OI&T: a. Develops a comprehensive strategy to manage risk to VA operations and assets, individuals, other organizations, and the		OI&T Director Enterprise Risk

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	Value (if required)	Owner
		Nation associated with the operation use of information systems; b. Implements the risk management strategy consistently across VA; and c. Reviews and updates the risk management strategy as required, to address organizational changes.		Management
PM-10	H, M, L	**Program Management – Security Authorization Process** OI&T: a. Manages (i.e., documents, tracks, and reports) the security state of organizational information systems and the environments in which those systems operate 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 risk management program.		OI&T OCS
PM-11	H, M, L	**Program Management – Mission/Business Process Definition** OI&T: 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 achievable protection needs are obtained.		VHA, VBA and NCA with OI&T, Service Delivery and Engineering
PM-12	H, M, L	**Program Management – Insider Threat Program** OI&T implements an insider threat program that includes a cross-discipline insider threat incident handling team.		VA-NSOC, OCS, and Enterprise Risk Management
PM-13	H, M, L	**Program Management – Information Security Workforce** OI&T establishes an information security workforce development and improvement program.		OI&T Resource Management
PM-14	H, M, L	**Program Management – Testing, Training, and Monitoring** OI&T: a. Implements a process for ensuring that VA plans for conducting security testing, training, and monitoring activities associated with VA information systems: (i) Are developed and maintained; and (ii) Continue to be executed in a timely manner; b. Reviews testing, training, and monitoring plans for		OIS

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	Value (if required)	Owner
		consistency with the VA risk management strategy and VA-wide priorities for risk response actions.		
PM -15	H, M. L	**Program Management – Contacts With Security Groups and Associations** OI&T establishes and institutionalizes contact with selected groups and associations within the security community: a. To facilitate ongoing security education and training for VA personnel; b. To maintain currency with recommended security practices, techniques, and technologies; and c. To share current security-related information including threats, vulnerabilities, and incidents.		DAS for OIS
PM-16	H, M, L	**Program Management – Threat Awareness Program** OI&T implements a threat awareness program that includes a cross-VA information-sharing capability.		VA-NSOC

This page is intentionally blank for the purpose of printing front and back copies.

DEPARTMENT OF VETERANS AFFAIRS

VA INFORMATION PROTECTION

VA SYSTEM SECURITY CONTROLS

ATTACHMENT 2

ORGANIZATION-DEFINED PARAMETERS (ODP)

HYBRID CONTROLS

This attachment contains VA parameters and values for security controls that NIST allows agencies to determine based on the agency's mission and business needs. Part of the control is considered common (control value is based on NIST and VA policy requirements and is applicable for all VA systems); however, the implementation of the control remains the responsibility of the field either at the national, regional or at the facility system level. In addition to the controls identified in this Attachment, controls defined within Appendix F that are not identified as common controls in Attachment 1 or system-specific controls in Attachment 3 are hybrid controls. The values provided in Appendix F and this attachment will be implemented, but tailoring is permitted for controls in this attachment, when an approved OIS RBD has been obtained from the DAS for OIS and is documented in the SSP in the VA-approved FISMA database.

HYBRID CONTROLS

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	Value
AC-1	H, M, L	**Access Control Policy and Procedures** OI&T develops, documents, and disseminates to defined personnel or roles: 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the access control policy and associated access controls; and	Policies are disseminated enterprise-wide. Procedures are disseminated to those responsible for implementing the requirements.
AC-1	H, M, L	**Access Control Policy and Procedures** Reviews and updates the current access control policy.	Every 5 years per VA Directive and Handbook 6330. 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.
AC-1	H, M, L	**Access Control Policy and Procedures** Reviews and updates the current access control procedures.	The field develops and maintains SOPs as needed.
AC-2	H, M, L	**Account Management** The Information System Owner, local CIO, or designee will identify and select types of information system accounts to support VA missions/business functions.	Specify account types as: 1. User Accounts; 2. Privileged Accounts; 3. Service Accounts; 4. Training Accounts; 5. Temporary; and 6. Emergency.
AC-2	H, M, L	**Account Management** The Information System Owner, local CIO, or designee will require approvals by designated organizational officials/positions for requests to create information system accounts.	System administrator or designee creates accounts upon approval of user's supervisor and CIO.
AC-2	H, M, L	**Account Management** The Information System Owner, local CIO, or designee will create, enable, modify, disable, and remove information system accounts in accordance with VA procedures or conditions.	VA procedures defined within this control and local SOPs.

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	Value
AC-2	H, M, L	**Account Management** The Information System Owner, local CIO, or designee will review accounts for compliance with account management requirements.	User Accounts: At least semi-annually or a frequency approved in the SSP VistA Menu Reviews (Supervisor): At least every 6 months Other Account Reviews: Frequency determined by the Information System Owner and approved in the SSP
AC-2 (2)	H, M	**Account Management – Removal of Temporary/Emergency Accounts** OI&T ensures information systems automatically remove or disable temporary and emergency accounts after use is no longer required.	Temporary Accounts: An automated termination (removal) date will be established at the time of creating the account. Emergency Accounts: Will be removed/terminated immediately upon conclusion of the emergency situation.
AC-2 (3)	H,M	**Account Management – Disable Inactive Accounts** OI&T ensures the information system automatically disables inactive accounts.	After 90 days of inactivity Accounts should be terminated based on the SOPs developed by OI&T.
AC-2 (5)	H	**Account Management – Inactivity Logout** VA requires that users log out when a time period of expected inactivity has occurred or describes when to log out.	The user has completed their required input. Users should 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.
AC-2 (13)	H	**Account Management – Disable Accounts for High-Risk Individuals** OI&T disables accounts of users posing a significant risk within a defined time period of discovery of the risk.	Immediately, after notification.
AC-4	H, M	**Information Flow Enforcement** The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on information flow control policies.	VA-NSOC flow control policy (for example: keeping export-controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within VA, restricting web requests to the Internet that are not from the internal web proxy server, limiting information transfers between organizations based on data structures and content).

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	Value
AC-6 (5)	H, M	**Least Privilege – Privileged Accounts** OI&T restricts privileged accounts on the information system to designated officials/positions.	Individuals who have been approved by their supervisor, the ISO, and the Information System Owner via OI&T's approved process. This process will ensure the user has received the necessary approvals, has the appropriate background investigation, signed the Elevated Privileges ROB, and has taken the required TMS training for elevated privileges.
AC-8	H, M, L	**System Use Notification** The information system displays to users a 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, directives, policies, regulations, standards, and guidance.	Message outlined in AC-8 of VA Handbook 6500
AC-8	H, M, L	**System Use Notification** The information system, for publicly accessible systems displays system use information conditions, before granting further access.	At logon
AC-17 (3)	H, M	**Remote Access – Managed Access Control Points** The information system routes all remote accesses through managed network access control points.	VA-approved Trusted Internet Connection gateways or approved connections
AC-19 (5)	H, M	**Access Control for Mobile Devices – Full-Device/Container-Based Encryption** OI&T employs full-device encryption or container encryption to protect the confidentiality and integrity of information on mobile devices.	Full-device or container encryption TRM approved mobile devices
CM-(2)	H, M	**Use of External Information Systems – Portable Storage Devices** OI&T restricts or prohibits the use of VA-controlled portable storage devices by authorized individuals on external information systems.	See AC-19 (h) for restrictions on VA portable storage devices.
AC-21	H, M	**Information Sharing** VA 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 information-sharing circumstances where user discretion is required.	Information System Owners ensure that VA Privacy requirements and other VA requirements (VHA, VBA, NCA mission/business processes) for sharing information have been met prior to enabling the sharing of the data electronically. Examples of documents to review: Data Use Agreements, MOU/ISAs, Contracts.

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	Value
AC-21	H, M	**Information Sharing** VA employs automated mechanisms or manual processes to assist users in making information-sharing/collaboration decisions.	POs use a manual process to review/approve the sharing of data to ensure there is legal authority to share the data and VA privacy requirements are being met.
AT-1	H, M, L	**Awarenes and Training Policy and Procedures** OI&T develops, documents, and disseminates to defined personnel or roles: 1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.	Policies are disseminated enterprise-wide. Procedures are disseminated to those responsible for implementing the requirements.
AT-1	H, M, L	**Awareness and Training Policy and Procedures** OI&T reviews and updates the current security awareness and training policy.	Every 5 years per VA Directive and Handbook 6330. 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.
AT-1	H, M, L	**Awareness and Training Policy and Procedures** OI&T reviews and updates the current: Security awareness and training procedures.	The field develops and maintains SOPs as needed.
AT-2	H, M, L	**Security Awareness Training** OI&T provides basic security awareness training to all users (including managers, senior executives, and contractors) of VA information systems or VA information at a defined frequency.	Annually (within a 365 day period)
AT-3	H, M, L	**Role-Based Security Training** OI&T provides role-based security training to personnel with assigned security roles and responsibilities at a defined frequency.	Individuals with significant security responsibilities will be assigned role-based training based upon individual needs identified by employee self-assessment and supervisor validation of the self-assessment.
AT-4	H, M, L	**Security Training Records** VA and OI&T retain individual training records for a defined time period.	7 years

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	Value
AU-1	H, M, L	**Audit and Accountability Policy and Procedures** OI&T develops, documents, and disseminates to defined personnel or roles: 1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	Policies are disseminated enterprise-wide. Procedures are disseminated to those responsible for implementing the requirements.
AU-1	H, M, L	**Audit and Accountability Policy and Procedures** OI&T reviews and updates the current audit and accountability policy.	Every 5 years per VA Directive and Handbook 6330. 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.
AU-1	H, M, L	**Audit and Accountability Policy and Procedures** OI&T **r**eviews and updates the current audit and accountability procedures.	The field develops and maintains SOPs as needed.
AU-11	H, M, L	**Audit Record Retention** OI&T retains audit records for a defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and VA information retention requirements.	A minimum of 1 year or as documented in the NARA retention periods, HIPAA legislation (for VHA), or whichever is greater. Audit logs which describe a security breach must be maintained for 6 years (HIPAA requirement).
CA-1	H, M, L	**Security Assessment and Authorization Policy and Procedures** OI&T develops, documents, and disseminates to defined personnel or roles: 1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	Policies are disseminated enterprise-wide. Procedures are disseminated to those responsible for implementing the requirements.
CA-1	H, M, L	**Security Assessment and Authorization Policy and Procedures** OI&T reviews and updates the current security assessment and authorization policy.	Every 5 years per VA Directive and Handbook 6330. 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.

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	Value
CA-1	H, M, L	**Security Assessment and Authorization Policy and Procedures** OI&T reviews and updates the current security assessment and authorization procedures.	The field develops and maintains SOPs as needed.
CA-2	H,M,L	**Security Assessments** OI&T assesses the security controls in the information system and its environment of operation to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the established security requirements.	1. Prior to receiving initial authorization; 2. When a significant change in the system or major change in the data requires reauthorization; and 3. Continuously based on requirements of the Information Security Continuous Monitoring program.
CA-2	H, M, L	**Security Assessments** OI&T provides the results of the SCA to designated organizational officials/positions.	SCA results should be sent to the Information System Owner, project manager, ISO, key system stakeholders, and OCS staff.
CA-2 (1)	H, M	**Security Assessments – Independent Assessors** OI&T employs independent assessors or assessment teams with an organization-defined level of independence to conduct SCAs.	External assessors or internal assessors outside of OIS
CA-2 (2)	H	**Security Assessments – Specialized Assessments** OI&T includes as part of SCAs, other types of testing.	As part of initial security authorizations and the continuous monitoring process where the frequency is determined by the Information Security Continuous Monitoring program, OIS in conjunction with Service Delivery and Engineering performs announced and unannounced assessments, either in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessments; performance/load testing.
CA-3	H, M, L	**System Interconnections** OI&T reviews and updates ISAs.	Annually
CA-3 (5)	H, M	**System Interconnections – Restrictions on External Network Connections** OI&T employs policy for allowing information systems to connect to external information systems.	Permit-by-exception for VA-owned systems
CA-5	H, M, L	**Plan of Action and Milestones** OI&T updates existing POA&Ms based on the findings from SCAs, security impact analyses, and continuous monitoring activities.	At least quarterly
CA-6	H, M, L	**Security Authorization** VA updates the security authorization.	Ongoing authorization through implementation of the Information Security Continuous Monitoring program and when a significant change in the system or major change in the data occurs.

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	Value
CA-7	H, M, L	**Continuous Monitoring** OI&T develops a continuous monitoring strategy and implements a continuous monitoring program that includes establishment of metrics to be monitored.	Determined by the Information Security Continuous Monitoring program.
CA-7	H, M, L	**Continuous Monitoring** OI&T develops a continuous monitoring strategy and implements a continuous monitoring program that includes establishment of frequencies for monitoring and for assessments supporting such monitoring.	Risk-based tiers of security controls tested on the frequency outlined in VA's Information Security Continuous Monitoring Security Control Evaluation Plan created and maintained by OCS.
CA-7	H, M, L	**Continuous Monitoring** OI&T develops a continuous monitoring strategy and implements a continuous monitoring program that includes reporting the security status of VA and the information system to the designated organizational officials/positions.	ISO, CIO, Information System Owner receive security status report. OCS determines frequency of status reporting.
CA-7 (1)	H, M	**Continuous Monitoring – Independent Assessment** OI&T employs independent assessors or assessment teams to monitor the security controls in the information system on an ongoing basis.	The AO determines the required degree of independence for assessors for continuous monitoring.
CA-8	H	**Penetration Testing** OI&T conducts penetration testing on information systems or system components.	OI&T conducts penetration testing quarterly on one-fourth of the total number of VA High systems.
CA-9	H, M, L	**Internal System Connections** OI&T authorizes internal connections of information system components or classes of components to the information system.	All intra-system connections including mobile devices, notebook/desktop computers, printers, copiers, fax machines, scanners, sensors and servers.
CM-1	H, M, L	**Configuration Management Policy and Procedures** OI&T develops, documents, and disseminates to defined personnel or roles: 1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	Policies are disseminated enterprise-wide. Procedures are disseminated to those responsible for implementing the requirements.
CM-1	H, M, L	**Configuration Management Policy and Procedures** OI&T reviews and updates the current configuration management policy.	Every 5 years per VA Directive and Handbook 6330. 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.

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	Value
CM-1	H, M, L	**Configuration Management Policy and Procedures** OI&T reviews and updates the current configuration management procedures.	The field develops and maintains SOPs as needed.
CM-2 (7)	H, M	**Baseline Configuration – Configure Systems, Components, or Devices for High-Risk Areas** OI&T issues information systems, system components, or devices with organization-defined configurations to individuals traveling to locations that OI&T deems to be of significant risk	A mobile device with a sanitized hard drive, limited applications, and additional hardening if appropriate can be provided.
CM-2 (7)	H, M	**Baseline Configuration – Configure Systems, Components, or Devices for High-Risk Areas** OI&T applies security safeguards to the devices when the individuals return.	Upon return the device will be examined for signs of physical tampering and purging/reimaging of the hard disk drive.
CM-3	H, M	**Configuration Change Control** OI&T retains records of configuration-controlled changes to the information system.	Per NARA - 806-3 PC Baseline Management Destroy/delete records related to each specific baseline 5 years after baseline is superseded.
CM-3	H, M	**Configuration Change Control** OI&T coordinates and provides oversight for configuration change control activities through configuration change control element (e.g., committee, board) that convenes on assigned schedule.	National or local CCB that convenes as dictated by their charter or local operating procedures.
CM-3 (1)	H	**Configuration Change Control – Automated Document/Notification/Prohibition of Changes** OI&T employs automated mechanisms to notify designated approval authorities of proposed changes to the information system and request change approval.	CCB
CM-6	H, M, L	**Configuration Settings** OI&T establishes and documents configuration settings for IT products employed within the information system using security configuration checklists that reflect the most restrictive mode consistent with operational requirements.	Service Delivery and Engineering approved configuration checklists
CM-6	H, M, L	**Configuration Settings** OI&T identifies, documents, and approves any deviations from established configuration settings for information system components based on operational requirements.	VA systems; Service Delivery and Engineering and OIS requirements

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	Value
CM-7 (4)	M	**Least Functionality – Unauthorized Software/Blacklisting** The Information System Owner identifies software programs not authorized to execute on the information system.	Any software not specifically approved via the TRM process is to be considered unauthorized. The Information System Owner should: • check the TRM Web site and with Service Delivery and Engineering management as needed; • understand that any software not approved is unauthorized; • install only authorized software; and • implement security controls to ensure unauthorized software is not allowed.
CM-7 (4)	M	**Least Functionality – Unauthorized Software/Blacklisting** The Information System Owner reviews and updates the list of unauthorized software programs.	OI&T's TRM Management Team continuously reviews and updates the approved and disapproved technologies on their Web site. The workgroup meets weekly and updates their Web site on a monthly basis. Existing entries are reviewed for accuracy by their authors annually on an individual basis.
CM-7 (5)	H	**Least Functionality – Authorized Software/Whitelisting** The Information System Owner identifies software programs authorized to execute on the information system.	Any software not specifically approved via the TRM process is to be considered unauthorized. The Information System Owner should check the TRM Web site and with Service Delivery and Engineering management as needed, understand that any software not approved is unauthorized, install only authorized software, and implement security controls to ensure unauthorized software is not allowed.
CM-7 (5)	H	**Least Functionality – Authorized Software/Whitelisting** The Information System Owner reviews and updates the list of unauthorized software programs.	OI&T's TRM Management Team continuously reviews and updates the approved and disapproved technologies on their Web site. The workgroup meets weekly and updates their Web site on a monthly basis. Existing entries are reviewed for accuracy by their authors annually on an individual basis.
CM-8	H, M, L	**Information System Component Inventory** OI&T reviews and updates the information system component inventory.	Annually
CM-11	H, M, L	**User-Installed Software** OI&T establishes policies governing the installation of software by users.	Approved policies and guidance (ROB, TRM, Enterprise System Build Guides)

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	Value
CM-11	H, M, L	**User-Installed Software** OI&T enforces software installation policies through defined methods.	Limiting user ability to install software and monitoring through application whitelisting tools and compliance monitoring tools
CM-11	H, M, L	**User-Installed Software** OI&T monitors policy compliance at a defined frequency.	As part of VA's continuous monitoring processes
CP-1	H, M, L	**Contingency Planning Policy and Procedures** OI&T develops, documents, and disseminates to defined personnel or roles: 1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.	Policies are disseminated enterprise-wide. Procedures are disseminated to those responsible for implementing the requirements.
CP-1	H, M, L	**Contingency Planning Policy and Procedures** OI&T reviews and updates the current contingency planning policy.	Every 5 years per VA Directive and Handbook 6330. 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.
CP-1	H, M, L	**Contingency Planning Policy and Procedures** OI&T reviews and updates the current contingency planning procedures.	The field develops and maintains SOPs as needed.
CP-2	H, M, L	**Contingency Plan** The Information System Owner develops a contingency plan for the information system that is reviewed and approved by designated organizational officials.	Business Continuity
CP-2	H, M, L	**Contingency Plan** The Information System Owner reviews the contingency plan for the information system.	Review annually and when one or more significant changes are made.
CP-3	H, M, L	**Contingency Training** The Operating Unit provides contingency training to information system users consistent with assigned roles and responsibilities within a defined time period of assuming a contingency role or responsibility.	Complete initial training within 30 days of assuming the role
CP-3	H, M, L	**Contingency Training** The Operating Unit provides contingency training to information system users consistent with assigned roles and responsibilities at a defined frequency thereafter.	Complete at least annually thereafter

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	Value
CP-8 (4)	H	**Telecommunications Services – Provider Contingency Plan** OI&T obtains evidence of contingency testing/training by providers.	Annually or as stated in the contract
IA-1	H, M, L	**Identification and Authentication Policy and Procedures** OI&T develops, documents, and disseminates to defined personnel or roles: 1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.	Policies are disseminated enterprise-wide. Procedures are disseminated to those responsible for implementing the requirements.
IA-1	H, M, L	**Identification and Authentication Policy and Procedures** OI&T reviews and updates the current identification and authentication policy.	Every 5 years per VA Directive and Handbook 6330. 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.
IA-1	H, M, L	**Identification and Authentication Policy and Procedures** OI&T reviews and updates the current identification and authentication procedures.	The field develops and maintains SOPs as needed.
IA-2 (11)	H, M	**Identification and Authentication (Organizational Users) – Remote Access – Separate Device** The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets the strength of mechanism requirements.	FIPS 201-1 requirements apply. Non-privileged users use PIV cards and privileged accounts require certificate based authentication or one-time passcodes token authentication.
IA-5	H, M, L	**Authenticator Management** OI&T manages information system authenticators by changing/refreshing authenticators at a determined frequency.	For single-factor authentication, user accounts will be changed every 90 days. For single-factor authentication, administrator accounts should be changed at a maximum of every 30 days and will be changed at a minimum of every 90 days. Service accounts will be changed at a minimum every 3 years.

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	Value
IA-5 (1)	H, M, L	**Authenticator Management – Password-Based Authentication** The information system, for password-based authentication, enforces minimum password complexity.	Passwords must contain at least 8 non-blank characters. They must contain characters from 3 of the following 4 categories: English upper case characters, English lower case characters, Base 10 digits, and non-alphanumeric special characters. Six of the characters must not occur more than once in the password. System administrator and service accounts must contain at least 12 non-blank characters and use 3 of the 4 categories as outlined above.
IA-5 (1)	H, M, L	**Authenticator Management – Password-Based Authentication** The information system, for password-based authentication enforces at least a number of changed characters when new passwords are created.	When changing a password 4 characters must be changed from the old password to the new password.
IA-5 (1)	H, M, L	**Authenticator Management – Password-Based Authentication** The information system, for password-based authentication enforces password minimum and maximum lifetime restrictions.	See requirements for frequency for changing/refreshing authenticators.
IA-5 (1)	H, M, L	**Authenticator Management – Password-Based Authentication** The information system, for password-based authentication prohibits reuse of a password	The same password should not be used if it has been used within the past 2 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 time frame.
IA-5 (3)	H, M	**Authenticator Management – In-Person or Trusted Third-Party Registration** The Operating Unit requires the registration process to receive defined types of authenticators be conducted by a designated person or trusted third party before a designated registration authority with authorization by a designated organizational official/position.	OI&T requires that the registration process for issuance of VA identity credentials, and the verification and provisioning process for acceptance for use in VA systems of credentials issued by third parties, shall follow the procedures defined in NIST SP 800-63 for the level of assurance applicable to that credential or token.
IA-5 (11)	H, M, L	**Authenticator Management – Hardware Token-Based Authentication** The information system, for hardware token-based authentication, employs mechanisms that satisfy specific token quality requirements.	PIV card using VA's approved PKI technology.

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	Value
IA-8 (3)	H, M, L	**Identification and Authentication (Non-Organizational Users) – Use of FICAM-Approved Products** OI&T employs only FICAM-approved information system components in defined information systems to accept third-party credentials.	Externally facing web applications and services
IR-1	H, M, L	**Incident Response Policy and Procedures** OI&T develops, documents, and disseminates to defined personnel or roles: 1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls.	Policies are disseminated enterprise-wide. Procedures are disseminated to those responsible for implementing the requirements.
IR-1	H, M, L	**Incident Response Policy and Procedures** OI&T reviews and updates the current incident response policy.	Every 5 years per VA Directive and Handbook 6330. 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.
IR-1	H, M, L	**Incident Response Policy and Procedures** OI&T reviews and updates the current incident response procedures.	The field develops and maintains SOPs as needed.
IR-2	H, M, L	**Incident Response Training** OI&T provides incident response training to information system users consistent with assigned roles and responsibilities within a defined time period of assuming an incident response role or responsibility.	30 days
IR-2	H, M, L	**Incident Response Training** OI&T provides incident response training to information system users consistent with assigned roles and responsibilities for a defined frequency thereafter.	Annually
IR-3	H, M	**Incident Response Testing** OI&T tests the incident response capability for the information system at a defined frequency using specified tests to determine the incident response effectiveness and documents the results.	Annually Using simulations and test scenarios
IR-6	H, M, L	**Incident Reporting** The Operating Unit and OI&T require personnel to report suspected security/privacy incidents to his/her ISO, PO, and supervisor.	Immediately upon suspicion

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	Value
IR-6	H, M, L	**Incident Reporting** The Operating Unit and OI&T report security/privacy incident information.	To US-CERT
IR-8	H, M, L	**Incident Response Plan** The Operating Unit and OI&T develop an incident response plan that is reviewed and approved by designated organizational personnel or roles.	Information System Owner, ISO, PO, and key system stakeholders
MA-1	H, M, L	**System Maintenance Policy and Procedures** OI&T develops, documents, and disseminates to defined personnel or roles: 1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls.	Policies are disseminated enterprise-wide. Procedures are disseminated to those responsible for implementing the requirements.
MA-1	H, M, L	**System Maintenance Policy and Procedures** OI&T reviews and updates the current system maintenance policy.	Every 5 years per VA Directive and Handbook 6330. 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.
MA-1	H, M, L	**System Maintenance Policy and Procedures** OI&T reviews and updates the current system maintenance procedures.	The field develops and maintains SOPs as needed.
MA-2	H, M, L	**Controlled Maintenance** OI&T requires that defined personnel or roles explicitly approve the removal of the information system or system components from VA facilities for off-site maintenance or repairs.	Information System Owner, local CIO, or designee
MA-3 (3)	H	**Maintenance Tools – Prevent Unauthorized Removal** OI&T prevents the unauthorized removal of maintenance equipment containing VA information by obtaining an exemption from designated organizational personnel or roles explicitly authorizing removal of the equipment from the facility.	Information System Owner, local CIO, or designee

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	Value
MP-1	H, M, L	**Media Protection Policy and Procedures** OI&T develops, documents, and disseminates to defined personnel or roles: 1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls.	Policies are disseminated enterprise-wide. Procedures are disseminated to those responsible for implementing the requirements.
MP-1	H, M, L	**Media Protection Policy and Procedures** OI&T reviews and updates the current media protection policy.	Every 5 years per VA Directive and Handbook 6330. 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.
MP-1	H, M, L	**Media Protection Policy and Procedures** OI&T reviews and updates the current media protection procedures.	The field develops and maintains SOPs as needed.
MP-6	H, M, L	**Media Sanitization** The Operating Unit and OI&T sanitize information system media prior to disposal, release out of VA control, or release for reuse using defined sanitization techniques and procedures in accordance with applicable Federal and VA standards and policies.	Refer to VA Handbook 6500.1 and applicable FSS SOP for appropriate sanitization techniques and procedures for specified types of digital and non-digital information system media.
MP-6 (2)	H	**Media Sanitization – Equipment Testing** OI&T tests sanitization equipment and procedures to verify that the intended sanitization is being achieved.	Annually
MP-6 (3)	H	**Media Sanitization – Non-Destructive Techniques** OI&T applies non-destructive sanitization techniques to portable storage devices prior to connecting such devices to the information system under the identified circumstances.	Applies sanitization techniques: • When devices are first purchased from the manufacturer or vendor prior to initial use; and • When OI&T loses a positive chain of custody for the device. Sanitization requirements are based upon VA Handbook 6500.1.
MP-7	H, M, L	**Media Use** The Operating Unit restricts the use of specific types of information system media on information systems or system components using security safeguards.	Restricts unapproved, non-FIPS 140-2 validated USB devices from connecting to VA systems through the use of blocking technology.

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	Value
PE-1	H, M, L	**Physical and Environmental Protection Policy and Procedures** OI&T develops, documents, and disseminates to defined personnel or roles: 1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.	Policies are disseminated enterprise-wide. Procedures are disseminated to those responsible for implementing the requirements.
PE-1	H, M, L	**Physical and Environmental Protection Policy and Procedures** OI&T reviews and updates the current physical and environmental protection policy.	Every 5 years per VA Directive and Handbook 6330. 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.
PE-1	H, M, L	**Physical and Environmental Protection Policy and Procedures** OI&T reviews and updates the current physical and environmental protection procedures.	The field develops and maintains SOPs as needed.
PE-3	H, M, L	**Physical Access Control** The Operating Unit provides security safeguards to control access to areas within the facility officially designated as publicly accessible.	Regulatory and policy guidance for signage requirements. VA facility provides safeguards per VA physical security policy Title 38 C.F.R. § 1.218, *Security and Law Enforcement at VA Facilities*, and VA Directive and Handbook 0730 and as defined by the local facility policy. Each facility has a local implementing SOP addressing hours of operation and visitor control.
PE-3	H, M, L	**Physical Access Control** The Operating Unit escorts visitors and monitors visitor activity under identified circumstances requiring visitor escorts and monitoring.	Within VHA medical facilities, visitors are escorted and monitored after operating hours. VHA medical facilities are generally open to the public with official business (38 C.F.R. § 1.218). Within VBA regional offices, visitors are sponsored and escorted at all times. VBA Regional Offices are generally located in controlled GSA owned space. For other locations, determined by the Information System Owner and documented in the SSP.

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	Value
PE-3	H, M, L	**Physical Access Control** The Operating Unit inventories physical access devices.	Physical access control systems at the facility level Inventories are completed every 12 months.
PE-8	H, M, L	**Access Records** OI&T maintains visitor access records to the facility where the information system resides.	1 year
PL-1	H, M, L	**Security Planning Policy and Procedures** OI&T develops, documents, and disseminates to defined personnel or roles (See Attachment 2): 1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls.	Policies are disseminated enterprise-wide. Procedures are disseminated to those responsible for implementing the requirements.
PL-1	H, M, L	**Security Planning Policy and Procedures** OI&T reviews and updates the current security planning policy.	Every 5 years per VA Directive and Handbook 6330. 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.
PL-1	H, M, L	**Security Planning Policy and Procedures** OI&T reviews and updates the current security planning procedures.	The field develops and maintains SOPs as needed.
PL-2	H, M, L	**System Security Plan** The Information System Owner reviews the security plan for the information system.	Annually
PL-4	H, M, L	**Rules of Behavior** VA reviews and updates the ROB.	At least every 5 years per VA Directive and Handbook 6330, with the review and update of VA Handbook 6500
PL-8	H, M	**Information Security Architecture** The Operating Unit reviews and updates the information security architecture to reflect updates in the EA.	Annually, or whenever significant changes are made

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	Value
PS-1	H, M, L	**Personnel Security Policy and Procedures** OI&T develops, documents, and disseminates to defined personnel or roles: 1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.	Policies are disseminated enterprise-wide. Procedures are disseminated to those responsible for implementing the requirements.
PS-1	H, M, L	**Personnel Security Policy and Procedures** OI&T reviews and updates the current personnel security policy.	Every 5 years per VA Directive and Handbook 6330. 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.
PS-1	H, M, L	**Personnel Security Policy and Procedures** OI&T reviews and updates the current personnel security procedures.	The field develops and maintains SOPs as needed.
PS-2	H, M, L	**Position Risk Designation** VA reviews and updates position risk designations consistent with policy and procedures as required.	Per VA Directive and Handbook 0710
PS-3	H, M, L	**Personnel Screening** VA rescreens individuals according to policy and procedures.	Per VA Directive and Handbook 0710
PS-4	H, M, L	**Personnel Termination** The Operating Unit, upon termination of individual employment, disables information system access.	At the same time (or just before) the employee is notified of his/her dismissal or upon receipt of resignation
PS-6	H, M, L	**Access Agreements** The Operating Unit reviews and updates the access agreements.	ROB – see PL-4: Rules of Behavior Other agreements – annually or as defined in the agreement
PS-6	H, M, L	**Access Agreements** The Operating Unit ensures that individuals requiring access to VA information and information systems re-sign access agreements to maintain access to VA information systems when access agreements have been updated or at a defined frequency.	ROBs - upon the annual anniversary date of their signing of the ROB. Other agreements - dependent on the nature and wording of the specific agreement.

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	Value
PS-7	H, M, L	**Third-Party Personnel Security** VA requires third-party providers to notify designated organizational officials/positions of any personnel transfers or terminations of third-party personnel who possess VA credentials and/or badges, or who have information system privileges.	Notify CO immediately when a contractor is reassigned or leaves contractor or subcontractor's employ or prior to an unfriendly termination
PS-8	H, M, L	**Personnel Sanctions** VA notifies designated organizational officials/positions when a formal employee sanctions process is implemented, identifying the individual sanctioned and the reason for the sanction.	Employee's immediate supervisor, the ISO, and CIO immediately
RA-1	H, M, L	**Risk Assessment Policy and Procedures** OI&T develops, documents, and disseminates to defined personnel or roles: 1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.	Policies are disseminated enterprise-wide. Procedures are disseminated to those responsible for implementing the requirements.
RA-1	H, M, L	**Risk Assessment Policy and Procedures** OI&T reviews and updates the current risk assessment policy.	Every 5 years per VA Directive and Handbook 6330. 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.

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	Value
RA-1	H, M, L	**Risk Assessment Policy and Procedures** OI&T reviews and updates the current risk assessment procedures.	The field develops and maintains SOPs as needed.
RA-3	H, M, L	**Risk Assessment** The Information System Owner documents risk assessment results.	Document results in the SSP.
RA-3	H, M, L	**Risk Assessment** The Information System Owner reviews risk assessment results.	At a frequency necessary to monitor and reduce risks.
RA-3	H, M, L	**Risk Assessment** The Information System Owner updates the risk assessment at a determined 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.	Annually

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	Value
RA-5	H, M, L	**Vulnerability Scanning** OI&T remediates legitimate vulnerabilities in accordance with an organizational assessment of risk.	Per OI&T's established response times. Critical - patches will be tested and applied within 30 days High - patches will be tested and applied within 60 days Moderate - patches will be tested and applied within 90 days Low - the Information System Owner will determine the patching time frame Emergent - patches will be tested and applied as soon as possible
SA-1	H, M, L	**System and Services Acquisition Policy and Procedures** OI&T develops, documents, and disseminates to defined personnel or roles: 1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.	Policies are disseminated enterprise-wide. Procedures are disseminated to those responsible for implementing the requirements.
SA-1	H, M, L	**System and Services Acquisition Policy and Procedures** Reviews and updates the current system and services acquisition policy.	Every 5 years per VA Directive and Handbook 6330. 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.
SA-1	H, M, L	**System and Services Acquisition Policy and Procedures** Reviews and updates the current system and services acquisition procedures.	The field develops and maintains SOPs as needed.
SA-3	H, M, L	**System Development Life Cycle Support** OI&T manages the information system using a defined SDLC that incorporates information security considerations.	SDLC guidance provided by Project Management Accountability System along with ProPath

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	Value
SA-9	H, M, L	**External Information System Services** OI&T requires that providers of external information system services comply with VA information security requirements and employ security controls in accordance with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.	VA Handbook 6500, App. F security controls defined in a MOU/ISA, contract, or other agreement (e.g., Data Use Agreement) as specified in the procedures or templates provided for each of these types of agreements.
SA-9	H, M, L	**External Information System Services** OI&T employs defined processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis.	Processes, methods and techniques for oversight of security control compliance within the agreement. For contracts, COR monitors contract and contacts CIO and ISO, as appropriate for security-related issues.
SA-15	H	**Development Process, Standards, and Tools** OI&T reviews the development process, standards, tools, and tool options/configurations to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy security requirements.	Prior to initiating contract or service agreement and as required during the development process VA Handbook 6500 security requirements
SA-16	H	**Developer-Provided Training** OI&T requires the developer of the information system, system component, or information system service to provide training on the correct use and operation of the implemented security functions, controls, and/or mechanisms.	Security training and/or security documentation provided prior to hand-off of the system/application to the Information System Owner.
SC-1	H, M, L	**System and Communications Protection Policy and Procedures** OI&T develops, documents, and disseminates to defined personnel or roles: 1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.	Policies are disseminated enterprise-wide. Procedures are disseminated to those responsible for implementing the requirements.
SC-1	H, M, L	**System and Communications Protection Policy and Procedures** OI&T reviews and updates the current system and communications protection policy.	Every 5 years per VA Directive and Handbook 6330. 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.

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	Value
SC-1	H, M, L	**System and Communications Protection Policy and Procedures** OI&T reviews and updates the current system and communications protection procedures.	The field develops and maintains SOPs as needed.
SC-5	H, M, L	**Systems and Communications Protection** OI&T (through the VA-NSOC) ensures that the information systems protect against or limit the effects of DoS attacks by employing security safeguards.	Examples of safeguards include boundary protection devices that filter certain types of packets to protect information system components on internal VA networks, employing increased capacity and bandwidth combined with service redundancy.
SC-7 (4)	H, M	**Boundary Protection – External Telecommunications Services** OI&T reviews exceptions to the traffic flow policy as required and removes exceptions that are no longer supported by an explicit mission/business need.	As required, per OI&T established processes and justified needs.
SC-7 (8)	H	**Boundary Protection – Route Traffic to Authenticated Proxy Servers** The information system routes defined internal communications traffic to defined external networks through authenticated proxy servers within the managed interfaces.	OI&T-defined internal communication traffic to OI&T-defined external networks.
SC-12	H, M, L	**Cryptographic Key Establishment and Management** OI&T establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with requirements for the key generation, distribution, storage, access, and destruction.	Federal law mandating FIPS 140-2 (or its successor) validated encryption for all Federal government systems.
SC-13	H, M, L	**Cryptographic Protection** OI&T requires that the information system implements cryptographic uses and type of cryptography required for each use in accordance with applicable Federal laws, Executive Orders, directives, policies, regulations, and standards.	FIPS 140-2 validated encryption (or its successor) for VA sensitive information during transmissions and at rest when outside of VA-owned or managed facilities (e.g., medical centers, CBOCs, regional offices, etc.)
SC-17	H, M	**Public Key Infrastructure Certificates** VA issues public key certificates under an appropriate certificate policy or obtains public key certificates from an approved service provider.	VA purchases public key certificates from an approved, shared service provider.
SC-28	H, M	**Protection of Information at Rest** The information system protects the confidentiality and/or integrity of information at rest.	Confidentiality and integrity of VA sensitive information both inside and outside of VA-owned or managed facilities.

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	Value
SI-1	H, M, L	**System and Information Integrity Policy and Procedures** OI&T develops, documents, and disseminates to defined personnel or roles: 1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.	Policies are disseminated enterprise-wide. Procedures are disseminated to those responsible for implementing the requirements.
SI-1	H, M, L	**System and Information Integrity Policy and Procedures** OI&T reviews and updates the current system and communications protection policy.	Every 5 years per VA Directive and Handbook 6330. 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.
SI-1	H, M, L	**System and Information Integrity Policy and Procedures** OI&T reviews and updates the current system and communications protection procedures.	The field develops and maintains SOPs as needed.
SI-2	H, M, L	**Flaw Remediation** OI&T installs security-relevant software and firmware updates within a defined time period of the release of the updates.	See **RA-5: Vulnerability Scanning**
SI-2 (2)	H, M	**Flaw Remediation – Automated Flaw Remediation Status** OI&T employs automated mechanisms to determine the state of information system components with regard to flaw remediation.	Monthly
SI-3	H, M, L	**Malicious Code Protection** OI&T configures malicious code protection mechanisms to perform periodic scans of the information system and real-time scans of files from external sources at endpoint and/or network entry/exit points as the files are downloaded, opened, or executed in accordance with VA security policy and takes identified action in response to malicious code detection.	Daily basis with daily virus definition updates.

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	Value
SI-3	H, M, L	**Malicious Code Protection** OI&T configures malicious code protection mechanisms to takes identified action in response to malicious code detection.	Enterprise patching should be in place to correct flaws. Files from external sources should be scanned on the endpoint (anti-virus workstation agent) and at network entry and exit points (anti-virus client on servers) and the malicious code quarantined.
SI-4	H, M	**Information System Monitoring** OI&T identifies unauthorized use of the information system through techniques and methods.	Malicious code protection; intrusion detection or prevention mechanisms; boundary protection devices such as firewalls, gateways, and routers.
SI-4 (4)	H, M	**Information System Monitoring – Inbound and Outbound Communications Traffic** The information system monitors inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	Daily by inspecting and monitoring all packets inbound and outbound. Supported by tools such as host-based intrusion prevention system, network-based intrusion prevention system, firewalls, routers, switches, etc.
SI-5	H, M, L	**Security Alerts, Advisories, and Directives** OI&T receives information system security alerts, advisories, and directives from external organizations on an ongoing basis.	US-CERT: Provides flow and signature-based visibility and alerting into malicious traffic sourced from or destined to VA through the use of Einstein sensors. Other Government Agencies: VA maintains an intelligence and technique sharing relationship with other government agencies. Open source research: VA leverages a number of publicly available resources to supplement their security and threat awareness.

This page is intentionally blank for the purpose of printing front and back copies.

DEPARTMENT OF VETERANS AFFAIRS

VA SYSTEM-SPECIFIC SECURITY CONTROLS

ATTACHMENT 3
SYSTEM-SPECIFIC CONTROLS
ORGANIZATION-DEFINED PARAMETERS (ODPs)
SYSTEM-SPECIFIC CONTROLS

This Attachment contains VA parameters and values for security controls that NIST allows agencies to determine based on the agency's mission and business needs. The controls in this attachment are considered system-specific controls and should be determined by the Information System Owner, using the recommended values when possible. They may be tailored to meet the unique specifications and environment of the system as determined by the Information System Owner. When the recommended values within this attachment cannot be implemented, a LRBD must be documented in the SSP in the VA-approved FISMA database.

SYSTEM-SPECIFIC CONTROLS

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OI&T Recommended Control Value Minimums	System-Specific Control Value - TBD by Information System Owner for Secure Baseline
AC-2 (4)	H, M	**Account Management – Automated Audit Actions** OI&T employs automated mechanisms to audit account creation, modification, enabling, disabling, and removal actions and notifies designated organizational officials/positions.	Information System Owners designate within the SSP the individuals/positions that are to be notified.	[Define personnel or roles]
AC-2 (11)	H	**Account Management – Usage Conditions** The information system enforces circumstances and/or usage conditions for information system accounts.	Information System Owners identify any specific usage conditions or circumstances (e.g., days of the week, time-of-day, durations of time) for specific information system accounts.	[Define conditions or circumstances and information system accounts]
AC-2 (12)	H	**Account Management – Account Monitoring/Atypical Usage** OI&T monitors information system accounts for atypical use and reports atypical usage of information system accounts to designated organizational officials/positions.	Information System Owner determines atypical circumstances/usage conditions as appropriate for particular system and reports atypical usage to the ISO.	[Define atypical use and VA personnel or roles]
AC-5	H, M	**Separation of Duties** OI&T separates duties of individuals; documents separation of duties of individuals; and defines information system access authorizations to support separation of duties.	Separation of duties includes: 1. Dividing mission functions and information system support functions among different individuals and/or roles; 2. Conducting information system support functions with different individuals (e.g., system management, programming, configurations management, quality assurance and testing, and network security); and 3. Ensuring security personnel administering access control functions do not also administer audit functions.	[Define duties of individuals]

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OI&T Recommended Control Value Minimums	System-Specific Control Value - TBD by Information System Owner for Secure Baseline
AC-6 (1)	H, M	**Least Privilege – Authorize Access to Security Functions** OI&T explicitly authorizes access to security functions and security-relevant information.	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	**Least Privilege – Non-Privileged Access for Non-Security** OI&T 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-6 (3)	H	**Least Privilege – Network Access to Privileged Commands** OI&T authorizes network access to privileged commands only for compelling operational needs and documents the rationale for such access in the security plan for the information system.	The Information System Owner determines the network accessed privileged commands and operational needs for the specific system and documents these in the SSP.	[Define privileged commands and compelling operational needs]
AC-7	H, M, L	**Unsuccessful Logon Attempts** The information system enforces a limit of consecutive invalid logon attempts by a user during a specified time period.	Five attempts during a one hour period for Low Five attempts during a one day (24 hour) period for Moderate and High	[Define number and time period]
AC-7	H, M, L	**Unsuccessful Logon Attempts** The information system automatically takes action when the maximum number of unsuccessful attempts is exceeded.	Locks the account One hour for Low Lock out until released by Administrator for Moderate and High	[Define action]
AC-10	H	**Concurrent Session Control** The information system limits the number of concurrent sessions for each account and/or account type to a maximum number of sessions.	Information System Owner defines accounts and/or account types. Three sessions for general users and five sessions for users with elevated privileges.	[Define account and/or account type and number]

Control	**Baseline** High, Moderate, Low	Per NIST SP 800-53	OI&T Recommended Control Value Minimums	System-Specific Control Value - TBD by Information System Owner for Secure Baseline
AC-11	H, M	**Session Lock** The information system prevents further access to the system by initiating a session lock after a period of inactivity or upon receiving a request from a user.	Fifteen minutes (Requests for increased time for specific individuals will be approved by the Information System Owner, local CIO or designee.)	[Define time period]
AC-12	H, M	**Session Termination** The information system automatically terminates a user session after defined conditions or trigger events requiring session disconnect.	Information System Owner defined. Examples are period of user inactivity or targeted responses to certain types of incidents, or time-of-day restrictions on information system use.	[Define conditions or trigger events requiring session disconnect]
AC-14	H, M, L	**Permitted Actions Without Identification or Authentication** The Information System Owner identifies user actions that can be performed on the information system without identification or authentication consistent with VA missions/business functions.	Information System Owner defines, if required.	[Define user actions]
AC-17 (4)	H, M	**Remote Access – Privileged Commands/Access** OI&T authorizes the execution of privileged commands and access to security-relevant information via remote access only for defined needs.	Information System Owners define when and by whom they allow remote privileged access to their systems.	[Define needs]
AC-18 (1)	H, M	**Wireless Access – Authentication and Encryption** The information system protects wireless access to the system using authentication of users and/or devices and FIPS 140-2 (or its successor) validated encryption.	Information System Owner defines whether user, device, or both as appropriate.	[Select (one or more): users; devices]
AC-22	H, M, L	**Publicly Accessible Content** VA reviews the content on the publicly accessible VA information system for non-public information and removes such information, if discovered.	As discovered or no less than quarterly review.	[Define frequency]

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OI&T Recommended Control Value Minimums	System-Specific Control Value - TBD by Information System Owner for Secure Baseline
AU-2	H, M, L	**Audit Events** OI&T determines that the information system must be capable of auditing events as defined by the Information System Owner.	Information 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; and/or • the setting of user identifiers.	[Define list of auditable events]
AU-2	H, M, L	**Audit Events** OI&T determines which events are to be audited within the information system including the frequency for each event.	Information 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	**Audit Events – Reviews and Updates** OI&T reviews and updates the audited events.	Annually or following an incident	[Define frequency]
AU-3 (1)	H, M	**Content of Audit Records – Additional Audit Information** The information system generates audit records containing additional, more detailed information.	Document and maintain information, such as individual identities of group account users.	[Define detailed information by type, locations, or subject]

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OI&T Recommended Control Value Minimums	System-Specific Control Value - TBD by Information System Owner for Secure Baseline
AU-3 (2)	H	**Content of Audit Records – Centralized Management of Planned Audit Record Content** The information system provides centralized management and configuration of the content to be captured in 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-4	H, M, L	**Audit Storage Capacity** The Information System Owner allocates audit record storage capacity in accordance with audit record storage requirements.	Information System Owner defines the system's audit storage capacity based on operational needs.	[Define audit record storage requirements]
AU-5	H, M, L	**Response to Audit Processing Failures** The information system alerts designated organizational officials/positions in the event of an audit processing failure.	Information System Owner defines the roles/positions within his or her organization that will receive system alerts.	[Define personnel and roles]
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 LRBD documented in the SSP. Possible actions: • Notifies system administrator by email when approaching capacity • Overwrites oldest audit records • Stops generating audit records	[Define actions to be taken]
AU-5 (1)	H	**Response to Audit Processing Failures – Audit Storage Capacity** The information system provides a warning to designated organizational officials/positions within a time period when allocated audit record storage volume reaches a percentage of repository maximum audit record storage capacity.	Information System Owner defines the roles/positions within his or her organization that will receive warning and the time period within which the warning will be sent when allocated audit record storage volume reaches 75% of repository maximum audit record storage capacity.	[Define personnel, roles, and/or locations; time period; and percentage]

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OI&T Recommended Control Value Minimums	System-Specific Control Value - TBD by Information System Owner for Secure Baseline
AU-5 (2)	H	**Response to Audit Processing Failures – Real-Time Alerts** The information system provides an alert in a defined time period to designated organizational officials/positions/locations when defined audit failure events requiring real-time alerts occur.	Immediately Information System Owner defines the roles/positions within his or her organization that will receive system alerts and the events that should trigger a real-time alert.	[Define real-time period, personnel, roles, and/or locations; and audit failure events requiring real-time alerts]
AU-6	H, M, L	**Audit Review, Analysis, and Reporting** OI&T reviews and analyzes information system audit records for indications of inappropriate or unusual activity, and reports findings to designated organizational officials/positions.	At least weekly Information System Owners define inappropriate or unusual activity specific to their system. Reports findings to ISO	[Define frequency; inappropriate or unusual activity; and personnel or roles]
AU-6 (5)	H	**Audit Review, Analysis, and Reporting – Integration/Scanning and Monitoring Capabilities** OI&T integrates analysis of audit records with analysis of (one or more): vulnerability scanning information; performance data; information system monitoring information; organization-defined data/information collected from other sources to further enhance the ability to identify inappropriate or unusual activity.	Vulnerability scanning information; performance data; information system monitoring information; other types of information specified by the Information System Owner.	[Select (one or more): vulnerability scanning information; performance data; information system monitoring information; [organization-defined data/information collected from other sources]]
AU-7 (1)	H, M	**Audit Reduction and Report Generation – Automatic Processing** The information system provides the capability to process audit records for events of interest based on defined audit fields within audit records.	Information System Owner-defined by the content of specific audit record fields including, for example, identities of individuals, event types, event locations, event times, event dates, system resources involved, IP addresses involved, or information objects accessed.	[Define audit fields within audit records]

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OI&T Recommended Control Value Minimums	System-Specific Control Value - TBD by Information System Owner for Secure Baseline
AU-8	H, M, L	**Time Stamps** The information system records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets a defined granularity of time measurement.	Information System Owner defines the granularity of time measurement.	[Define granularity of time measurement]
AU-8 (1)	H, M	**Time Stamps – Synchronization with Authoritative Time Source** The information system compares the internal information system clocks with a defined authoritative time source.	Information System Owner to determine frequency and authoritative time source.	[Define frequency and authoritative time source]
AU-8 (1)	H, M	**Time Stamps – Synchronization with Authoritative Time Source** The information system synchronizes internal information system clocks to the authoritative time source when the time difference is greater than a defined time period.	Settings are adjusted to time zone and if time sync varies by more than two minutes, reset to default authoritative source.	[Define time period]
AU-9 (2)	H	**Protection of Audit Information – Audit Backup on Separate Physical Systems/Components** The information system backs up audit records onto a physically different system or system component than the system or component being audited.	Information System Owner defines frequency.	[Define frequency]
AU-9 (4)	H, M	**Protection of Audit Information – Access by Subset of Privileged Users** OI&T authorizes access to management of audit functionality to only a subset of privileged users.	Information System Owner determines which privileged system users have access to management of audit functionality and includes this information in the SSP.	[Define subset of privileged users]
AU-10	H	**Non-Repudiation** The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed actions to be covered by non-repudiation.	Information System Owner determines actions to be covered.	[Define actions to be covered by non-repudiation]
AU-12	H, M, L	**Audit Generation** The information system provides audit record generation capability for the auditable events defined in **AU-2: Auditable Events** at defined information system components.	Information System Owner defined components.	[Define system components]

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OI&T Recommended Control Value Minimums	System-Specific Control Value - TBD by Information System Owner for Secure Baseline
AU-12	H, M, L	**Audit Generation** The information system allows designated organizational officials/positions to select which auditable events are to be audited by specific components of the information system.	Information System Owner defined personnel or roles that can select which auditable events are to be audited by the specific components of the information system.	[Define personnel or roles]
AU-12 (1)	H	**Audit Generation – System-Wide/Time Correlated Audit Trail** 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.	Information System Owner defined components Information System Owner defined tolerance	[Define system components and level of tolerance for relationship between time stamps and audit trail]
AU-12 (3)	H	**Audit Generation – Changes by Authorized Individuals** The information system provides the capability for designated organizational officials/positions to change the auditing to be performed on information system components based on selectable event criteria within time thresholds.	Information System Owner defines individuals and roles that have been authorized to change the auditing to be performed on specified information system components based on Information System Owner-defined selectable criteria within a determined threshold.	[Define individuals or roles; information system components; selectable event criteria; and thresholds]
CM-2 (1)	H, M	**Baseline Configuration – Reviews and Updates** The Information 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 an annual basis A significant change to the system occurs that affects security	[Define frequency of baseline review and for what circumstances]
CM-2 (3)	H, M	**Baseline Configuration – Retention of Previous Configurations** OI&T retains previous versions of baseline configurations of the information system to support rollback.	Information System Owner defines the number of previous versions of baseline configurations specific to his/her system.	[Define previous versions of baseline configurations of the information system]

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OI&T Recommended Control Value Minimums	System-Specific Control Value - TBD by Information System Owner for Secure Baseline
CM-3 (1)	H	**Configuration Change Control – Automated Document/Notification/Prohibition of Changes** OI&T employs automated mechanisms to highlight proposed changes to the information system that have not been approved or disapproved.	Organization will prepare time frame according to guidance from CCB.	[Define time frame]
CM-3 (1)	H	**Configuration Change Control – Automated Document/Notification/Prohibition of Changes** OI&T employs automated mechanisms to notify designated organization officials when approved changes to the information system are completed.	Information System Owner documents personnel to be notified when approved changes to the information system are completed.	[Define personnel]
CM-5 (2)	H	**Access Restrictions for Change – Review System Changes** The Information System Owner reviews information system changes and circumstances to determine whether unauthorized changes have occurred.	Monthly audits of changes. Information System Owner indicates what warrants a review of information system changes and the specific circumstances justifying such reviews to help determine whether unauthorized changes have occurred.	[Define frequency and circumstances]
CM-5 (3)	H	**Access Restrictions for Change – Signed Components** The information system prevents the installation of software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by OI&T.	Software programs will include patches, service packs and device drivers.	[Define software and firmware components]
CM-6 (1)	H	**Configuration Settings – Automated Central Management/Application/Verification** OI&T employs automated mechanisms to centrally manage, apply and verify configuration settings for information system components.	Information System Owner defines information system components.	[Define information system components}

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OI&T Recommended Control Value Minimums	System-Specific Control Value - TBD by Information System Owner for Secure Baseline
CM-6 (2)	H, M, L	**Configuration Settings – Respond to Unauthorized Changes** OI&T employs security safeguards to respond to unauthorized changes to VA-defined configuration settings.	The Information System Owner defines how to respond to unauthorized changes to the approved configuration settings. May include: alerting designated organizational personnel, restoring established configuration settings, or in extreme cases halting affected system processing.	[Define safeguards and configuration settings]
CM-7	H, M, L	**Least Functionality** The Information System Owner configures the information system to provide only essential capabilities and prohibits or restricts the use of other identified functions, ports, protocols, and/or services.	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]
CM-7 (1)	H, M	**Least Functionality – Periodic Review** The Information System Owner reviews the information system to identify unnecessary and/or non-secure functions, ports, protocols, and services.	At a minimum, annually review systems for unauthorized ports/services.	[Define frequency]
CM-7 (1)	H, M	**Least Functionality – Periodic Review** The Information System Owner disables functions, ports, protocols, and services within the information system deemed to be unnecessary and/or non-secure.	Information System Owner defines ports, functions, services that have been disabled on the system.	[Define functions, ports, protocols, and services within the information system deemed to be unnecessary and/or non-secure]
CM-7 (2)	H	**Least Functionality – Prevent Program Execution** The Information System Owner prevents program execution in accordance with one or more of the following specifications: VA policies regarding software usage and restrictions and/or rules authorizing the terms and conditions of software program usage.	Information System Owner selects the appropriate specification for the system, either VA policies regarding software usage and restrictions and/or rules authorizing the terms and conditions of software program usage.	[Select from options provided]

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OI&T Recommended Control Value Minimums	System-Specific Control Value - TBD by Information System Owner for Secure Baseline
CM-8	H, M, L	**Information System Component Inventory** OI&T develops and documents an inventory of information system components that includes information necessary for effective information system component accountability.	Required information as outlined by OI&T Service Delivery and Engineering	[Define necessary information for property accountability]
CM-8 (3)	H	**Information System Component Inventory – Automated Unauthorized Component Detection** The Information System Owner employs automated mechanisms to detect the presence of unauthorized hardware, software, and firmware components within the information system.	Continuous monitoring established on a schedule determined by Information System Owner and documented in security plan.	[Define frequency]
CM-8 (3)	H	**Information System Component Inventory – Automated Unauthorized Component Detection** The Information System Owner takes the following actions when unauthorized components are detected (one or more): disables network access by such components; isolates components; notifies designated organizational officials/positions.	Information System Owner determines if the system disables network access and/or notifies the Information System Owner to disable network access depending on assessment of risk.	[Select (one or more): disables network access by such components; isolates the components; notifies [Assignment: organization-defined personnel or roles]]
CM-8 (4)	H	**Information System Component Inventory – Accountability Information** OI&T includes in the information system component inventory information, a means for identifying individuals responsible/accountable for administering those components.	Identify system users by name, position, or role.	[Select (one or more): name; position; role]
CP-2	H, M, L	**Contingency Plan** The Information 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	**Contingency Plan** The Information 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	OI&T Recommended Control Value Minimums	System-Specific Control Value - TBD by Information System Owner for Secure Baseline
CP-2 (3)	H	**Contingency Plan – Resume Essential Missions/Business Functions** The Information System Owner plans for the resumption of essential missions and business functions after contingency plan activation.	Identify time period that the Information System Owner determines when essential operations will resume once the contingency plan has been activated.	[Define time period]
CP-2 (4)	H	**Contingency Plan – Resume all Missions/Business Functions** The Information System Owner plans for the resumption of all missions and business functions within a defined time period of contingency plan activation.	Time frame as determined by the Information System Owner and outlined in system's contingency plan.	[Define time period]
CP-4	H, M, L	**Contingency Plan Testing and Exercises** OI&T tests the contingency plan for the information system using OI&T-defined tests to determine effectiveness of the plan and VA's readiness to execute the plan.	Annually test contingency plan Tests will have a specific objective such as: determining the availability of needed backup files; validity/functionality of the backup files; and implementation of fire and evacuation procedures and implementation of manual procedures.	[Define frequency and type of test]
CP-7	H, M	**Alternate Processing Site** OI&T establishes an alternate processing site including necessary agreements to permit the transfer and resumption of defined information system operations for essential missions and business functions when the primary processing capabilities are unavailable.	Information System Owner defines the information system operations that are essential for mission and business functions. This trigger point (downtime before contingency plan is activated) is set by criticality to VA mission and business need, identified within the contingency plan, and tested for in the SCA.	[Define information system operations and time period according to recovery time and recovery point objectives]

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OI&T Recommended Control Value Minimums	System-Specific Control Value - TBD by Information System Owner for Secure Baseline
CP-8	H, M	**Telecommunications Services** OI&T establishes alternate telecommunications services including necessary agreements to permit the resumption of defined information system operations for essential missions and business functions when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.	Information System Owner defines the telecommunication operations that are required for essential missions and business functions. 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 information system operations and time period]
CP-9	H, M, L	**Information System Backup** OI&T conducts backups of user-level information contained in the information system consistent with recovery time and recovery point objectives.	Frequency defined by Information System Owner in conjunction with Information Owner.	[Define frequency according to recovery time and point objective]
CP-9	H, M, L	**Information System Backup** OI&T conducts backups of system-level information contained in the information system consistent with recovery time and recovery point objectives.	Frequency defined by Information System Owner in conjunction with Information Owner.	[Define frequency according to recovery time and point objective]
CP-9	H, M, L	**Information System Backup** OI&T 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	**Information System Backup – Testing for reliability/Integrity** OI&T tests backup information to verify media reliability and information integrity.	Frequency defined by Information System Owner in conjunction with Information Owner	[Define frequency]
CP-9 (3)	H	**Information System Backup – Separate Storage for Critical Information** OI&T stores backup copies of critical information system software and other security-related information in a separate facility or in a fire-rated container that is not co-located with the operational system.	Information System Owner determines, based on system, what specific critical information is to be backed up and stored.	[Define critical information system software and other related information]

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OI&T Recommended Control Value Minimums	System-Specific Control Value - TBD by Information System Owner for Secure Baseline
CP-9 (5)	H	**Information System Backup – Transfer to Alternate Storage Site** OI&T transfers information system backup information to the alternate storage site at a frequency and transfer rate consistent with the recovery time and recovery point objectives.	Information System Owner defines frequency based on system's contingency plan.	[Define time period and transfer rate consistent with the recovery time and recovery point objectives]
CP-10 (4)	H	**Information System Recovery and Reconstitution – Restore Within Time Period** OI&T provides the capability to restore information system components from configuration-controlled and integrity-protected information representing a known, operational state for the components.	Within recovery-restoration time periods	[Define restoration time period(s)]
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.	Information System Owner defines list of devices that must uniquely identify and authenticate before establishing either a local, remote, or network connection.	[Define list of specific and type of device(s) and Select (one or more): local; remote; network]
IA-4	H, M, L	**Identifier Management** OI&T manages information system identifiers by receiving authorization from designated organizational officials/positions to assign an individual, group, role, or device identifier.	Information System Owner or designee	[Define personnel or roles]
IA-4	H, M, L	**Identifier Management** OI&T manages information system identifiers by preventing reuse of identifiers.	At least 2 years	[Define time period]
IA-4	H, M, L	**Identifier Management** OI&T manages information system identifiers by disabling the identifier after a time period of inactivity.	Ninety days	[Define time period of inactivity]
IR-8	H, M, L	**Incident Response Plan** The Operating Unit and OI&T distribute copies of the incident response plan to a list of incident response personnel (identified by name and/or by role) and organizational elements.	Key personnel identified in the incident response plan and reviewed/updated annually or when change in personnel occurs.	[Define list of IR personnel by name/role for copies]
IR-8	H, M, L	**Incident Response Plan** The Operating Unit and OI&T review the incident response plan.	Annually	[Define frequency]

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OI&T Recommended Control Value Minimums	System-Specific Control Value - TBD by Information System Owner for Secure Baseline
IR-8	H, M, L	**Incident Response Plan** The Operating Unit and OI&T communicate incident response plan changes to a defined list of incident response personnel (identified by name and/or by role) and organizational elements.	Prepare and distribute incident response plan to key personnel and provide updates when incurred.	[Define list of IR personnel by name/role for copies]
MA-2	H, M, L	**Controlled Maintenance** OI&T includes maintenance-related information in VA maintenance records.	Information System Owner defines maintenance-related information.	[Define maintenance-related information]
MA-6	H, M	**Timely Maintenance** The Information System Owner obtains maintenance support and/or spare parts for information system components within a time frame suitable to avoid failure.	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. Information System Owner defines time period for delivery of support or parts.	[Define list of security-critical system components and time period]
MP-2	H, M, L	**Media Access** The Information System Owner restricts access to information in printed form or on digital media to a defined list of authorized individuals.	Information systems media both paper and electronic. Establish access list for Low, Moderate, and High.	[Define types of media and list authorized individuals]
MP-3	H, M	**Media Marking** OI&T exempts specific types of information system media or hardware from marking as long as the media remain within the designated controlled areas.	Removable media documented in SSP, such as Disk Packs and backup tapes Secured computer room is the designated controlled area.	[Define list of exempted media types and the designated controlled area(s)]
MP-4	H, M	**Media Storage** OI&T physically controls and securely stores types of digital and non-digital media within controlled areas.	Information systems media, both paper and electronic Controlled area defined by the Information System Owner	[Define media and controlled areas]

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OI&T Recommended Control Value Minimums	System-Specific Control Value - TBD by Information System Owner for Secure Baseline
MP-5	H, M	**Media Transport** The Operating Unit protects and controls types of information system media during transport outside of controlled areas using security safeguards.	Information systems media, both paper and electronic Double-wrap and secure physical container when appropriate to prevent loss or compromise	[Define type of media and security safeguards for transport]
PE-2	H, M, L	**Physical Access Authorizations** OI&T reviews the access list detailing authorized facility access by individuals.	Bi-annually for Low Quarterly for Moderate and High	[Define frequency]
PE-3	H, M, L	**Physical Access Control** The Operating Unit enforces physical access authorizations at entry/exit points to the facility where the information system resides by: 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress/egress to the facility using PACSs/devices and/or guards.	Information System Owner defines the entry/exit locations for system that requires PACS. Information System Owner selects the appropriate devices and/or guards.	[Defined entry/exit points to the facility where the information system resides] [Select (one or more): [organization-defined physical access devices]; guards]
PE-3	H, M, L	**Physical Access Control** The Operating Unit maintains physical access audit logs for entry/exit points.	Information System Owner defines the locations that require physical access audit logs.	[Define entry/exit points]
PE-3	H, M, L	**Physical Access Control** The Operating Unit changes combinations and keys as specified in the security plan and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.	Define frequency within security plan.	[Define frequency]
PE-3 (1)	H	**Physical Access Control – Information System Access** The Operating Unit enforces physical access authorizations to the information system in addition to the physical access controls for the facility at physical spaces containing one or more components of the information system.	To be determined by Information System Owner for specific environment	[Define physical spaces containing one or more components of the information system]

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OI&T Recommended Control Value Minimums	System-Specific Control Value - TBD by Information System Owner for Secure Baseline
PE-4	H, M	**Access Control for Transmission Medium** The Operating Unit controls physical access to information system distribution and transmission lines within VA facilities using security safeguards.	To be determined by Information System Owner and/or CIO for specific environment. Security safeguards include locked wiring closets, disconnected or locked spare jacks, and or protection of cabling by conduit or cable trays.	[Define system distribution and transmission lines and define security safeguards]
PE-6	H, M, L	**Monitoring Physical Access** The Operating Unit reviews physical access logs at a defined frequency and upon occurrence of defined events or potential indications of events.	Information System Owner defines frequency of reviews and additional events or potential indications of events per his or her environment which may require additional reviews.	[Define frequency and define events or potential indications of events]
PE-6 (4)	H	**Monitoring Physical Access – Monitoring Physical Access to Information Systems** OI&T monitors physical access to the information system in addition to the physical access monitoring of the facility as physical spaces containing one or more components of the information system.	Information System Owner defines the physical spaces that contain one or more information system.	[Define physical spaces containing one or more components of the information system]
PE-8	H, M, L	**Access Records** OI&T 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 locations 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-11	H, M	**Emergency Power** The Operating Unit provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system and/or transition of the information system to long-term alternate power in the event of a primary power source loss.	Select (one or more): An orderly shutdown of the system or transition of the information system to long-term alternate power.	[Select (one or more): an orderly shutdown of the information system; transition of the information system to long-term alternate power.]

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OI&T Recommended Control Value Minimums	System-Specific Control Value - TBD by Information System Owner for Secure Baseline
PE-13 (1)	H	**Fire Protection – Detection Devices/Systems** The Operating Unit employs fire detection devices/systems for the information system that activate automatically and notify designated organizational officials/positions and emergency responders in the event of a fire.	Information System Owner or CIO defines the personnel or roles to be notified and also includes the emergency responders that must be notified in the event of a fire.	[Define personnel or roles and emergency responders]
PE-13 (2)	H	**Fire Protection – Suppression Devices/Systems** The Operating Unit employs fire suppression devices/systems for the information system that provide automatic notification of any activation to designated organizational officials/positions and emergency responders.	Information System Owner or CIO defines what personnel or roles are to be automatically notified and also includes the emergency responders that must be notified in the event of a fire.	[Define personnel or roles and emergency responders]
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 at acceptable levels.	Document acceptable levels in SSP in compliance with recommended manufacturer requirements.	[Define acceptable levels]
PE-14	H, M, L	**Temperature and Humidity Controls** The Operating Unit monitors temperature and humidity levels.	Consistently monitor according to recommended manufacturer requirements.	[Define frequency]
PE-15 (1)	H	**Water Damage Protection – Automation Support** The Operating Unit employs mechanisms to detect the presence of water in the vicinity of the information system and alerts designated organizational officials/positions.	The Information System Owner defines the personnel or roles that should be notified in case of water in the vicinity of the information system.	[Define personnel or roles]
PE-16	H, M, L	**Delivery and Removal** The Operating Unit authorizes, monitors, and controls types of information system components entering and exiting the facility and maintains records of those items.	Information system-related items (i.e., hardware, firmware, software)	[Define types of components]
PE-17	H, M	**Alternate Work Site** The Operating Unit employs security controls at alternate work sites.	Controls, both physical and logical, established per VA Handbook 6500	[Identify any unique specific controls required]

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OI&T Recommended Control Value Minimums	System-Specific Control Value - TBD by Information System Owner for Secure Baseline
PE-18	H	**Location of Information System Components** 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.	The Information System Owner defines physical and environmental hazards specific to location of system.	[Define physical and environmental hazards]
PL-2	H, M, L	**System Security Plan** The Information System Owner distributes copies of the security plan and communicates subsequent changes to the plan to designated organizational officials/positions.	Information System Owner identifies personnel or roles of individuals who should receive a copy of the SSP.	[Define personnel or roles]
PL-2 (3)	H, M	**System Security Plan – Plan/Coordinate with Other Organizational Entities** The Information System Owner plans and coordinates security-related activities affecting the information system with designated individuals or groups before conducting such activities in order to reduce the impact on other organizational entities.	Information System Owner identifies individuals or groups that should be notified in order to reduce the impact on other organizational entities.	[Defined individuals or groups]
PS-4	H, M. L	**Personnel Termination** The Operating Unit or Human Resources, upon termination of individual employment, conducts exit interviews that include a discussion of information security topics.	Nondisclosure agreements, if applicable	[Define information security topics]
PS-4	H, M, L	**Personnel Termination** The Operating Unit, upon termination of individual employment, notifies designated organizational officials/positions within a defined time period.	Human Resources, Facility Director, and Information System Owner determine personnel or roles to be notified and time period.	[Define personnel or roles and time period]
PS-4 (2)	H	**Personnel Termination – Automated Notification** The Operating Unit employs automated mechanisms to notify designated organizational officials/positions upon termination of an individual.	Information System Owner works with facility management to determine what personnel, positions and/or roles are notified.	[Define personnel or roles]

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OI&T Recommended Control Value Minimums	System-Specific Control Value - TBD by Information System Owner for Secure Baseline
PS-5	H, M, L	**Personnel Transfer** The Operating Unit initiates transfer or reassignment actions promptly.	Appropriate transfer/ reassignment actions to be initiated include: • Reissuing keys, identification cards, and building passes; closing old accounts; • Establishing new accounts; and • Changing system access authorizations. Changes should occur as soon as possible but no later than 30 days after the transfer action.	[Define action and time period]
PS-5	H, M, L	**Personnel Transfer** The Operating Unit notifies designated organizational officials/positions within a defined time period.	Human Resources, Facility Director, and Information System Owner determine personnel or roles to be notified and time period.	[Define personnel or roles and period]
RA-3	H, M, L	**Risk Assessment** The Information System Owner disseminates risk assessment results to designated organizational officials/positions.	The Information System Owner determines the personnel or roles that should receive risk assessment results. The ISO should receive a copy.	[Define personnel or roles]
RA-5	H, M, L	**Vulnerability Scanning** OI&T scans for vulnerabilities in the information system and hosted applications at a defined frequency and/or randomly and when new vulnerabilities potentially affecting the system/applications are identified and reported.	Monthly and/or randomly in accordance with OI&T approved process	[Define frequency and/or randomly in accordance with organization-defined process]
RA-5	H, M, L	**Vulnerability Scanning** OI&T shares information obtained from the vulnerability scanning process and SCAs with designated organizational officials/positions to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).	OCS and Information System Owner-defined personnel or roles	[Define personnel or roles]

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OI&T Recommended Control Value Minimums	System-Specific Control Value - TBD by Information System Owner for Secure Baseline
RA-5 (2)	H,M	**Vulnerability Scanning – Update by Frequency/Prior to New Scan/When Identified** OI&T updates the information system vulnerabilities scanned at a defined frequency, prior to a new scan, or when new vulnerabilities are identified and reported.	Information System Owner uses a system or organizational level process to address findings from a vulnerability scan conducted on a monthly basis.	[Select (one or more): [organization-defined frequency]; prior to a new scan; when new vulnerabilities are identified and reported]
RA-5 (4)	H	**Vulnerability Scanning – Discoverable Information** OI&T determines what information is discoverable by adversaries and subsequently takes corrective actions.	Information System Owner defines corrective actions.	[Define corrective actions]
RA-5 (5)	H	**Vulnerability Scanning – Privileged Access** The information system implements privileged access authorization to identified information system components for selected vulnerability scanning activities.	Information System Owner defines the specific system components that require privileged access authorization and defines what specific vulnerability scanning activities require these privileged access authorizations.	[Define information system components and vulnerability scanning activities]
SA-4 (2)	H, M	**Acquisitions – Design/Implementation Information for Security Controls** The Operating Unit requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; at a defined level of detail.	Information System Owner determines the design based on security and business requirements and must include system/security design, interfaces, design documents, and lower-level system development documentation.	[Select (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [organization-defined level of detail]]
SA-5	H, M, L	**Information System Documentation** The Operating Unit documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or non-existent and takes defined actions in response.	Information System Owner outlines actions taken when documentation is not available.	[Define actions]

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OI&T Recommended Control Value Minimums	System-Specific Control Value - TBD by Information System Owner for Secure Baseline
SA-5	H, M, L	**Information System Documentation** The Operating Unit distributes documentation to designated organizational officials/positions.	Information System Owner defines the personnel or roles within his or her organization that are provided and maintain system documentation.	[Define personnel or roles]
SA-9 (2)	H, M	**External Information System Services – Identification of Functions/Ports/Protocols/Services** OI&T requires providers of external information system services to identify the functions, ports, protocols, and other services required for the use of such services.	Information System Owner defines all applicable external information service providers.	[Define external information system services]
SA-10	H, M	**Develop Configuration Management** OI&T requires the developer of the information system, system component, or information system service to perform configuration management during system, component, or service (one or more): design; development; implementation; and/or operation.	Select one or more: (1) design; (2) development; (3) implementation; (4) operation	[Select (one or more): design; development; implementation; operation]
SA-10	H, M	**Develop Configuration Management** OI&T requires the developer of the information system, system component, or information system service to document, manage and control the integrity of changes to defined configuration items under configuration management.	Information System Owner defines the configuration items that should be included in configuration management of the system.	[Define configuration items under configuration management]
SA-10	H, M	**Develop Configuration Management** OI&T requires the developer of the information system, system component, or information system service to track security flaws and flaw resolution within the system component, or service and report findings to authorized personnel.	Information System Owner defines personnel that should be notified.	[Define personnel]
SA-11	H, M	**Developer Security Testing and Evaluation** OI&T requires the developer of the information system, system component, or information system services to perform one or more of the following: unit; integration; system; and/or regression testing/evaluation at a defined depth and coverage.	Select one or more of the following: unit, integration, system, regression Define breadth/depth.	[Select (one or more): unit; integration; system; regression and define breadth/depth and coverage].

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OI&T Recommended Control Value Minimums	System-Specific Control Value - TBD by Information System Owner for Secure Baseline
SA-12	H	**Supply Chain Protection** The Operating Unit protects against supply chain threats to the information system, system component, or information system service by employing a list of safeguards to protect against supply chain threats as part of a comprehensive, defense-in-breadth information security strategy.	Information System Owner to define security safeguards	[Define security safeguards]
SC-7	H, M, L	**Boundary Protection** OI&T implements subnetworks for publicly accessible system components that are separated from internal VA networks.	Select physically or logically	[Select: physically; logically]
SC-7 (21)	H	**Boundary Protection – Isolation of Information System Components** OI&T employs boundary protection mechanisms to separate information system components supporting missions and/or business functions.	Information System Owners define how the security functions are separated from VA's business data within the system. For example, Medical Device Isolation Architecture (MDIA) for medical devices.	[Define information system components and missions and/or business functions]
SC-8	H, M	**Transmission Confidentiality and Integrity** The information system protects the confidentiality and/or integrity of transmitted information.	Select (one or more): confidentiality and/or integrity	[Select (one or more): confidentiality; integrity]
SC-8 (1)	H, M	**Transmission Confidentiality and Integrity – Cryptographic or Alternate Physical Protection** The information system implements cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission unless otherwise protected by alternative physical safeguards.	Select one or more: (1) prevent unauthorized disclosure of information; (2) detect changes to information. Identify alternative physical safeguards (ex. protected distribution system) in SSP, if applicable.	[Select (one or more): prevent unauthorized disclosure of information; detect changes to information] [Define alternative physical safeguards]
SC-10	H, M	**Network Disconnect** The information system terminates the network connection associated with a communications session at the end of the session or after a period of inactivity.	The time period of inactivity will be determined by the Information System Owner. It may be a set of time periods by type of network access or for specific accesses.	[Define time period of inactivity]

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OI&T Recommended Control Value Minimums	System-Specific Control Value - TBD by Information System Owner for Secure Baseline
SC-15	H, M, L	**Collaborative Computing Devices** OI&T prohibits remote activation of collaborative computing devices unless an exception is defined where remote activation is to be allowed.	Circumstances documented in the SSP.	[Define exceptions for remove activation]
SC-24	H	**Fail in Known State** The information system will fail to a known state for defined types of failures preserving system state information in failure.	Information System Owners will determine known state, types of failures and system state information.	[Define known state, types of failures and system state]
SI-4	H, M	**Information System Monitoring** OI&T monitors the information system to detect attacks and indicators of potential attacks in accordance with monitoring objectives.	OI&T-defined monitoring objectives. Examples may include proper system functioning, indicators of system malfunction or compromise.	[Define monitoring objectives]
SI-4	H, M	**Information System Monitoring** OI&T provides information system monitoring information to designated organizational officials/positions as needed and/or at a defined frequency.	Information System Owner provides the information system monitoring information to Information System Owner-defined individuals or roles. Information System Owner determines the frequency in which the information system monitoring information is provided.	[Define information system monitoring information] [Define personnel or roles] [Select (one or more): as needed; [organization-defined frequency]]
SI-4 (5)	H, M	**Information System Monitoring – System-Generated Alerts** The information system alerts designated organizational officials/positions when indications of compromise or potential compromise occur.	Information System Owners determine personnel or roles that receive alerts when indications of compromise or potential compromises occur.	[Define personnel or roles] [Define list of compromise indicators]
SI-5	H, M, L	**Security Alerts, Advisories, and Directives** OI&T Disseminates security alerts, advisories, and directives to select (one or more): designated organizational officials/positions; elements within VA; and/or external organizations as designated by the Information System Owner.	Information System Owner defines individuals and roles of those that should receive security alerts, advisories, and directives. Select one or more: • personnel or roles; • other offices within OI&T; and/or • external organizations.	[Select (one or more): [organization-defined personnel or roles]; [organization-defined elements within the organization]]; [organization-defined external organizations]

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OI&T Recommended Control Value Minimums	System-Specific Control Value - TBD by Information System Owner for Secure Baseline
SI-6	H	**Security Functionality Verification** The information system verifies the correct operation of security functions.	Information System Owner defines the security functions for specific system.	[Define security functions]
SI-6	H	**Security Functional Verification** The information system performs the verification at system transitional states, upon command by user with appropriate privilege, and/or at a defined frequency.	Information System Owner selects when to perform verification from those options listed based on what is appropriate for the system.	[Select (one or more): [organization-defined system transitional states]; upon command by user with appropriate privilege; [organization-defined frequency]
SI-6	H	**Security Functional Verification** The information system notifies designated organizational officials/positions of failed security verification tests.	Information System Owner defines personnel or roles within his or her organization that are notified of failed security verification tests.	[Define personnel or roles]
SI-6	H, M	**Security Functional Verification** The information system shuts the information system down, restarts the information system, and/or defines alternative actions when anomalies are discovered.	Information System Owner selects the appropriate choice from those listed that is appropriate for the system.	[Selection (one or more): shuts the system down; restarts the information system; [organization-defined alternative action(s)]]
SI-7	H, M	**Software, Firmware, and Information Integrity** OI&T employs integrity verification tools to detect unauthorized changes to software, firmware, and information.	Information System Owner determines the appropriate software, firmware, and information to be checked by integrity verification tools to detect unauthorized changes.	[Define software, firmware, and information]

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OI&T Recommended Control Value Minimums	System-Specific Control Value - TBD by Information System Owner for Secure Baseline
SI-7 (1)	H, M	**Software, Firmware, and Information Integrity – Integrity Checks** The information system performs an integrity check of software, firmware, and information at startup, at defined transitional states or security-relevant events, and/or at a defined frequency.	Information System Owner selects the appropriate software, firmware, and information to be checked at select one or more: (1) at startup; (2) at Information System Owner-defined transitional states or security-relevant events; (3) quarterly.	[Define software, firmware, and information] [Select (one or more): at startup; at [organization-defined transitional states or security-relevant events]; [organization-defined frequency]]
SI-7 (2)	H	**Software, Firmware, and Information Integrity – Automated Notifications of Integrity Violations** OI&T employs automated tools that provide notification to designated organizational officials/positions upon discovering discrepancies during integrity verification.	Information System Owner determines and documents roles/personnel that receive notifications.	[Define personnel or roles]
SI-7 (5)	H	**Software, Firmware, and Information Integrity – Automated Response to Integrity Violations** The information system automatically shuts the information system down, restarts the information system, and/or implements security safeguards when integrity violations are discovered.	Information System Owner selects the appropriate choice from those listed that is appropriate for the system. Select one or more: (1) shuts the information system down; (2) restarts the information system; and/or (3) implements Information System Owner defined security safeguards.	[Select (one or more): shuts the information system down; restarts the information system; implements [organization-defined security safeguards]]
SI-7 (7)	H, M	**Software, Firmware, and Information Integrity – Integration of Detection and Response** OI&T incorporates the detection of unauthorized security-relevant changes to the information system into VA incident response capability.	Information System Owner determines the appropriate security-relevant changes to the information system into the incident response capability. Examples include unauthorized changes to established configuration settings or unauthorized elevation of information system privileges.	[Define security-relevant changes to the information system]

Control	Baseline High, Moderate, Low	Per NIST SP 800-53	OI&T Recommended Control Value Minimums	System-Specific Control Value - TBD by Information System Owner for Secure Baseline
SI-10	H, M	**Information Input Validation** The information system checks the validity of information inputs.	Information System Owner in conjunction with Information Owner determines and defines input validation checks that should be completed.	[Define information inputs]
SI-11	H, M	**Error Handling** The information system reveals error messages only to designated organizational officials/positions.	Information System Owner determines and documents personnel or roles that should receive error routing.	[Define personnel or roles]
SI-16	H, M	**Memory Protection** The information system implements security safeguards to protect its memory from unauthorized code execution.	Information System Owner defines security safeguards.	[Define security safeguards]