Department of Veterans Affairs
Washington, DC 20420

VA HANDBOOK 6500
Transmittal Sheet
February 24, 2021

RISK MANAGEMENT FRAMEWORK FOR VA INFORMATION SYSTEMS
VA INFORMATION SECURITY PROGRAM

1. **REASON FOR ISSUE:** Reissue handbook to provide policy and procedural guidance on the VA Risk Management Framework (RMF) process. Reissues VA Handbook 6500 to align with VA policy in VA Directive 6500, VA Cybersecurity Program.

2. **SUMMARY OF CONTENTS/MAJOR CHANGES:**

   a. VA Handbook 6500 addresses all steps of the RMF as defined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Revision 2;

   b. Incorporates content from VA Handbook 6500.3, Assessment, Authorization and Continuous Monitoring of VA Information Systems; and

   c. Removes security and privacy control descriptions, baselines, and organization-defined parameters, which is in the Information Security Knowledge Service.

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

4. **RELATED DIRECTIVE:** VA Directive 6500, VA Cybersecurity Program.

5. **RESCISSIONS:** VA Handbook 6500, Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program, dated March 10, 2015, and its appendices, and VA Handbook 6500.3, Assessment, Authorization and Continuous Monitoring of VA Information Systems, dated February 3, 2014.

CERTIFIED BY:

/s/
John P. Medve
Acting Assistant Secretary for
Enterprise Integration

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/
Dominic A. Cussatt
Acting Assistant Secretary for Information
and Technology/ Chief Information Officer

DISTRIBUTION: Electronic Only

RISK MANAGEMENT FRAMEWORK FOR VA INFORMATION SYSTEMS
VA INFORMATION SECURITY PROGRAM

CONTENTS

PARAGRAPH **PAGE**

RISK MANAGEMENT FRAMEWORK FOR VA INFORMATION SYSTEMS
VA INFORMATION SECURITY PROGRAM

CONTENTS, cont.

PARAGRAPH **PAGE**

RISK MANAGEMENT FRAMEWORK FOR VA INFORMATION SYSTEMS
VA INFORMATION SECURITY PROGRAM

CONTENTS, cont.

APPENDICES **PAGE**

FIGURES **PAGE**

TABLES **PAGE**

RISK MANAGEMENT FRAMEWORK FOR VA INFORMATION SYSTEMS VA INFORMATION SECURITY PROGRAM

1. PURPOSE.

a. Updates VA Handbook 6500 to align with VA policy in VA Directive 6500, VA Cybersecurity Program;

b. Establishes associated cybersecurity policy and assigns responsibilities for executing and maintaining the Risk Management Framework (RMF);

c. Directs visibility of authorization documentation and reuse of artifacts between and among VA Information Technology (IT) stakeholders; and

d. Provides procedural guidance for the reciprocal acceptance of authorization decisions and artifacts within VA and between VA and other Federal agencies, for the authorization and connection of information systems.

2. SCOPE.

a. The VA Handbook 6500 satisfies the Federal and statutorily requirements of:

(1) Federal Information Security Modernization Act (FISMA);

(2) U.S. Code (U.S.C) title 38, Veterans’ Benefits Act, Subchapter III - Information Security;

(3) National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Risk Management Framework for Information Systems and Organizations, A System Life Cycle Approach for Security and Privacy;

(4) Office of Management and Budget (OMB) Circular A-130;

(5) The Privacy Act of 1974;

(6) Health Insurance Portability and Accountability Act of 1996 (HIPAA); and

(7) The Health Information Technology for Economic and Clinical Health (HITECH) Act.

b. This handbook serves all Administrations, Staff Offices, Staff Organizations, Boards, and Special Programs of the Department of Veterans Affairs associated with the design, development, implementation, assessment, operation, maintenance, and disposition of information systems including:

(1) Individuals with mission or Business Ownership responsibilities or fiduciary responsibilities (e.g., heads of Federal agencies);

(2) Individuals with information system, information security, or privacy management,

oversight, or governance responsibilities (e.g., senior leaders, Risk Executives, Authorizing Officials (AOs), Chief Information Officers (CIO), Chief Information Security Officers (CISOs), and Senior Agency Officials for Privacy (SAOP));

(3) Individuals responsible for conducting security or privacy assessments and for monitoring information systems, for example, Control Assessors, auditors, and System Owners;

(4) Individuals with security or privacy implementation and operational responsibilities, for example, System Owners, Common Control Providers, Information Owners/Stewards, mission or Business Owners, Security or Privacy Architects, and Information System Security or Privacy engineers;

(5) Individuals with information system development and acquisition responsibilities (e.g., Program Managers, Procurement Officials, component product and system developers, Systems Integrators, and Enterprise Architects); and

(6) Individuals with logistical or disposition-related responsibilities (e.g., Program Managers, Procurement Officials, System Integrators, and Property Managers).

c. All VA IT that receive, process, store, display, or transmit VA information. These technologies are broadly grouped as VA Information Systems, Platform IT, cyber-physical systems, IT services, and IT products. This includes IT supporting research, development, test and evaluation, and IT operated by a contractor or other entity on behalf of VA.

d. Nothing in this handbook alters or supersedes the existing authorities and policies of VA and other Federal laws and regulations.

3. BACKGROUND/OVERVIEW.

a. VA will establish and use a multi-level risk management approach that addresses security and privacy risk at the organization level, the mission/business process level, and the information system level. VA's approach in this handbook is consistent with the principles described in NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View.

b. The forms of VA IT, as shown in Figure 1, range in size and complexity. The forms encompass individual hardware and software products, stand-alone systems, massive computing environments, enclaves, and networks.

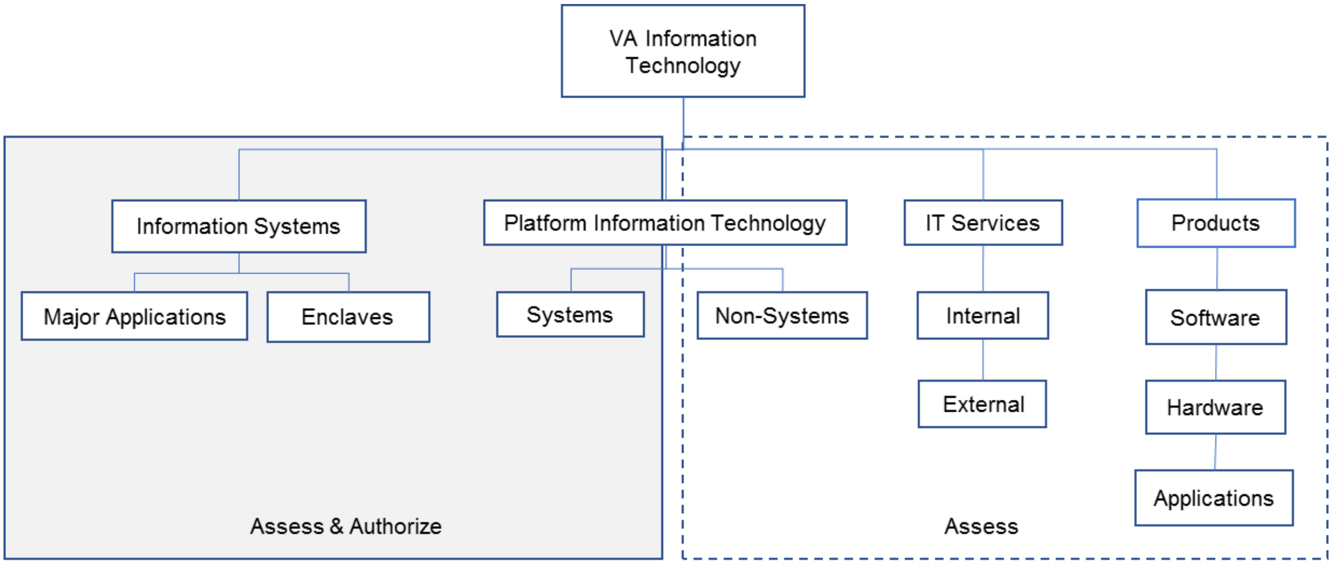

Figure 1: VA IT Resources

c. The risk management for VA IT will be conducted as described in this handbook and consistent with the principals established in NIST SP 800-37. The RMF consists of the steps and depicted in Figure 2.

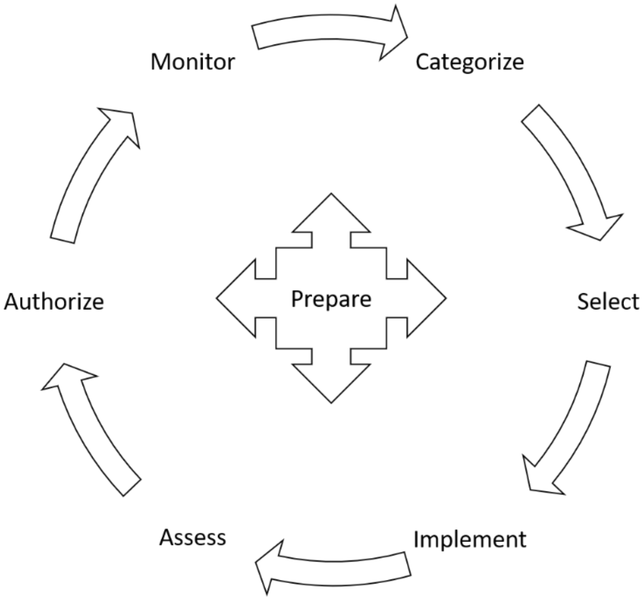

Figure 2: VA Risk Management Framework Steps

d. The RMF will inform the system development life cycle (SDLC) by addressing security and privacy requirements for all VA IT. The relationship between the RMF and SDLC is summarized in Appendix D, High-level Summary of RMF Tasks.

4. RESPONSIBILITIES.

a. VA Directive 6500 describes the responsibilities for VA senior officials, information owners, information system users, and the Office of Inspector General for information security. Each subordinate VA directive and handbook issued by the Office of Information Security 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. Table 1 identifies the RMF roles assigned at VA and the appropriate authority for the appointment of each RMF role.

Table 1: Appointment of RMF Roles

Role	Appointed By
Chief Information Officer	Secretary
Senior Agency Official for Privacy	Secretary
Chief Information Security Officer	Chief Information Officer
Authorizing Official	Chief Information Officer
Risk Executive Function	Chief Information Officer
Chief Privacy Officer	Senior Agency Official for Privacy
Information System Security Officer	Under Secretary
Information Security Architect	Under Secretary
Information System Security Engineer	Under Secretary
Security Control Assessor	Chief Information Security Officer
Authorizing Official Designated Representative	Authorizing Official
Information System Owner	Associate Deputy Assistant Secretary for Enterprise Program Management Office Deputy Assistant Secretary for Information Technology Operations and Services
Privacy Officer	Chief Privacy Officer
Risk Management Framework Technical Advisory Group Representative	Under Secretaries, Assistant Secretaries and Other Key Officials

c. 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/**Chief Information Officer (CIO) shall:

(a) Oversee implementation of this handbook, direct and oversee the cybersecurity risk management of VA IT, and distribute RMF information standards and sharing requirements;

(b) In coordination with the Deputy Assistant Secretary for Development, Security and Operations (DAS DevSecOps), the Associate Deputy Assistant Secretary for Enterprise Program Management Office (ADAS EPMO) and the Associate Deputy Assistant Secretary for Information Technology Operations and Services (ADAS ITOPS), ensure development testing, evaluation and operational testing, and evaluation activities and findings are integrated into the RMF;

(c) Ensure trained and qualified AOs are appointed in writing for all VA information systems and platform IT systems operating within or on behalf of VA in accordance with VA Directive 6500 and that the systems are authorized in accordance with this handbook:

i. The AO role must be assigned to government personnel only; and

ii. Relevant IT expertise must be a factor in the selection and appointment of AOs responsible for authorizing IT systems.

(2) **Office of Information Technology (OIT) Deputy Assistant Secretary for Information Security.** The Deputy Assistant Secretary (DAS) for Information Security, as the Chief Information Security Officer (CISO) under the authority, direction, and control of the VA CIO, shall:

(a) Direct and coordinate the VA Cybersecurity Program, which includes the establishment and maintenance of the RMF. In addition, the VA CISO oversees the Risk Management Framework Technical Advisory Group (RMF TAG) and the Information Security Knowledge Service;

(b) Provide guidance at a design and architectural level for Information System Security Engineering services;

(c) Inform VA Office of Acquisition, Logistics, and Construction (OALC) of acquisition program risks related to failure in addressing cybersecurity requirements in accordance with the VA Cybersecurity Program;

(d) Assist in development of VA Architecture and Engineering to support the RMF (and indirectly authorization decisions);

(e) Ensure that security controls and assessment procedures used by VA are consistent with control correlation identifiers (CCIs), security requirements guides, security technical implementation guides (STIGs), and NIST;

(f) Support development and providing RMF training and awareness products and a distributive training capability to support VA IT, and post the training materials on the Information Security Knowledge Service; and

(g) Identify, develop and provide VA Enterprise RMF management tools.

(3) **Executive Director for Office of Acquisitions, Logistics, and Construction (OALC)** shall coordinate with the VA CIO to ensure RMF processes are appropriately integrated with VA acquisition system processes for acquisitions of VA IT.

(4) **OIT Deputy Assistant Secretary for Development, Security and Operations (DAS DevSecOps)**, in coordination with the VA CIO, ADAS EMPO and ADAS ITOPS ensures development testing and evaluation, and operational testing and evaluation activities and findings are integrated into the RMF.

(5) **OIT Associate Deputy Assistant Secretary for Enterprise Program Management Office (ADAS EPMO)** ensures integration of development testing and evaluation activities into the RMF and provides the RMF TAG with input as appropriate or required, and shall:

(a) Ensure integration of development testing and evaluation activities into the RMF and provide the RMF TAG with input as appropriate or required;

(b) Develop risk model and risk assessment tools to help ensure that VA programs and projects are reviewed by the approving authority for alignment with the VA Technical Reference Model;

(c) Ensure that information security requirements necessary to protect the organization's core mission and business processes are adequately addressed in all aspects of enterprise architecture, including reference models, segment and solution architectures, and the resulting information systems supporting those mission and business processes;

(d) Assist in development of VA architecture and engineering to support the RMF (and indirectly, authorization decisions); and

(e) IT Workforce Development supporting development and providing RMF training and awareness products in a distributive training capability to support VA IT and post the training materials on Information Security Knowledge Service.

(6) **OIT Associate Deputy Assistant Secretary for Information Technology Operations and Services (ADAS ITOPS)**, under the authority, direction, and control of the VA CIO, shall:

(a) Review plans and results of operational testing to ensure adequate evaluation of cybersecurity for all VA IT acquisitions subject to oversight;

(b) In coordination with VA CIO, ensure integration of IT operations and services activities into the RMF and provide the RMF TAG with input as appropriate or required; and

(c) Verify that an Information System Owner is appointed for all information systems and platform IT systems.

(7) **Under Secretaries, Assistant Secretaries and Other Key Officials** shall:

(a) Ensure that all VA information system and platform IT systems are categorized according to the guidelines provided in this handbook;

(b) Develop and issue guidance for platform IT systems that reflects operational and environmental demands as needed;

(c) Ensure VA IT under their authority comply with the RMF;

(d) Ensure participation in the RMF TAG; and

(e) Ensure that contracts and other agreements include specific IT security requirements in accordance with this handbook.

(8) **Senior Agency Official for Privacy (SAOP)** shall:

(a) Review and approve, in accordance with Federal Information Processing Standard (FIPS) Publication 199 and NIST SP 800-60, the categorization of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of Personally Identifiable Information (PII);

(b) Review the authorization package for information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII, to ensure that privacy risks are managed prior to system authorization; and

(c) Determine whether additional measures are required to manage privacy risks prior to leveraging the authorization.

(9) **VA Enterprise Architect** shall:

(a) Be responsible for strategies, standards, and plans that have been developed for achieving an assured, integrated, and survivable information enterprise;

(b) Provide guidance at a design and architectural level for information system security engineering service;

(c) Assist in the development of VA architecture and engineering to support the RMF and indirectly, authorization decisions); and

(d) Advise AOs, Information System Security Officers, and the Risk Executive Function on a range of security-related issues including, for example, information system boundaries, assessing severity of information system weaknesses and deficiencies, Plan of Action and Milestones (POA&M), risk mitigation approaches, security alerts, and potentially adverse effects of identified vulnerabilities

(10) **Risk Management Framework Technical Advisory Group (RMF TAG)** will provide implementation guidance for the RMF by interfacing with VA IT,

cybersecurity community of interest, and other entities. The RMF TAG shall:

(a) Provide detailed analysis and authoring support for the Information Security Knowledge Service;

(b) Recommend changes to security controls, security control baselines, VA assignment values, associated implementation guidance, and assessment procedures to the VA CIO;

(c) Recommend changes to cybersecurity risk management processes to the VA CIO;

(d) Advise VA forums established to resolve RMF priorities and cross-cutting issues;

(e) Develop and manage automation requirements for VA services that support the RMF; and

(f) Develop guidance for facilitating RMF reciprocity throughout VA.

(11) **Information System Security Officer** (ISSO) has authority and responsibility to establish and manage a coordinated security assessment process for information technologies governed by the VA cybersecurity program and shall:

(a) Review and recommend guidance of the RMF within the VA cybersecurity program;

(b) Track the assessment and authorization status of information systems and platform IT systems governed by the VA cybersecurity program;

(c) Identify and recommend changes and improvements to the security assessment process, security test and evaluation, and risk assessment methodology, including procedures, risk factors, assessment approach, and analysis approach to the RMF TAG for inclusion in the Information Security Knowledge Service;

(d) Serve as the single cybersecurity coordination point for joint or VA-wide programs that are deploying information technologies to VA enclaves;

(e) Maintain and report information system and platform IT systems assessment and authorization status and issues in accordance with VA guidance;

(f) Coordinate with the information system security manager to ensure security issues are addressed appropriately;

(g) Collect and maintain data as needed to meet system cybersecurity reporting;

(h) Communicate the value of IT security throughout all levels of the organization stakeholder;

(i) Maintain cooperative relationships with business partners or System Owners of other interconnected systems;

(j) Verify and validate, in conjunction with the Information System Owners and managers, that appropriate security measures are implemented and functioning as intended;

(k) Ensure that protection and detection capabilities are acquired or developed within Area of Responsibility (AOR) using the information system security engineering approach and that these capabilities are consistent with organization-level cybersecurity architecture;

(l) Manage local information security programs and serve 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);

(m) Identify alternative information compensating controls to address organizational security objective;

(n) Identify IT security program implications of new technologies or technology upgrades;

(o) Interpret and recommend security requirements relative to the capabilities of new information technologies;

(p) At a local level, interpret patterns of noncompliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise cybersecurity program;

(q) Monitor information security data sources to maintain organizational situational awareness;

(r) Monitor the system and its environment of operation in close coordination with the Information System Owner;

(s) Monitor compliance with the security awareness training requirements for each employee and contractor;

(t) Serve as the liaison to the VA Training Manager to ensure security awareness training is provided within their AOR;

(u) Coordinate, monitor, and conduct periodic reviews to ensure compliance with the VA National or Contractor Rules of Behavior (RoB) requirement for users of VA information systems and VA information;

(v) Collaborate with the 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;

(w) Participate in security self-assessments, external and internal audits of system safeguards and program elements, and in Assessment & Authorization (A&A) of the systems supporting the offices and facilities within their AOR;

(x) Assess the security impact of system changes and providing recommendations of those changes;

(y) Collaborate in the development and maintenance of information System Security Plan (ISSP) and system risk analysis in coordination, advisement, and participation with the System Owner;

(z) Provide cybersecurity and supply chain risk management guidance within AOR for the development of Continuity of Operations Plans (CONOPs);

(aa) Ensure that cybersecurity awareness and training are provided to IT personnel commensurate with their responsibilities, and Rules of Behavior (RoB) are signed in accordance to cybersecurity guidelines, processes and requirements;

(bb) Provide system-related input on cybersecurity requirements to be included in statements of work and other appropriate procurement documents, as appropriate;

(cc) Define and provide security and privacy requirements for the system, and the environment of operation to the System Owner;

(dd) Recognize and notify the VA-CSOC of any confirmed or suspected incident within one hour of discovery of the potential incident and assisting in the investigation, if necessary, in accordance with VA policy;

(ee) Recommend resource allocations required to securely operate and maintain an organization's cybersecurity requirements;

(ff) Recommend and assist in the development of local security policies and procedures, coordinate review and approval of those policies and procedures, and review compliance;

(gg) Responsible for assisting in physical and environment protection and personnel security and managing corrective measures as the result of a cybersecurity incident or discovery of a vulnerability;

(hh) Ensure compliance with Federal security requirements and VA security policies;

(ii) Collaborate with facility Privacy Officers and others as appropriate for the implementation and assurance of reasonable safeguards as required by the Privacy Act, the HIPAA Privacy and Security Rules, and other Federal privacy statutes;

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

(kk) Promote awareness of local security issues among management and ensure sound security principles are reflected in the organization's vision and goals;

(ll) Oversee local policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies;

(mm) Participate in the Risk Governance process to provide security risks, mitigations, and input on other technical risk;

(nn) At a local level, evaluate the effectiveness of the procurement function in addressing information security requirements, and supply chain risks through procurement activities and recommend improvements;

(oo) Work with System Owner to forecast ongoing service needs to ensure security assumptions are integrated appropriately; and

(pp) Ensure that security policies and procedures are integrated into the System Security Plan and Risk Analysis processes and documents for the protection of critical dependencies (heating, ventilation & air conditioning (HVAC), electricity, water, sewage, badging etc.).

(12) **Information System Security Manager** (ISSM) advises appropriate AO of changes affecting the VA's cybersecurity posture and shall:

(a) In coordination with key stakeholders, assist with the creation of the organization's information security plans and policies;

(b) In coordination with Information System Owners, evaluate cost/benefit, economic, and risk analysis in decision-making process;

(c) Report the security and privacy posture of the system to the AO and other organizational officials on an ongoing basis in accordance with VA RMF strategy;

(d) Provide guidance when it comes to analyzing and evaluating networks and security vulnerabilities, and managing security systems such as anti-virus, firewalls, patch management, intrusion detection, and encryption daily;

(e) Coordinate with organizational managers to ensure a coherent, coordinated, and holistic approach to security across the operational units;

(f) Ensure that cybersecurity inspections, tests, and reviews are coordinated for the network environment;

(g) At all levels of the organization, interpret patterns of noncompliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise's cybersecurity program;

(h) Ensure that security improvement actions are evaluated, validated, and implemented as required;

(i) Participate in an information security risk assessment during the Security Assessment and Authorization process; and

(j) Define the operating unit's information security compliance/assessment program to include the development, management, and reporting of POA&Ms.

(13) **Authorizing Officials (AOs)** are selected from senior leadership positions within business owner and mission owner organizations to promote accountability in authorization decisions that balance mission and business needs and security concerns. AOs shall:

(a) Review security and business risk and provide risk-based decisions (acceptance or rejection) on behalf of the Department;

(b) Ensure all appropriate RMF tasks are initiated and completed, with appropriate documentation, for assigned information systems and platform IT systems;

(c) Monitor and tracking overall execution of CCI-level POA&M;

(d) Promote reciprocity to the maximum extent possible; but

(e) Not delegate authorization decisions to the AO designated representative.

(14) **Authorizing Official Designated Representative (AODR)**, acting on behalf of the AO shall:

(a) Review security and business risks and make risk-based decision recommendations for AO consideration;

(b) Coordinate and conduct the day-to-day activities associated with managing risk to information systems and organizations;

(c) Carry out many of the activities of the AO related to the execution of the RMF; however

(d) The only activity that cannot be delegated by the AO to the designated representative is the authorization decision and signing of the associated authorization decision document (i.e., the acceptance of risk).

(15) **Information System Owner**, in alignment with the AO chain of command for the Department, must have a full understanding of the SDLC process and shall:

(a) Receive security assessment results from the assessor to ensure accuracy, take appropriate steps to reduce or eliminate vulnerabilities, and submit completed authorization packages to AO for adjudication;

(b) Obtain an ISSO for each assigned information system or platform IT system with the support, authority, and resources to satisfy the responsibilities established in this handbook;

(c) Categorize systems in accordance with FIPS 199 and document the categorization in the appropriate document;

(d) Assist in the overall development, maintenance, and tracking of the security plan for assigned information system and platform IT systems, to include identification of applicable CCIs (Common security controls owner performs this function for inherited controls.);

(e) Monitor the implementation and compliance of the VA approved Continuous Monitoring strategy for the system;

(f) Ensure that accurate documentation of asset identification and authorization boundaries are properly identified, monitored, and maintained;

(g) Based on guidance from the AO, the Information System Owner informs appropriate organizational officials of the need to conduct the security authorization, ensures that the necessary resources are available for the effort, and provides the required information system access, information, and documentation to the security control assessor;

(h) Report the security and privacy posture of the system to the AO and other organizational officials in accordance with the organizational continuous monitoring strategy;

(i) Address the operational interests of the user community (i.e., users who require access to the system to satisfy mission, business, or operational requirements);

(j) Conduct initial remediation actions on the controls and reassess remediated controls;

(k) Based on guidance from AO, the Information System Owner informs appropriate organizational officials of the need to conduct security authorization;

(l) Lead in the development and maintenance of contingency/continuity plans and system risk analysis for all systems within their area of responsibility in coordination, advisement, and participation with the ISSO;

(m) Lead and/or assist in the procurement, development, integration, modification, operation, maintenance, and disposal of an information system;

(n) Evaluate cost/benefit, economic, and risk analysis in decision-making process;

(o) Periodically repeat 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;

(p) Ensure that all VA employees in their respective organizations complete required security and privacy awareness training initially and annually thereafter and ensure employees complete role-based training as required by their specific duties/responsibilities;

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

(r) Participate in risk assessments by coordination, advisement, and reviews as outlined in the System Security Plan;

(s) Ensure cybersecurity requirements from the ISSO are incorporated within environment of operation for the system;

(t) Recognize and notify the responsible ISSO and Privacy Officer of any suspected incidents within one hour upon discovery and assist in the investigation of incidents if necessary;

(u) Identify requirements for resources needed to effectively implement technical security controls;

(v) In coordination with the ISSO, forecast ongoing service needs to ensure security assumptions are integrated appropriately; and

(w) Integrate security policies and procedures into continuity/contingency planning documents for the protection of critical dependencies (HVAC, electricity, water, sewage, badging etc.).

(16) **Chief Privacy Officer** shall assist in the development of the system-level privacy policies and procedures, and ensure compliance with VA privacy policies and procedures.

(17) **Privacy Officer** shall:

(a) Assist in the development of the system-level privacy policies and procedures, and ensure compliance with VA privacy policies and procedures;

(b) Monitor a system and its environment of operation to include developing and updating privacy plans, working in conjunction with the ISSO; and

(c) In coordination with the Information System Owner, ISSO and other Privacy Services Office stakeholders, assess and submit a Privacy Impact Assessment (PIA) and Privacy Threshold Analysis (PTA) when required.

(18) **Information System Security Engineer** shall:

(a) Capture and refine security requirements for systems and ensure that the requirements are effectively integrated into systems and system elements through security or privacy architecting, design, development, and configuration; and

(b) Implement any activity associated with protecting information and information systems from unauthorized system activity or behavior to provide confidentiality, integrity, and availability.

(19) **Security Control Assessors** are appointed under the CISO and shall:

(a) Conduct an onsite assessment of the security controls employed within 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);

(b) Provide an assessment of the severity of weaknesses or deficiencies discovered in the information system and its environment of operation through the onsite assessment and recommend corrective actions to address identified vulnerabilities;

(c) Prepare a security assessment report containing the results, findings, and recommendations from the assessment and provide the results to the System Owner and to the Office of Information Security (OIS) ; and

(d) Conduct and/or monitor risk assessments of continuous monitoring tools.

(20) **Information Security Architect** shall:

(a) Serve as the primary liaison between the Enterprise Architect and the Information Systems Security Engineer and coordinate with System Owners, Common Control Providers, and Information System Security or Privacy Officers on the allocation of controls**;**

(b) In coordination with ISSOs or Privacy Officers, advise AOs, CIOs, Senior Accountable Officials for Risk Management or Risk Executive Function, Senior Agency Information Security Officers, and SAOPs on a range of security and privacy issues; and

(c) Be generally responsible for aspects of the enterprise architecture that protect information and information systems from unauthorized system activity or behavior to provide confidentiality, integrity, and availability.

(21) **Risk Executive Function** is an individual or group within an organization that provides a comprehensive, organization-wide approach to risk management. The VA Secretary may choose to retain the Risk Executive Function, or to delegate the function. Membership within this function requires a mix of skills, expertise, and perspectives to understand the strategic goals and objectives of the VA organization, organizational missions/business functions, technical possibilities and constraints, and key mandates and guidance that shape VA operations. This role is an inherent U.S. Government function and is assigned to government personnel only. The group is led by the Senior Accountable Official for Risk Management and serves as the common risk management resource for stakeholders having a vested interest in the mission/business success of VA. The Risk Executive Function shall:

(a) Ensure that risk considerations for systems (including authorization decisions for those systems and the common controls inherited by those systems), are viewed from an organization-wide perspective regarding the organization's strategic goals and objectives in carrying out its core missions and business functions;

(b) Ensure that managing risk is consistent throughout the organization, reflects organizational risk tolerance, and is considered along with other types of risk to ensure mission/business success;

(c) Coordinate with senior leaders and executives to establish risk management roles and responsibilities, manage threat, vulnerability, and security and privacy risk (including supply chain risk) information for organizational systems and the environments in which the systems operate;

(d) Identify the organizational risk posture based on the aggregated risk from the operation and use of systems and the respective environments of operation for which the organization is responsible;

(e) Provide oversight for the risk management activities carried out by organizations to help ensure consistent and effective risk-based decisions; and

(f) Presume neither a specific organizational structure nor formal responsibility assigned to any one individual or group within the organization.

5. RISK MANAGEMENT OF INFORMATION TECHNOLOGY PRODUCTS, SERVICES, AND Platform information technology.

a. The Information System Security Officer (ISSO), with the review and approval of the responsible AO, is responsible for ensuring all products, services and platform IT have completed the appropriate evaluation and configuration processes prior to incorporation into or connection to an information system or platform IT system.

(1) Information Technology Products. IT products will be configured in accordance with applicable STIGs. STIGs are product-specific and document applicable federal policies and security requirements, as well as best practices and configuration guidelines. STIGs are associated with security controls through CCIs, which are decompositions of NIST SP 800-53 security controls into single, actionable, measurable items. Security Requirements Guides are developed by Defense Information Systems Agency (DISA) to provide general security compliance guidelines and serve as source guidance documents for STIGs. When a STIG is not available for a product, the DISA Requirements Guide and other NIST approved checklists published on the NIST checklist repository may be used. STIG and Security Requirements Guide compliance results for products will be documented as security control assessment results within a product-level security assessment report and reviewed by the responsible ISSO, Security Control Assessor (under the direction of the AO) prior to acceptance or connection into an authorized computing environment (e.g., an information system or platform IT system with an authorization). This review ensures products will not introduce vulnerabilities into the hosting information system or platform IT system, and maximizes testing and review results to minimize duplication of effort across VA. See the Information Security Knowledge Service for additional guidance on the review of products.

(2) Information Technology Services. In general, IT services are outside the service user organization’s authorization boundary, and the service user’s organization has no direct control over the application or assessment of required security controls. There are internal IT services and external IT services. VA organizations that use external IT services are typically not responsible for authorizing them (i.e., issuing an authorization decision). However, for use of external IT services, the VA must review the external assessment package, present the risk to the Department and AO for approval based on the signed Authority to Use (ATU).

(a) Internal IT services are delivered by VA Information Systems. VA organizations that use internal IT services must ensure the categorization of the VA Information System delivering the service is appropriate to the system and data utilized. Written agreements describing the roles and responsibilities of both the providing and the receiving organization are in place.

(b) VA organizations that use external IT services provided by a non-VA Federal government agency must ensure the categorization of the Information System delivering the service is appropriate to the confidentiality, integrity, and availability needs of the information and mission, and that the Information System delivering the service is operating under a current authorization from that agency. Interagency agreements or government statements of work for these external services must contain requirements for Service Level Agreements that include the application of appropriate security controls. The AO should review other Federal agency security packages and approve such packages for use by VA.

(c) VA organizations that use external IT services provided by a commercial or other non-Federal government entity must ensure the security protections of the Information System delivering the service is appropriate to the confidentiality, integrity, and availability needs of the VA organization's information and mission via the Enterprise Mission Assurance Support Services (eMASS) tool. VA organizations must perform categorization in accordance with FIPS 199 and tailor appropriately to determine the set of security and privacy controls to be included in requests for proposals. VA organizations will assess the adequacy of security proposed by potential service providers and accept the proposed approach, negotiate changes to the approach to meet VA needs, or reject the offer. The accepted security approach must be documented in the resulting contract or order.

(d) VA organizations contracting for external IT services in the form of commercial cloud computing services must comply with VA cloud computing policy, VA Handbook 6517, Risk Management Framework for Cloud Computing Services.

(3) Platform Information Technology. Platform IT that does not rise to the level of a platform IT system may be categorized using FIPS 199 with the resultant security and privacy control baselines tailored as needed. Otherwise, the specific cybersecurity needs of platform IT must be assessed on a case-by-case basis and security and privacy controls applied as appropriate. These include computer resources, both hardware and software, that are physically a part of, and are

essential to the mission performance of cyber-physical systems (e.g. medical devices).

6. PROCEDURES.

a. The RMF process is applicable to all information system and platform IT systems, as well as VA-partnered systems where it has been agreed that VA standards will be followed. IT below the system level (e.g., products, IT services) will not be subjected to the full process. However, IT below the system level must be securely configured in accordance with applicable VA policies and security controls, documented in the authorization package for acceptance or connection into an authorized computing environment (i.e., an authorized information system or platform IT system).

b. There are seven steps in the RMF; a preparatory step to ensure that organizations are ready to execute the process and six main steps. All seven steps are essential for the successful execution of the RMF. The steps are:

(1) **PREPARE.**

(a) The Prepare step is intended to leverage activities already being conducted within security, privacy, and supply chain programs to emphasize the importance of having VA-wide governance and the appropriate resources in place to enable the execution of cost-effective and consistent risk management processes across VA. The Prepare step assists in the execution of the RMF from an organizational and a system-level perspective by establishing a plan and priorities for managing security and privacy risk.

(b) The organizational-level prepare steps include:

i. Risk Management Roles. Identifying individuals within VA and assign key roles for executing the RMF. The roles and responsibilities may include personnel that are internal or external to VA;

ii. Risk Management Strategy. Developing a risk management strategy for the VA that includes a determination and expression of VA risk tolerance. The risk management strategy guides and informs risk-based decisions including how security and privacy risk is framed, assessed, responded to, and monitored;

iii. Organizational Risk Assessment. Developing a VA-wide risk assessment or update to current risk assessment. Risk assessment at the organization level leverages aggregated information from system-level risk assessment results, continuous monitoring, and any strategic risk considerations relevant to the VA;

iv. Organizationally-Tailored Control Baselines and Cybersecurity Framework Profiles. Tailoring control baselines for VA-wide use. A VA-wide tailored baseline provides a fully specified set of controls, control enhancements, and supplemental guidance derived from established controls baselined in

Committee on National Security Systems Instruction (CNSSI) 1253, encompassed in the Cybersecurity Framework Profile;

v. Common Control Identification. Identifying, documenting and publishing common controls that are available for inheritance by information system and platform IT systems. A particular requirement may not be fully met by a common control. In such cases, the control is considered a hybrid control and is noted as such by VA, including specifying which parts of the control requirements are provided for inheritance by the common control and which parts are to be provided at the system level;

vi. Impact-Level Prioritization. Prioritizing organizational systems with the same impact level. This task is carried out only after VA systems have been categorized; and

vii. Organizational Continuous Monitoring Strategy. Developing and implementing a VA-wide strategy for monitoring control effectiveness which identifies the minimum monitoring frequency for implemented controls across VA.

(c) The system-level prepare steps include:

i. Mission or Business Focus. Identifying the missions, business functions, and mission/business processes that the system is intended to support;

ii. System Stakeholders. Identifying stakeholders who have an interest in the design, development, implementation, assessment, operation, maintenance, or disposal of the system;

iii. Asset Identification. Identifying assets that require protection;

iv. Privacy Assessment. Determine the privacy risks for systems that access or use Personal Identifiable Information (PII)/Personal Health Information (PHI). Complete PTA of any system that will use or access PII/PHI. If PII/PHI are identified, then a PIA must be completed. Contact the ISO for assistance with identification of risks and compliance documentation.

v. Authorization Boundary. Determining the authorization boundary of the system; whether logical or geographical, for the purposes of obtaining an Authorization to Operate (ATO).

vi. Information Types. Identifying the types of information to be processed, stored, and transmitted by the system;

vii. Information Life Cycle. Identifying and understanding all stages of the information life cycle for each information type of information processed, stored, or transmitted by the system;

viii. Risk Assessment. Conducting a system-level risk assessment and update the risk assessment results in accordance with the organizational continuous monitoring strategy;

ix. Requirements Definition. Defining the security and privacy requirements for the system and the environment of operation;

x. Enterprise Architecture. Determining the placement of the system within the enterprise architecture;

xi. Requirements Allocation. Allocating security and privacy requirements to the system and to the environment of operation; and

xii. System Registration. Registering the system with organizational program or management offices.

(4) **CATEGORIZE SYSTEM.**

(a) System Description. Document the characteristics of the system.

i. These include system design and requirements documentation; authorization boundary information; list of security and privacy requirements allocated to the system, system elements, and the environment of operation; physical or other processes controlled by system elements; system element information; system component inventory; system element supply chain information, including inventory and supplier information; security categorization; data map of the information life cycle for information types processed, stored, and transmitted by the system; information on system use, users, and roles.

(b) Security Categorization. Categorize the system and document the security categorization results.

i. In the categorization process, the System Owner identifies the potential impact (low, moderate, or high) resulting from loss of confidentiality, integrity, and availability if a security breach occurs. 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. Completion of a PTA and PIA, based on FIPS 200, aids in appropriate system categorization selection.

ii. For acquisition programs, the categorization will be documented as a required capability in the initial capabilities document, the capability development document, the capabilities production document, and the cybersecurity strategy within the program protection plan. Specific guidance on determining the security category for information types and information systems is included in the Information Security Knowledge Service.

iii. To determine a National Security System (NSS), the following must be adhered to:

a. Determine impact values for the information types processed, stored, transmitted or protected by the information system and for the system; and

b. Identify overlays that apply to the information system and its operating environment to account for additional factors that influence the selection of security controls.

iv. In preparation for selecting and specifying the appropriate security controls for organizational information systems and their respective environments of operation, organizations categorize their information and information system. To categorize the information and information system, complete the following activities:

a. Identify all the types of information processed, stored, or transmitted by an information system, determine their provisional security impact values, and adjust the information types' provisional security impact values; and

b. Determine the security category for the information system and make any necessary adjustments. The security category of a system can be changed or modified to reflect management decisions to allocate more stringent or less stringent security controls.

v. Selecting the applicable initial security and privacy control baseline from FIPS 200 based on the information system categorization. These security and privacy control baselines identify the specific security controls from NIST SP 800-53 that are applicable to the system categorization. Information System Owners select one of three sets of security control baselines 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 website.)

(c) Security Categorization Review and Approval. Review and approve the security categorization results and decision.

(5) **SELECT SECURITY CONTROLS.**

(a) Control Selection. Select the controls for the system and the environment of operation.

i. Common controls are selected as "common" and provided via the Information Security Knowledge Service based on risk assessments conducted by these entities at the Tier 1 (Organization) and Tier 2 (Mission/Business Processes) levels.

ii. By identifying the security and privacy controls that are provided by the organization as common solutions for information system and platform IT systems and documenting the assessment and authorization of the controls in a security plan (or equivalent document), individual systems within those organizations can leverage these common controls through inheritance. CCIs 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 the Information Security Knowledge Service.

iii. All other controls are considered hybrid controls. See the Information Security Knowledge Service for identification of common controls for VA and additional information on how they are documented within the security authorization package.

iv. Identify the security and privacy control baseline for the system, as provided in FIPS 200, and document it in the security plan. The baselines identified in FIPS 200 address the overall threat environment for VA Information Systems and Platform IT systems. In this step, the applicable security controls baseline and relevant overlays for a system are assigned. See FIPS 200 and the Information Security Knowledge Service for detailed procedures.

v. System Owner identifying overlays that apply to the information system or platform IT system due to information contained within the system or environment of operation. Overlays may add or subtract security controls, or provide additional guidance regarding security controls, resulting in a set of security and privacy controls applicable to that system that is a combination of the baseline and overlay. The combination of baselines and overlays address the unique security protection needs associated with specific types of information or operational requirements. Overlays reduce the need for ad hoc or case-by-case tailoring (modifying) by allowing communities of interest to develop standardized overlays that address their specific needs and scenarios. Access to the overlays, and guidance regarding how to determine which overlays may apply, are included in the Information Security Knowledge Service. The Information Security Knowledge Service is the approved source for detailed security control descriptions, implementation guidance and assessment procedures. Examples of overlays include:

a. Unique mission environments (e.g., space platform overlay);

b. Platform IT systems (including special categories of Platform IT systems (medical devices), such as Industrial Control Systems or tactical platform IT systems); and

c. Systems containing PII or systems containing PHI as defined in HIPAA.

vi. For systems that have been determined to be an NSS, the Security Control Selection is a two-step process:

a. Select the initial security and privacy control set.

b. Tailor the initial security and privacy control set.

vii. Once the security category of the information system is determined, organizations begin the security control selection process. To identify the initial security and privacy control set, complete the following activities:

a. Select the baseline security and privacy controls corresponding to the security category of the system (i.e., the impact values determined for each security objective [confidentiality, integrity, and availability]).

b. Apply any overlay(s) identified as applicable during security categorization. If the use of multiple overlays results in conflicts between the application or removal of security controls, the AO (or designee), in coordination with the Information Owner/Steward, Information System Owner, and Risk Executive Function resolves the conflict.

c. Document the initial security and privacy control set and the rationale for tailoring security controls in the security plan.

(b) Control Tailoring. Tailoring decisions must be aligned with operational considerations and the environment of the information system or platform IT system and should be coordinated with mission owner(s). Security and privacy controls should be added or removed only as a function of specified, risk-based determinations. Tailoring decisions, including the specific rationale (e.g., mapping to risk tolerance) for those decisions, are documented in the security plan for the system. Every selected control must be accounted for. The tailoring process includes:

i. Applying scoping considerations to the initial baseline of security and privacy 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. Reference NIST SP 800-53B for guidance on how to apply scoping considerations to tailor the baselines.

ii. Selecting or specifying compensating controls to adjust the initial set of security controls to obtain an equivalent set deemed to be more feasible to implement.

(c) Control Allocation. Allocate security and privacy controls to the system and to the environment of operation. After applying the scoping considerations, a compensating control(s) or control enhancement(s) may be employed in lieu of the normal baseline controls. 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.

i. To facilitate selection of appropriate compensating controls for the system, compensating controls may be employed only under the following conditions:

a. A baseline control is selected; and

b. A rationale is supplied and documented in the security plan that explains why the baseline control could not be used and how the compensating control provides equivalent protection.

ii. Organization-Defined Parameters. Specifying organization-defined parameters in the security and privacy controls via explicit assignment and selection statements to complete the definition of the tailored set of security and privacy controls:

iii. Organization-Defined Parameters are portions of security and privacy controls containing VA management-defined parameters. VA identifies Organization-Defined Parameters for common, hybrid, and system-specific controls in the Information Security Knowledge Service.

iv. Common Organization-defined Parameters are program management controls and have been determined to be applicable to all OIT systems. OIT management is responsible for implementing and managing these controls.

v. Hybrid Organization-defined Parameters are appropriate for all VA Systems. The Information System Owner documents any deviation from these values or from the security and privacy controls in the security plan.

vi. System-Specific Organization-defined Parameters are recommended security and privacy control values for systems. Information System Owners should tailor these Organization-Defined Parameters to align with the specific operating conditions of the information system as described above.

vii. Supplementing Tailored Baseline Control Sets are only if necessary. These are supplemental controls or control enhancements that consider local conditions, including environment of operation, organization-specific security requirements, specific threat information, cost-benefit analyses, or special circumstances, and are based on risk assessments consistent with NIST SP 800-30.

a. If the tailored security and privacy controls are not adequate, additional security and privacy controls or control enhancements may be needed and added to the baseline. When this becomes necessary, CCIs from CNSSI 1253 should be considered first. The following conditions are examples that might require supplemental controls to be added:

(1) Cross-Domain Solutions: Security and privacy 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 controls, and other security protections.

(2) Mobility: Security and privacy 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.

(3) Highly Sensitive Information and Information Sharing: Additional security and privacy controls and enhancements may be needed to protect privileged access in the event access to sensitive information, including PII and PHI, is required.

(4) Application-Layer Security: Security and privacy 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.

b. 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:

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

(2) Prohibiting access to information by removing network components that permit access (e.g. air-gapping); and

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

c. Control enhancements and security functionality specific to the information system may also be governed by additional regulations, requirements, standards, and policies.

viii. 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:

a. 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.

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

c. 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.

d. 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.

e. Information and System Non-Persistence: Security and privacy control baselines assume that information has some level of persistence. When information persistence is limited in duration, security and privacy 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.

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

g. Technology-Related Considerations: Security controls that refer to specific technologies (e.g., wireless, cryptography, public key infrastructure) 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.

h. Security Objective-Related Considerations: Security and privacy 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;

(2) Is supported by an assessment of risk; and

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

i. Policy/Regulatory-Related Considerations: Security and privacy controls related to laws, policies, standards, or regulations (e.g., PTA, PIA) are required only if they are consistent with the types of information and information systems covered by the applicable laws, policies, standards, or regulations.

j. 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.

(d) Documentation of Planned Control Implementations. VA Information System and platform IT systems must have a security plan that provides an overview of the security requirements for the system and describes the security controls in place or plan for meeting those requirements. The security plan should include implementation status, responsible entities, resources, and estimated completion dates. Security plans may also include, but are not limited to, a compiled list of system characteristics or qualities required for system registration, and key security-related documents such as a risk assessment, PIA, system interconnection agreements, contingency plan, security configurations, configuration management plan, and incident response plan.

(e) Continuous Monitoring Strategy System. Develop and implement a system-level strategy for the continuous monitoring of the effectiveness of security controls employed within or inherited by the system and monitoring of any proposed or actual changes to the system and its environment of operation. The strategy must include the plan for annual assessments of a subset of implemented security controls, and the level of independence required of the assessor. The breadth, depth, and rigor of these annual assessments should be reflective of the security categorization of the system and threats to the system. The system-level continuous monitoring strategy must conform to all applicable published VA-level continuous monitoring strategies in recommendation to the Information Security Knowledge Service guidelines.

(f) Plan Review and Approval. The approval of the security plan establishes the level of effort required to successfully complete the remainder of the steps in the RMF and provides the basis of the security specification for the acquisition of the system, subsystems, or components. For acquisition programs, approval should be accomplished before the issuance of the design and development request for proposals. If the security plan is deemed unacceptable, the AO or AODR sends the plan back to the Information System Owner for appropriate action. The AO or AODR approval of the security plan must be documented in the security plan.

(6) **IMPLEMENT SECURITY CONTROLS.**

(a) Control Implementation. Implement the security controls specified in the security plan in accordance with VA implementation guidance found in the Information Security Knowledge Service.

i. Products used within an information system or platform IT system boundary will be configured in accordance with VA enterprise baselines based on applicable NIST approved checklists tailored for VA.

ii. Information System Owners will implement and test VA-approved security controls as specified in the approved security plan and according to DISA STIG.

iii. Security controls are implemented consistent with VA and security architecture and standards, employing system and software engineering methodologies, security engineering principles, and secure coding techniques. VA recommended security control implementation guidance is available in the Information Security Knowledge Service.

iv. The Project Manager and System Owner must ensure early and ongoing involvement by information system security engineers. Information system security engineer(s) must translate security controls into system specifications, ensure the successful integration of those specifications into the system design, and ensure security engineering tradeoffs do not impact the ability of the system to meet the fundamental mission requirements. This includes ensuring that technical and performance requirements derived from the assigned security controls are included in requests for proposals and subsequent contract documents for design, development, production, and maintenance.

v. The proposed system security design must be addressed in preliminary and critical design reviews. System security design should address security controls that may be satisfied through inheritance of common controls. In addition, mandatory configuration settings are established and implemented on IT products in accordance with Federal and VA policies.

vi. Program Managers for programs acquiring information system or platform IT systems must integrate the security engineering of cybersecurity requirements and cybersecurity testing considerations into the program's overall systems engineering process. The Program Manager must document and update this approach in the program's systems engineering plan and program protection plan throughout the system development life cycle, systems engineering, development test and evaluation, and program protection plan processes.

vii. Document the security control implementation in accordance with VA implementation guidance found in the Information Security Knowledge Service in the security plan, providing a description of the control implementation if not implemented in accordance with the Information Security Knowledge Service guidance. This description should include planned inputs, expected behavior, and expected outputs. See the Information Security Knowledge Service for specific control documentation requirements, including required artifacts, templates, and best practices.

viii. Security controls that are available for inheritance (e.g. common controls) by information system and platform IT systems will be identified and have associated compliance status provided by hosting or connected systems.

(b) Update Control Implementation Information. Document changes to planned control implementations based on the “as-implemented” state of controls.

(7) **ASSESS SECURITY CONTROLS.**

(a) Assessor Selection. Select the appropriate assessor or assessment team for the type of control assessment to be conducted.

(b) Assessment Plan. Develop, review, and approve a plan to assess the security and privacy controls. An assessment methodology is provided in the Information Security Knowledge Service as a model for use or adaptation. OIT will use this model, or justify the use of another risk assessment methodology to assess the impact on reciprocity with other Federal agencies. The risk assessment is one element to be used to determine the level of overall system cybersecurity risk and as a basis for a recommendation for risk acceptance or denial. Information systems and platform IT systems must:

i. Ensure security control assessment activities are coordinated with the following: interoperability and supportability certification efforts, development test and evaluation events, and operational development test and evaluation events; and

ii. Ensure the coordination of activities is documented in the security assessment plan and the program test and evaluation documentation to maximize effectiveness, reuse, and efficiency. Where appropriate, integrated testing should include the evaluation of survivability, assessment of controls, and certification testing, as well as development test and evaluation and operational development test and evaluation.

(c) Control Assessments. Assess the security controls in accordance with the security assessment plan and VA assessment procedures. For newly acquired or already existing VA IT, assessment procedures are used to verify that a security control has been properly implemented. Security Requirements Guide, Center for Interent Security Benchmarks and STIG compliance results will be documented and used as part of the overall security control assessment. The Information Security Knowledge Service is the authoritative source for security control assessment procedures. Actual results are recorded in eMASS, which generates the security assessment report (SAR). POA&Ms are developed as part of the security authorization package, along with any artifacts produced during the assessment (e.g., output from automated test tools or screen shots that depict aspects of system configuration). For inherited security controls, assessment test results and supporting documentation are maintained by the providing system and are made available to Security Control Assessors of receiving systems on request. For common controls inherited from the enterprise, instructions for documenting compliance are provided in the Information Security Knowledge Service. Security Control Assessors will not give POA&Ms to the system for an inherited control deficiency, however they will consider the deficiency in the overall security risk of the assessed system.

(d) Security Assessment Reports. The security assessment report documents the findings of compliance with assigned security controls based on actual assessment results. It addresses security controls in a non-compliant status, including existing and planned mitigations. A security assessment report is always required before an authorization decision. If a compelling mission or business need requires the rapid introduction of a new information system or platform IT system, control assessment and a security assessment report are still required.

i. If no vulnerabilities are found through the process of executing the assessment procedures, the security control is recorded as compliant. If vulnerabilities are found, the control is recorded as non-compliant in the security assessment report and POA&M, with sufficient explanation.

ii. Security controls that are not technically or procedurally relevant to the system, as determined by the AODR, will be recorded as not applicable with sufficient justification.

iii. The status and results of all security control assessments assigned to an authorization boundary set will be recorded in the security assessment report. VA implementation guidance and assessment procedures are available in the Information Security Knowledge Service. Assessment procedures used that are not in accordance with the Information Security Knowledge Service will be documented fully in the security assessment report.

iv. Vulnerability severity values are assigned to all non-compliant controls as part of the security control analysis to indicate the severity associated with the identified vulnerability. Vulnerability severity values are identified in NIST SP 800-30. Vulnerability severity values for security controls are informed by assessment at the CCI level. If a control has a STIG or Security Requirements Guide associated through CCIs, the vulnerabilities identified by STIG or Security Requirements Guide assessments will be used to inform the overall vulnerability severity value for the security control.

v. Non-compliant controls are subjected to a risk assessment process that considers multiple factors in producing the risk level. As described in NIST SP 800-30, these factors include, but are not limited to:

a. A determination that a credible or validated threat source and potential event exists that is capable of, and likely to exploit vulnerabilities in the implementation of the control;

b. Vulnerability severity level and pre-disposing conditions. This includes the Security Control Assessor’s estimate of the adequacy of existing mitigations or compensating controls to address the vulnerability and mitigations provided by the hosting enclave, service provider, or other protective measures;

c. The cybersecurity attribute (i.e., confidentiality, integrity, or availability) and associated categorization impact level (high, moderate, low) related to the control; and

d. The security assessment report must address all non-compliant controls and clearly communicate system cybersecurity risk, and any recommendations for special instructions to accompany the authorization decision.

(e) Remediation Actions. The System Owner conducts initial remediation actions on security controls based on the findings and recommendations of the security assessment report and the Security Control Assessor reassesses the remediated control(s), as appropriate. System Owners and ISSOs review assessment findings and determine the severity or seriousness of the findings and whether the findings are sufficiently significant to be worthy of further investigation or remediation. If weaknesses or deficiencies are corrected, the remediated components are reassessed for effectiveness and to determine the extent to which they are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system. Original assessment results are not changed; the security assessment report is updated with the findings from the reassessment.

(f) Plan of Action and Milestones (POA&Ms). System Owners and Common Control Providers will prepare the POA&Ms based on the findings and recommendations of the assessment reports. A full discussion and templates for preparing a POA&M are provided in the Information Security Knowledge Service.

i. A POA&M:

a. Identifies tasks that need to be accomplished to remediate or mitigate vulnerabilities and type of weakness;

b. Specifies resources required to accomplish the elements of the plan and roles responsible; and

c. Includes milestones for completing tasks, milestone changes and their scheduled completion dates.

ii. POA&Ms are maintained throughout the system life cycle. Once posted to the POA&M, vulnerabilities will be updated after correction or mitigation actions are completed, but not removed.

iii. Inherited vulnerabilities must be addressed in the POA&M for the system.

iv. POA&Ms can be approved throughout a system’s life cycle.

v. POA&Ms must be monitored and tracked until identified security vulnerabilities have been corrected or remediated and the RMF documentation is appropriately adjusted.

(8) **AUTHORIZE SYSTEM.**

(a) Special System Configurations. Prior to authorizing a system, the following must be considered:

i. Cross Domain Solution. Cross Domain Solutions are typically deployed within the information system or platform information system authorization boundary on the system with the higher impact level and are included in the information system or platform IT system authorization. The AO responsible for the information or platform IT system must consider the security and privacy impact level in the overall authorization decision. The security requirements for the integrity of the information transfer must be considered and implemented based on the higher impact level of the connected information system or platform IT system.

ii. Unified Capabilities. Unified capabilities products are implemented inside the authorization boundaries of VA Information Systems and platform IT systems, and the unified capabilities product information assurance certification documentation is used to support the overall system assessment and authorization.

iii. Stand-Alone Systems. Stand-alone information system and platform IT systems are types of enclaves that are not interconnected to any other network. Stand-alone information system and platform IT systems do not transmit, receive, route, or exchange information outside of the system’s authorization boundary. They may range in size from a single workstation to multiple interconnected subsystems as long as they meet the foregoing criteria. Stand-alone information system and platform IT systems are authorized as any other information system and platform IT systems but assigned security control sets may be tailored (modified) as appropriate with the approval of the AODR. Stand-alone information system and platform IT systems must always be clearly identified as such in the authorization documentation. Additionally, identical stand-alone information system and platform IT systems that have identical security control implementation and approved baseline are to be deployed to multiple locations may be type authorized.

iv. Systems Operated by a Contractor or Other Entity on Behalf of VA. Externally-owned information system and platform IT systems that are dedicated to VA processing and are effectively under VA configuration control must be authorized as VA Information System and platform IT systems. A VA AO must render an authorization decision for this type of VA system prior to VA use. The following additional requirements apply:

a. Security responsibilities of the contractor or other entity must be made explicit in the contract or other binding agreement, along with any other performance and service-level parameters by which the VA entity will measure the cybersecurity performance of the system for the purpose of authorization;

b. Technical security of the externally-owned information system and platform IT systems is the responsibility of the contractor or other entity;

c. Responsibility for procedural and administrative security will be shared between the contractor or other entity and VA; and

d. Security requirements for such a system must be determined by the categorization and control selection process, just as for other VA Information Systems. Any required security controls that are not explicit in the contract or otherwise covered by a Service Level Agreement must be assessed as non-compliant. All such non-compliant security controls must be documented in a POA&M with an explanation as to why accepting the risk of operating the system with the control(s) in a non-compliant status is acceptable.

v. VA Partnered Systems. VA partnered systems are information systems or platform IT systems that are developed jointly by VA and non-VA mission partners, comprised of VA and non-VA Information Systems, or contain a mix of VA and non-VA information consumers and producers (e.g., jointly developed systems, multi-national or coalition environments, Cloud environments, or first responder environments). Security control selection, system authorization, and other risk management considerations for VA-partnered systems must be clearly defined via a formal partnership agreement: Memorandum of Agreement, Memorandum of Understanding, or Service Level Agreement. To the extent possible, the negotiated risk management approach should be aligned with the RMF. Regardless of the risk management approach employed, a VA AO must render an authorization decision for a VA-partnered system prior to VA use of the capability.

(b) Authorization Package. The security authorization package must be assembled and submitted for adjudication. The security authorization package must contain or provide links to the appropriate documentation for any security controls that are being satisfied through inheritance (e.g., security authorization packages including PTA and if applicable, PIA, contract documents, Memorandum of Agreement, and Service Level Agreement). The Contingency Plan, Disaster Recovery Plan, and Incident Response Plan are also required to be included in the authorization package. A complete list of required documents for the authorization package will be posted on the Information Security Knowledge Service and updated as necessary. The security authorization package is submitted for review and final acceptance.

(c) Risk Analysis and Determination. The risk to organizational operations (including missions, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation must be analyzed and determined. Consideration to the current security state of the system (as reflected by the risk assessment and recommendations provided in the security assessment report) must be weighed against the operational needs for the system. Weighing these factors, a final determination of risk to VA operations and assets, individuals, other organizations, and the Nation from the operation and use of the system must be rendered.

i. The Information Security Knowledge Service provides additional guidance and tools for conducting system authorization risk assessments.

ii. A VA authorization decision is expressed as an ATO, an Interim Authorization to Test, or a Denial of ATO. An information system or platform IT system is considered unauthorized if an authorization decision has not been made.

iii. If overall risk is determined to be acceptable and there are no non-compliant controls with a level of risk of “Very High” or “High”, then the authorization decision should be issued in the form of an ATO. An ATO decision must specify an authorization determination that is within three years of the authorization date unless the information system or platform IT system has a system-level continuous monitoring program compliant with VA continuous monitoring policy as issued.

iv. If non-compliant controls with a level of risk of “Very High” or “High” exist that cannot be corrected or mitigated prior to completion of Security Control Assessor or standing up the system, but overall system risk is determined to be acceptable due to mission criticality, then the authorization decision will be issued in the form of an ATO with conditions and only with permission of the responsible AO.

v. The ATO with conditions should specify an AO review period that is within six months of the authorization date. The POA&Ms supporting this ATO must document identified vulnerabilities and specify corrective actions to be completed before the review.

vi. If the system still requires operation with a level of risk of “Very High” or “High” after one year, the AO must again grant permission for continued operation of the system. This authority cannot be delegated below the VA AO. The AO must concur in writing or through certified digital/electronic signature that the security risk of continued system operation is acceptable due to mission criticality. The AO provides a copy of the concurrence and authorization decision document with supporting rationale to the VA Quality, Privacy, and Risk Board and the VA CISO. This authorization decision closely manages risk while allowing system operation.

vii. If the risk determination is being made to permit testing of the system in an operational information environment or with live data and the risk is acceptable, then the authorization decision should be issued in the form of an Interim Authorization to Test.

viii. The Information System Owner along with the ISSO must monitor and track the overall execution of system-level POA&Ms until identified security vulnerabilities have been corrected or remediated and the RMF documentation is appropriately adjusted.

ix. For full and independent operational testing, an ATO (rather than an Interim Authorization to Test) may be required if operational testing and evaluation is being conducted in the operational environment or on deployed capabilities. In this case, the ATO should be reviewed following operational testing and evaluation for modification as necessary in consideration of the operational test results.

x. All applicable security controls should be tested and satisfied before testing in an operational environment or with live data, except for those that can only be tested in an operational environment. In consultation with the Information System Owner or Program Manager, the AODR will determine which security controls can only be tested in an operational environment.

xi. If risk is determined to be unacceptable, the authorization decision should be issued in the form of a Denial of ATO. If the system is already operational, the AO will issue a Denial of ATO and stop operation of the system immediately. Network connections will be immediately terminated for any system issued a Denial of ATO. A Denial of ATO may also be issued coincidental to implementing a decommissioning strategy for a system.

xii. Documentation supporting an authorization decision will be provided in electronic form if requested by AOs of interconnecting information system and platform IT systems.

(d) Risk Response. Identify and implement a preferred course of action in response to the risk determined as defined within the system POA&M.

(e) Authorization Decision. Determine if the risk from the operation or use of the information system or the provision or use of common controls is acceptable. An authorization decision for information system or platform IT system cannot be made without completing the required assessments and analysis, as recorded in the security authorization package. Deploying organizations must provide the complete security authorization package to receiving organizations. Security authorization documentation will be posted to provide visibility of authorization status and documentation to planned receiving sites.

i. Type Authorization. The type authorization is used to deploy identical copies of an information system or platform IT system. This allows a single security authorization package to be developed for an archetype (common) version of a system. The system can then be deployed to multiple locations with a set of installation, security control and configuration requirements, or operational security needs that will be provided by the hosting enclave.

ii. Authorization with Multiple Authorizing Officials. This approach, also known as a joint authorization, is employed when multiple officials either from the same or different organizations, have a shared interest in authorizing a system:

a. The AOs collectively are responsible and accountable for the system and jointly accept the system-related security risks that may adversely impact organizational operations and assets, individuals, other organizations, and the Nation;

b. Organizations choosing a joint authorization approach are expected to work together on the planning and execution of RMF tasks, and to formally document their agreement and progress in implementing the tasks. Collaborating on the security categorization, selection of security controls, plan for assessing the controls to determine effectiveness, POA&Ms, and system-level continuous monitoring strategy is necessary for a successful joint authorization;

c. The specific terms and conditions of the joint authorization are established by the participating parties in the joint authorization, including, for example, the process for ongoing determination and acceptance of risk; and

d. The joint authorization remains in effect only as long as there is mutual agreement among AOs and the authorization meets the requirements established by Federal or organizational policies.

iii. Leveraging of an Existing Authorization. The final approach, leveraged authorization, is employed when a VA AO chooses to accept some or all of the information in an existing security authorization package generated by another Federal agency (referred to in this handbook as the “owning organization”) based on a need to use the same information resources (e.g., information system or services provided by the system). The VA AO reviews the owning organization’s security authorization package as the basis for determining risk to the leveraging organization before accepting the authorization. To the extent that a leveraged authorization includes an information system that creates, collects, uses, processes, stores, maintains, disseminates, discloses, or disposes of PII, the VA AO must consult the SAOP. The SAOP may determine that additional measures are required to manage privacy risks prior to leveraging the authorization. It is VA policy that the reciprocal acceptance of existing VA and other Federal agency and Department system authorizations (i.e., leveraged authorizations), and the artifacts contributing to the authorization decisions, must be employed to the maximum extent. This handbook and the Information Security Knowledge Service provide procedural guidance regarding reciprocity.

iv. Cybersecurity Reciprocity (referred to in this handbook as “reciprocity”) is an essential element in ensuring IT capabilities are developed and fielded rapidly and efficiently across the VA Information Enterprise. Applied appropriately, reciprocity reduces redundant testing, assessing, and documentation, as well as the associated costs in time and resources. The VA RMF presumes acceptance of existing test and assessment results and authorization documentation. In order to facilitate reciprocity, the following must be adhered to:

a. Information system and platform IT systems have only a single valid authorization. Multiple authorizations indicate multiple systems under separate ownership and configuration control.

b. Deploying systems with valid authorizations (from a VA organization or other Federal agency) are intended to be accepted into receiving organizations without adversely affecting the authorizations of either the deployed system or the receiving enclave or site. Deploying system Information System Owners and Program Managers must coordinate system security requirement with receiving organizations or their representatives early and throughout system development.

c. An authorization decision for information system or platform IT system cannot be made without completing the required assessments and analysis, as recorded in the security authorization package. Deploying organizations, for reciprocity with other Federal agencies, must provide the complete security authorization package to receiving organizations. Systems being deployed across VA IT will have security authorization documentation to provide visibility of authorization status to planned receiving sites.

d. The process for the receiving organization (VA or other Federal agency) to accept information system and platform IT systems is:

    (1) Review the complete security authorization package.

    (2) Determine the security impact of connecting the deploying system within the receiving enclave or site.

    (3) Determine the risk of hosting the deploying system within the enclave or website.

    (4) If the risk is acceptable, execute a documented agreement between deploying and receiving organizations (e.g., Memorandum of Understanding, Memorandum of Agreement, Service Level Agreement) for the maintenance and monitoring of the security posture of the system.

    (5) Document the acceptance by the receiving AO.

    (6) Update the receiving enclave or site authorization documentation for inclusion of the deployed system.

(7) Receiving organizations have the right to refuse deploying systems due to a security authorization package that introduces excessive risk to the enclave or site. Refusals must be documented by the refusing AO and provided to the deploying organization's Information System Owner or Program Manager, AO, and to the refusing organization's Information System Security Officer. Disputes should be resolved at the lowest possible level. Disputes that cannot be resolved will be raised to the next appropriate level.

(8) The cases below describe the proper application of VA policy on reciprocity in the most frequently occurring scenarios:

(a.) The receiving site executes the acceptance process. Issues identified during the acceptance process will be negotiated between the deploying Information System Owner or Program Manager and the receiving enclave or site Information System Owner. Following resolution of any issues, which may result in modifications in either the deploying system or the receiving environment, the deploying system is allowed to be incorporated or connected to the hosting environment. The nature or magnitude of any modifications to the deploying system or receiving site may result in additional assessment activities, but the deploying system and receiving environment retain their own separate authorizations. It is the joint responsibility of the Information System Owners of deploying systems and the receiving sites to ensure the system design reflects the security, technical and threat environment of the planned receiving sites, as well as leveraging any common controls. Unresolved issues, disputes, and refusals are addressed and acceptance by the receiving AO is documented.

(9) The VA Quality, Privacy, and Risk Board may make an enterprise level risk acceptance determination for authorized enterprise systems. If the VA Quality, Privacy, and Risk Board accepts the risk on behalf of the VA Information Enterprise, the receiving organization cannot refuse to deploy the system.

(10) A system is authorized by another U.S. Government agency and a VA organization takes ownership of the system for deployment into VA IS or enclaves. Systems with an existing authorization issued by other Federal agencies require authorization by a VA AO in accordance with this handbook prior to operating. The receiving enclave or site will maximize reuse of the external agency's security authorization package to support the authorization by the VA AO. Following the issuance of a VA authorization, subsequent deployment of the system by the VA Information System Owner or Program Manager to VA receiving sites will follow the review and acceptance process described.

(11) A system is authorized by a VA organization for its own use, and subsequently provided to another VA organization for it to use as a separately owned, managed and maintained system. In this case, the receiving organization becomes the information owner and must authorize the system in accordance with this handbook. The receiving enclave or site will maximize reuse of the existing authorization documentation to support the authorization by the receiving AO. Following the issuance of the authorization, subsequent deployment of the system by the Information System Owner to other receiving sites will follow the review and acceptance process.

(12) A VA system is authorized and subsequently deployed for acceptance into receiving sites authorized by a U.S. Government agency other than VA. In this case, the VA system's security authorization documentation is made available to the receiving U.S. Government agency. If the receiving agency determines there is insufficient information in the documentation or inadequate security measures in place for establishing an acceptable level of risk, the receiving agency may negotiate with the deploying VA organization for additional security measures or security-related information. The additional security measures or security- related information may be provided by the VA organization, the system developer, the receiving agency, some other external third party, or a combination of the above.

(13) A VA organization plans to use an IT service under contract from a commercial entity that has been authorized by a VA or other U.S. Government agency. In this case, the VA organization leverages an existing authorization and maximizes reuse of the existing authorization documentation to support a new authorization by a VA AO. If the VA organization determines there are inadequate security measures in place for establishing an acceptable level of risk, the VA organization may negotiate with IT service provider for additional security measures or security-related information. Upon assessment and approval of all newly included security measures and the documentation of all applicable security measures in the contract agreement with the IT service provider, the VA organization AO issues an authorization.

(f) Authorization Reporting. Report the authorization decision and any deficiencies in controls that represent significant security or privacy risk.

(g) System and Environment Changes. Monitor the information system and its environment of operation for changes that impact the security and privacy posture of the system. Changes to the technology or machine elements include upgrades to hardware, software, or firmware; changes to the human elements include for example, staff turnover or a reduction in force; and modifications to the surrounding physical and environmental elements include for example, changes in the location of the facility or the physical access controls protecting the facility.

(h) Ongoing Assessments. Assess the controls implemented within and inherited by the system in accordance with the continuous monitoring strategy. Included in the security controls assigned to all information system and platform IT systems are security controls related to configuration and deficiency management, performance monitoring, and periodic independent evaluations (i.e., penetration testing, and security control assessment).

(i) Ongoing Risk Response. Respond to risk based on the results of ongoing monitoring activities, risk assessments, and outstanding items in plans of action and milestones. An organizational assessment of risk and system-level risk assessment results guide and inform the decisions regarding ongoing risk response. Controls that are modified, enhanced, or added as part of ongoing risk response are reassessed by assessors to ensure that the new, modified, or enhanced controls have been implemented correctly, are operating as intended, and producing.

i. Assessment information produced by an assessor during continuous monitoring is provided to the System Owner and the common control provider in updated assessment reports or via reports from automated security/privacy management and reporting tools.

ii. The AO determines the appropriate risk response to the assessment findings or approves responses proposed by the System Owner and common control provider. The System Owner and common control provider subsequently implement the appropriate risk response.

a. When the risk response is acceptance, the findings remain documented in the security and privacy assessment reports and are monitored for changes to risk factors.

b. When the risk response is mitigation, the planned mitigation actions are included in and tracked using the plans of action and milestones.

iii. If requested by the AO, Control Assessors may provide recommendations for remediation actions.

iv. Recommendations for remediation actions may also be provided by an automated security/privacy management and reporting tool.

(j) Authorization Package Updates. Update plans, assessment reports, and POA&Ms based on the results of the continuous monitoring process.

(k) Security and Privacy Reporting. Report the security and privacy posture of the system to the AO and other organizational officials in accordance with the organizational continuous monitoring strategy.

(l) System Disposal. Implement a system disposal strategy and execute required actions when a system is removed from operation.

(m) Ongoing Authorization. Review the security and privacy posture of the system on an ongoing basis, as needed, at least annually or when a major change to the system occurs, to determine whether the risk remains acceptable.

(9) **CONTINUOUS MONITORING**

(a) In accordance with Appendix I (d) to OMB Circular A-130, systems and common controls should be reauthorized as needed, on a time- or event-driven basis in accordance with agency risk tolerance. The results of an annual review or a major change in the cybersecurity posture at any time may indicate the need for reassessment and reauthorization of the system.

(b) VA shall develop a security and privacy continuous monitoring strategy and implement a security and privacy continuous monitoring program that assesses security and privacy controls and associated risks at a frequency sufficient to support risk-based decisions.

(c) Remediation actions based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in the POA&M are conducted. Systems with a current ATO that are found to be operating in an unacceptable cybersecurity posture must have the newly identified vulnerabilities and associated level of risk added to an existing or newly created POA&M.

(d) POA&Ms are updated based on the results of the system-level continuous monitoring process.

(e) The security status of the system (including the effectiveness of security controls employed within and inherited by the system) must be reported on an ongoing basis in accordance with the monitoring strategy.

(f) Formal reauthorization is required whenever a system undergoes a significant change or when there is a major change in the information collected or maintained.

(g) Prior to implementing a change, determine if the proposed change is a change requiring reauthorization. Decisions regarding whether a system requires reauthorization will be based on an analysis of risk.

i. A significant change to an information system may include changes to the system itself or to the environment of operation.

a. Significant changes to the information system may include but are not limited to: installation of a new or upgraded operating system, middleware component, or application; modifications to system ports, protocols, or services; installation of a new or upgraded hardware platform;

modifications to cryptographic modules or services; or modifications to security controls.

b. Significant changes to the environment of operation may include but are not limited to: moving to a new facility; adding new core missions or business functions; modifications to the mission or business use of the system; acquiring specific and credible threat information that the organization is being targeted by a threat source; or establishing new or modified laws, policies or regulations.

ii. Major changes to the information collected or maintained are those changes that could result in greater disclosure of information or a change in the way personal data is used.

a. Systems that have been evaluated as having a sufficiently robust system-level continuous monitoring program (as defined by emerging VA continuous monitoring policy) may operate under a continuous reauthorization. Continuous monitoring does not replace the security authorization requirement; rather, it is an enabler of ongoing authorization decisions.

b. VA is responsible for the continuous monitoring and ongoing authorization of the system. VA may include as part of the agreement with the owning organization (e.g., contract) a requirement that the owning organization must share results from continuous monitoring activities conducted by the owning organization to maintain the authorization and the terms and conditions (e.g., frequency, format) required for the owning organization to report continuous monitoring results.

c. Security Authorization Documentation. The security authorization documentation consists of all artifacts developed through RMF activity. Security authorization documentation is maintained throughout a system's life cycle. The security authorization package consists of the security plan, SAR, POA&M, risk assessment report, and the authorization decision document, and is the minimum information necessary for the acceptance of an information system or platform IT system by a receiving organization, and the system-level continuous monitoring strategy as part of the security authorization package. Detailed information on the content of the security authorization package is available in the Information Security Knowledge Service.

d. Decommissioning Strategy

(1) VA will implement a system decommissioning strategy, when needed, which executes required actions when an information system or platform IT system is removed from service.

(2) When a system is removed from operation, a number of RMF-related actions are required. Before decommissioning, any control inheritance relationships should be reviewed and assessed for impact.

(3) Once the system has been decommissioned, the security plan should be updated to reflect the system’s decommissioned status and the system should be removed from all tracking systems. Other artifacts and supporting documentation should be disposed of according to its sensitivity or classification based on National Archives and Records Administration regulations.

(4) Data or objects in cybersecurity infrastructures that support the VA Information Enterprise, such as key management, identity management, vulnerability management, and privilege management, should be reviewed for impact.

APPENDIX A. Terms and Definitions

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

2. **Authorization to Operate (ATO):** The official management decision given by the AO to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. SOURCE: CNSSI 4009

3. **Authorization:** Access privileges granted to a user, program, or process or the act of granting those privileges. SOURCE: NIST SP 800-37

4. **Authorization Boundary:** All components of an information system to be authorized for operation by an AO but excludes separately authorized systems to which the information system is connected. SOURCE: NIST SP 800-37

5. **Authorizing Official (AO):** A 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 800-37

6. **Authorizing Official Designated Representative (AODR):** The AODR is an organizational official designated by the AO who is empowered to act on behalf of the AO to coordinate and conduct the day-to-day activities associated with managing risk to information systems and organizations. This includes carrying out many of the activities related to the execution of the RMF. The only activity that cannot be delegated by the AO to the designated representative is the authorization decision and signing of the associated authorization decision document (i.e., the acceptance of risk).

7. **Business Owner:** See Mission Owner.

8. **Common Controls**: A security control that is inherited by one or more organizational information systems. SOURCE: NIST SP 800-37

9. **Control Correlation Identifier (CCI):** Allows a high-level statement in a policy document to be ‘decomposed’ and explicitly associated with the low-level security settings that must be assessed to determine compliance with the objectives of that specific statement. SOURCE: NIST SP 800-53, CNSSI 4009

10. **Cross Domain Solution:** A form of controlled interface that provides the ability to manually and/or automatically access and/or transfer information between different security domains. SOURCE: NIST SP 800-37

11. **Cybersecurity:** Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. SOURCE: CNSSI 4009

12. **Cybersecurity Operations Center (CSOC):** Collects cyber threat intelligence, monitors adversarial behavior, responds to cyber security incidents, reports cyber threats and vulnerabilities, and provides cyber security consulting services that protects VA information systems. SOURCE: VA Information Security Knowledge Service

13. **Denial of Authorization to Operate**: Determination that the risk from the operation or use of the information system or the provision or use of common controls is unacceptable. SOURCE: NIST SP 800-37

14. **Enclave:** A set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter. SOURCE: CNSSI 4009

15. **Hardware:** The material physical components of an information system. SOURCE: CNSSI 4009

16. **Information Owner:** Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, classification, collection, processing, dissemination, and disposal. See information steward. SOURCE: CNSSI 4009

17. **Information Security Knowledge Service:** The Information Security Knowledge Service is a dynamic online knowledge base, supports RMF implementation, planning, and execution by functioning as the authoritative source for VA security control baselines, security control descriptions, security control overlays, and implementation guidance and assessment procedures. The Information Security Knowledge Service also supports the RMF TAG by enabling TAG functions and activities, including maintenance of membership; voting, analysis, and authoring; and configuration control of Information Security Knowledge Service enterprise content and functionality.

18. **Information Steward:** Individual or group that helps to ensure the careful and responsible management of Federal information belonging to the Nation as a whole, regardless of the entity or source that may have originated, created, or compiled the information. Information stewards provide maximum access to Federal information to elements of the Federal government and its customers, balanced by the obligation to protect the information in accordance with the provisions of FISMA and any associated security-related Federal policies, directives, regulations, standards, and guidance. SOURCE**:** NIST SP 800-37

19. **Information System:** A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. SOURCE: CNSSI 4009, 38 U.S.C. § 5727(13)

20. **Information System Security Officer (ISSO)**: Individual assigned responsibility by the CISO, management official, or Information System Owner for maintaining the appropriate operational security posture for an information system or program. SOURCE: CNSSI 4009; NIST SP 800-30

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

22. **Information Technology (IT) Product:** Individual IT hardware or software items. Products can be commercial, or government-provided and can include, but are not limited to, operating systems, office productivity software, firewalls, and routers. SOURCE: VA Directive 6500

23. **Information Technology (IT) Service:** A capability provided to one or more VA entities by an internal or external provider based on the use of IT and that supports a VA mission or business process. An IT Service consists of people, processes, and technology. SOURCE: VA Directive 6500

24. **Interim Authorization to Test:** Temporary authorization to test an information system in a specified operational information environment within the timeframe and under the conditions or constraints enumerated in the written authorization. SOURCE: CNSSI 4009

25. **Middleware:** Software that aggregates and filters data collected by RFID readers and possibly passes the information to an enterprise subsystem database. Middleware may also be responsible for monitoring and managing readers. SOURCE: NIST SP 800-98

26. **Mission Owner:** The mission owner, also referred to as business owner, is the senior official or executive within an organization with specific mission or line of business responsibilities and that has a security or privacy interest in the organizational systems supporting those missions or lines of business. SOURCE: NIST SP 800-37

27. **National Security System (NSS):** Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency – (i) the function, operations, or use of which (I) involves intelligence activities; (II) involves cryptologic activities related to national security; (III) involves command and control of military forces; (IV) involves equipment that is an integral part of a weapon or weapons systems; or (V) is critical to the direct fulfilment of a military or intelligence missions or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. Subparagraph (i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). SOURCE: 44 U.S.C. 3542 (b) (2).

28. **Network:** Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices. SOURCE: CNSSI 4009

29. Penetration Testing: A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system. SOURCE: CNSSI 4009; OMB Memorandum 02-01

30. 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

31. Plan of Action & Milestones (POA&M): A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. SOURCE: CNSSI 4009

32. Platform Information Technology: IT, both hardware and software, which is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems. SOURCE: VA Directive 6500

33. Platform Information Technology System: A collection of platform IT within an identified boundary under the control of a single authority and security policy. The systems may be structured by physical proximity or by function, independent of location. SOURCE: CNSSI 4009-2015 (DoDI 8500.01)

34. 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

35. Privacy Officer: The Privacy Officer 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 Privacy Officer to assist in mitigating damage when PII is compromised. SOURCE: VA Directive 6509

36. Privacy Threshold Analysis (PTA): A PTA is used to identify IT systems, rulemakings, programs, or pilot projects that involve SPI and other activities that otherwise impact the privacy of individuals as determined by the Director, Privacy Service, and to assess whether there is a need for a PIA, whether a System of Records Notice is required, and if any other privacy requirements apply to the IT system. A PTA includes a general description of the IT system, technology, rulemaking, program, pilot project, or other

Department activity and describes what SPI is collected (and from whom) and how that information is used. SOURCE: VA Handbook 6508.1

37. **Program Manager:** The individual with responsibility for and authority to accomplish program or system objectives for development, production, and sustainment to meet the user's operational needs. SOURCE: NIST SP 800-53

38. **Protected Health Information (PHI):** Individually identifiable health information held by a covered entity or by a business associate acting on its behalf. PHI excludes education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv), and employment records held by a covered entity in its role as employer. Within VA, VHA is the only covered entity. Certain other VA components, such as OIT, are business associates of VHA. SOURCE: 45 C.F.R. 160.103; VA Directive 6066.

39. **Reciprocity:** Mutual agreement among participating VA enterprises along with VA and other Federal agencies reviewing authorization packages to accept each other's security assessments in order to reuse information system resources and/or to accept each other's assessed security posture in order to share information. SOURCE: CNSSI 4009

40. **Risk:** A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs, and (ii) the likelihood of occurrence. Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. Adverse impacts to the Nation include, for example, compromises to information systems that support critical infrastructure applications or are paramount to government continuity of operations as defined by the Department of Homeland Security. SOURCE: CNSSI 4009

41. **Risk assessment:** The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. SOURCE: CNSSI 4009

42. **Risk Executive Function:** An individual or group within an organization that helps to ensure that (i) security risk-related considerations for individual information systems, to include the authorization decisions for those systems, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its mission and business functions; and (ii) managing risk from individual information systems is consistent across the organization, reflects organizational risk tolerance, and is considered along with other organizational risks affecting mission/business success. SOURCE: CNSSI 4009

43. **Risk Management:** The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i)

establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time. SOURCE: CNSSI 4009

44. **Risk Management Framework (RMF):** A structured approach used to oversee and manage risk for an enterprise. SOURCE: CNSSI 4009

45. **Risk Mitigation:** Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process. SOURCE: CNSSI 4009

46. **Risk Tolerance:** The level of risk an entity is willing to assume in order to achieve a potential desired result. SOURCE: CNSSI 4009-2015; NIST SP 800-32

47. **Security:** A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise’s risk management approach. SOURCE: CNSSI 4009

48. **Security Assessment Plan:** Provides the objectives for the security control assessment and a detailed roadmap of how to conduct such an assessment. SOURCE: NIST SP 800-53A

49. **Security Assessment Report:** Provides a disciplined and structured approach for documenting the findings of the assessor and the recommendations for correcting any identified vulnerabilities in the security controls. SOURCE: CNSSI 4009

50. **Security Control Assessor:** The individual, group, or organization responsible for conducting a security control assessment. SOURCE: CNSSI 4009

51. **Security Control Assessment:** The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. SOURCE: CNSSI 4009

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

53. **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: CNSSI 4009

54. **Security Domain:** A domain that implements a security policy and is administered by a single authority. SOURCE: CNSSI 4009

55. **Security Plan:** Formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. SOURCE: NIST SP 800-37

56. **Security Requirements Guide:** Compilation of control correlation identifiers (CCIs) grouped in more applicable, specific technology areas at various levels of technology and product specificity. Contains all requirements that have been flagged as applicable from the parent level regardless if they are selected on a VA baseline or not.

57. **Security Technical Implementation Guide (STIG):** Based on Department of Defense (DoD) policy and security controls. Implementation guide geared to a specific product and version. Contains all requirements that have been flagged as applicable for the product which have been selected on a VA baseline. SOURCE: VA Directive 6500

58. **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

59. **Service Level Agreement:** Defines the specific responsibilities of the service provider and sets the customer expectations. SOURCE: CNSSI 4009

60. **Software:** Computer programs (which are stored in and executed by computer hardware) and associated data (which also is stored in the hardware) that may be dynamically written or modified during execution. SOURCE: CNSSI 4009

This page is intentionally blank

APPENDIX B. Acronyms and Abbreviations

Acronym/ Abbreviation	Definition
A&A	Assessment & Authorization
ADAS	Associate Deputy Assistant Secretary
AO	Authorizing Official
AODR	Authorizing Official Designated Representative
AOR	Area of Responsibility
ATO	Authorization to Operate
CCI	Control Correlation Identifier
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CPO	Chief Privacy Officer
CSOC	Cybersecurity Operations Center
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CONOPS	Continuity of Operations Plans
DAS	Deputy Assistant Secretary
DevOps	Development and Operations
DISA	Defense Information Systems Agency
eMASS	Enterprise Mission Assurance Support Services
EPMO	Enterprise Program Management Office
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health
ISSM	Information System Security Manager
ISSO	Information System Security Officer
ISSP	Information System Security Plan
IT	Information Technology
ITOPS	Information Technology Operations and Services
NIST	National Institute of Standards and Technology
NSS	National Security System
OALC	Office of Acquisitions, Logistics, and Construction
OIS	Office of Information Security
OIT	Office of Information Technology
OMB	Office of Management and Budget
PHI	Protected Health Information
PIA	Privacy Impact Assessment

Acronym/ Abbreviation	Definition
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
PTA	Privacy Threshold Analysis
RMF	Risk Management Framework
RoB	Rules of Behavior
SAOP	Senior Agency Official for Privacy
SAR	Security Assessment Report
SDLC	System Development Life Cycle
SP	Special Publication
SPI	Sensitive Personal Information
STIG	Security Technical Implementation Guide
TAG	Technical Advisory Group
U.S.C.	United States Code

This page is intentionally blank

APPENDIX C. References

1. Statutes and Regulations

a. 38 U.S.C. §§ 5721-28, Information Security

b. Health Information Technology for Economic and Clinical Health (HITECH) Act, Pub. L. 111-5, 123 Stat. 226, 260 (2009), codified at 42 U.S.C. § 17932

c. Health Insurance Portability and Accountability Act (HIPAA), Pub. L. 104-191, 110 Stat. 1936 (1996)

d. 45 C.F.R. Parts 160 and 164, HIPAA Privacy, Security, and Breach Notification Rules

2. Federal Information Processing Standards (FIPS) Publications

a. FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems

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

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

a. NIST SP 800-30, Guide for Conducting Risk Assessments, September 2012

b. NIST SP 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy

c. NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View

d. NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations

e. NIST SP 800-53 A, Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans

f. NIST SP 800-63, Digital Identity Guidelines

g. NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

h. NIST ANNEX Security and Privacy Controls URL:

NIST ANNEX Security and Privacy Controls

4. Office of Management and Budget (OMB) Publications

a. OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources

b. OMB Circular M-19-17, Identity, Credential, and Access Management (ICAM)

5. Committee on National Security System Instruction (CNSSI)

a. Committee on National Security System Instruction 4009, National Information Assurance Glossary

b. Committee on National Security System Instruction 1253, Security Categorization and Control Selection for national Security Systems.

6. VA Directives and Handbooks

c. VA Handbook 0710, Personnel Security and Suitability Program

d. VA Directive 6500, VA Cybersecurity Program

e. VA Handbook 6500.6, Contract Security

f. VA Handbook 6508.1, Procedures for Privacy Threshold Analysis and Privacy Impact Assessment

g. VA Handbook 6517, Risk Management Framework for Cloud Computing Services

7. Other References

a. VA Information Security Knowledge Service Portal - VA Information Security Knowledge Service Portal

b. The Clinger-Cohen Act

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

APPENDIX D. High-Level Summary of RMF Tasks

Table 1: Prepare Tasks—Organization Level

Task	SDLC Phase	Primary Responsibility	Supporting Role	References
Task P-1 Risk Management Roles		Head of Agency Chief Information Officer (CIO) Senior Agency Official for Privacy (SAOP)	Authorizing Official (AO) Authorizing Official Designated Representative (AODR) Senior Accountable Official for Risk Management Risk Executive (Function) Chief Information Security Officer (CISO)	SP 800-160 v1 (Human Resource Management Process) SP 800-181 NIST CSF (Core Identify Function)
Task P-2 Risk Management Strategy		Head of Agency	Senior Accountable Official for Risk Management Risk Executive (Function) Chief Information Officer (CIO) Chief Information Security Officer (CISO) Senior Agency Official for Privacy (SAOP)	SP 800-30 SP 800-39 (Organization Level) SP 800-160 v1 (Risk Management, Decision Management, Quality Assurance, Quality Management, Project Assessment and Control Processes) SP 800-161 IR 8062 IR 8179 (Criticality Analysis Process B); NIST CSF (Core Identify Function)
Task P-3 Risk Assessment—Organization		Senior Accountable Official for Risk Management	Chief Information Officer (CIO)	SP 800-30 SP 800-39 (Organization Level,

Task	SDLC Phase	Primary Responsibility	Supporting Role	References
		Risk Executive (Function) Chief Information Security Officer (CISO) Senior Agency Official for Privacy (SAOP)	Authorizing Official (AO) Authorizing Official Designated Representative (AODR) Mission or Business Owner	Mission/Business Process Level) SP 800-161 IR 8062
Task P-4 Organizationally-Tailored Control Baselines and Cybersecurity Framework Profiles (Optional)		Mission or Business Owner Senior Accountable Official for Risk Management Risk Executive (Function)	Chief Information Officer (CIO) Authorizing Official (AO) Authorizing Official Designated Representative (AODR) Chief Information Security Officer (CISO) Senior Agency Official for Privacy (SAOP)	SP 800-53 SP 800-53B SP 800-160 v1 (Business or Mission Analysis and Stakeholder Needs and Requirements Definition Processes) NIST CSF (Core, Profiles)
Task P-5 Common Control Identification		Chief Information Security Officer (CISO) Senior Agency Official for Privacy (SAOP)	Mission or Business Owner Senior Accountable Official for Risk Management Risk Executive (Function) Chief Information Officer (CIO) Authorizing Official (AO) Authorizing Official Designated Representative (AODR) Common Control Provider System Owner (SO)	SP 800-53

Task	SDLC Phase	Primary Responsibility	Supporting Role	References
Task P-6 Impact-Level Prioritization (Optional)		Senior Accountable Official for Risk Management Risk Executive (Function)	Chief Information Security Officer (CISO) Senior Agency Official for Privacy (SAOP) Mission or Business Owner System Owner (SO) Chief Information Officer (CIO) Authorizing Official (AO) Authorizing Official Designated Representative (AODR)	FIPS 199 FIPS 200 SP 800-30 SP 800-39 (Organization and System Levels) SP 800-59 SP 800-60 v1 SP 800-60 v2 SP 800-160 v1 (System Requirements Definition Process) IR 8179] (Criticality Analysis Process B) CNSSI 1253 NIST CSF (Core [Identify Function] Profiles).
Task P-7 Continuous Monitoring Strategy—Organization		Senior Accountable Official for Risk Management Risk Executive (Function)	Chief Information Officer (CIO) Chief Information Security Officer (CISO) Senior Agency Official for Privacy (SAOP) Mission or Business Owner System Owner (SO) Authorizing Official (AO)	SP 800-30 SP 800-39 (Organization, Mission or Business Process, System Levels) SP 800-53 SP 800-53A SP 800-137 SP 800-161 IR 8011 v1

Task	SDLC Phase	Primary Responsibility	Supporting Role	References
			Authorizing Official Designated Representative (AODR)	IR 8062 NIST CSF (Core Identify, Detect Functions) CNSSI 1253

Table 2: Prepare Tasks—System Level

Task	SDLC Phase	Primary Responsibility	Supporting Role	References
Task P-8 Mission or Business Focus	New – Initiation (concept/requirements definition) Existing – Operations/Maintenance	Mission or Business Owner	Authorizing Official (AO) Authorizing Official Designated Representative (AODR) System Owner (SO) Information Owner or Steward Chief Information Officer (CIO) Chief Information Security Officer (CISO) Senior Agency Official for Privacy (SAOP)	SP 800-39 (Organization and Mission/Business Process Levels) SP 800-64 SP 800-160 v1 (Business or Mission Analysis, Portfolio Management, and Project Planning Processes) NIST CSF (Core Identify Function) IR 8179 (Criticality Analysis Process B)
Task P-9 System Stakeholders	New – Initiation (concept/requirements definition) Existing – Operations/Maintenance	Mission or Business Owner System Owner (SO)	Chief Information Officer (CIO) Authorizing Official (AO) Authorizing Official Designated Representative (AODR) Information Owner or Steward	SP 800-39 (Organization Level) SP 800-64 SP 800-160 v1 (Stakeholder Needs and Requirements Definition and Portfolio Management Processes)

Task	SDLC Phase	Primary Responsibility	Supporting Role	References
			Chief Information Security Officer (CISO) Senior Agency Official for Privacy (SAOP) Chief Acquisition Officer	SP 800-161 NIST CSF (Core Identify Function)
Task P-10 Asset Identification	New – Initiation (concept/requirements definition) Existing – Operations/Maintenance	System Owner (SO)	Authorizing Official (AO) Authorizing Official Designated Representative (AODR) Mission or Business Owner Information Owner or Steward Chief Information Security Officer (CISO) Senior Agency Official for Privacy (SAOP) System Administrator	SP 800-39 (Organization Level) SP 800-64 SP 800-160 v1 (Stakeholder Needs and Requirements Definition Process) IR 8179 (Criticality Analysis Process C) NIST CSF (Core Identify Function)
Task P-11 Authorization Boundary	New – Initiation (concept/requirements definition) Existing – Operations/Maintenance	Authorizing Official (AO)	Chief Information Officer (CIO) Mission or Business Owner System Owner (SO) Chief Information Security Officer (CISO) Senior Agency Official for Privacy (SAOP)	SP 800-18 SP 800-39 (System Level) SP 800-47 SP 800-64 SP 800-160 v1 (System Requirements Definition Process)

Task	SDLC Phase	Primary Responsibility	Supporting Role	References
			Enterprise Architect	NIST CSF (Core Identify Function)
Task P-12 Information Types	New – Initiation (concept/requirements definition) Existing – Operations/Maintenance	Senior Agency Official for Privacy (SAOP) System Owner (SO) Information Owner or Steward	Information System Security Officer (ISSO) System Privacy Officer (PO) Mission or Business Owner	OMB A-130 SP 800-39 (System Level) SP 800-60 v1 SP 800-60 v2 NIST CSF (Core Identify Function)
Task P-13 Information Life Cycle	New – Initiation (concept/requirements definition) Existing – Operations/Maintenance	Senior Agency Official for Privacy (SAOP) System Owner (SO) Information Owner or Steward	Chief Information Officer (CIO) Mission or Business Owner Security Architect Privacy Architect Enterprise Architect Systems Security Privacy Engineer	OMB A-130 OMB M-13-13 NIST CSF (Core Identify Function) IR 8062
Task P-14 Risk Assessment—System	New – Initiation (concept/requirements definition) Existing – Operations/Maintenance	System Owner (SO) Information System Security Officer (ISSO) System Privacy Officer (PO)	Senior Accountable Official for Risk Management Risk Executive (Function) Authorizing Official (AO) Authorizing Official Designated Representative (AODR) Mission or Business Owner	FIPS 199 FIPS 200 SP 800-30 SP 800-39 (Organization Level) SP 800-59 SP 800-60 v1 SP 800-60 v2 SP 800-64 SP 800-160 v1 (Stakeholder Needs

Task	SDLC Phase	Primary Responsibility	Supporting Role	References
			Information Owner or Steward Information System Security Officer (ISSO)	and Requirements Definition and Risk Management Processes) SP 800-161 (Assess) IR 8062 IR 8179 NIST CSF (Core Identify Function) CNSSI 1253
Task P-15 Requirements Definition	New – Initiation (concept/requirements definition) Existing – Operations/Maintenance	Mission or Business Owner System Owner (SO) Information Owner or Steward System Privacy Officer (PO)	Authorizing Official (AO) Authorizing Official Designated Representative (AODR) Chief Information Security Officer (CISO) Senior Agency Official for Privacy (SAOP) Information System Security Officer (ISSO) Chief Acquisition Officer Security Architect Privacy Architect Enterprise Architect	SP 800-39 (Organization Level) SP 800-64 SP 800-160 v1 (Stakeholder Needs and Requirements Definition Process) SP 800-161 (Multi-Tiered Risk Management) IR 8179 NIST CSF (Core Protect, Detect, Respond, Recover Functions; Profiles)
Task P-16 Enterprise Architecture	New – Initiation (concept/requirements definition)	Mission or Business Owner Enterprise Architect	Chief Information Officer (CIO) Authorizing Official (AO)	SP 800-39 (Mission/Business Process Level) SP 800-64

Task	SDLC Phase	Primary Responsibility	Supporting Role	References
	Existing – Operations/Maintenance	Security Architect Privacy Architect	Authorizing Official Designated Representative (AODR) Chief Information Security Officer (CISO) Senior Agency Official for Privacy (SAOP) System Owner (SO) Information Owner or Steward	SP 800-160 v1 (System Requirements Definition Process) NIST CSF (Core Identify Function; Profiles) OMB FEA
Task P-17 Requirements Allocation	New – Initiation (concept/requirements definition) Existing – Operations/Maintenance	Security Architect Privacy Architect Information System Security Officer (ISSO) System Privacy Officer (PO)	Chief Information Officer (CIO) Authorizing Official or Authorizing Official Designated Representative Mission or Business Owner Chief Information Security Officer (CISO) Senior Agency Official for Privacy (SAOP) System Owner (SO)	SP 800-39 (Organization, Mission/Business Process, and System Levels) SP 800-64 SP 800-160 v1 (System Requirements Definition Process) NIST CSF (Core [Identify Function]; Profiles) OMB FEA
Task P-18 System Registration	New – Initiation (concept/requirements definition) Existing – Operations/Maintenance	System Owner (SO)	Mission or Business Owner Chief Information Officer (CIO) Information System Security Officer (ISSO)	None

Task	SDLC Phase	Primary Responsibility	Supporting Role	References
			System Privacy Officer (PO)	

Table 3: Categorize Tasks

Task	SDLC Phase	Primary Responsibility	Supporting Role	References
Task C-1 System Description	New – Initiation (concept/requirements definition) Existing – Operations/Maintenance	System Owner (SO)	Authorizing Official (AO) or Authorizing Official Designated Representative (AODR) Information Owner or Steward Information System Security Officer (ISSO) System Privacy Officer (PO)	SP 800-18 NIST CSF (Core Identify Function)
Task C-2 Security Categorization	New – Initiation (concept/requirements definition) Existing – Operations/Maintenance	System Owner (SO); Information Owner or Steward	Senior Accountable Official for Risk Management or Risk Executive (Function) Chief Information Officer (CIO) Chief Information Security Officer (CISO) Senior Agency Official for Privacy (SAOP) Authorizing Official (AO) or Authorizing Official Designated Representative (AODR) Information System Security Officer (ISSO) System Privacy Officer (PO)	FIPS 199 FIPS 200 SP 800-30 SP 800-39 (System Level) SP 800-59 SP 800-60 v1 SP 800-60 v2 SP 800-160 v1 (Stakeholder Needs and Requirements Definition and System Requirements Definition Processes) IR 8179 CNSSI 1253 NIST CSF (Core Identify Function)

Task	SDLC Phase	Primary Responsibility	Supporting Role	References
Task C-3 Security Categorization Review and Approval	New – Initiation (concept/requirements definition) Existing – Operations/Maintenance	Authorizing Official (AO) or Authorizing Official Designated Representative (AODR) Senior Agency Official for Privacy (SAOP)	Senior Accountable Official for Risk Management or Risk Executive (Function) Chief Information Officer (CIO) Chief Information Security Officer (CISO)	FIPS 199 SP 800-30 SP 800-39 (Organization Level) SP 800-160 v1 (Stakeholder Needs and Requirements Definition Process) CNSSI 1253 NIST CSF (Core Identify Function)

Table 4: Select Tasks and Outcomes

Task	SDLC Phase	Primary Responsibility	Supporting Role	References
Task S-1 Control Selection	New – Development/Acquisition Existing – Operations/Maintenance	System Owner (SO); Common Control Provider	Authorizing Official (AO) or Authorizing Official Designated Representative (AODR) Information Owner or Steward Systems Security Engineer Privacy Engineer Information System Security Officer (ISSO) System Privacy Officer (PO)	FIPS 19 FIPS 200 SP 800-30 SP 800-53 SP 800-53B SP 800-160 v1 (System Requirements Definition, Architecture Definition, and Design Definition Processes) SP 800-161 (Respond and Chapter 3 IR 806 IR 8179 CNSSI 1253; NIST CSF (Core Identify, Protect, Detect, Respond, Recover Functions; Profiles)
Task S-2 Control Tailoring	New – Development/Acquisition Existing – Operations/Maintenance	System Owner (SO); Common Control Provider	Authorizing Official (AO) or Authorizing Official Designated Representative (AODR) Information Owner or Steward Systems Security Engineer Privacy Engineer	FIPS 199 FIPS 200 SP 800-30 SP 800-53 SP 800-53B SP 800-160 v1 (System Requirements Definition, Architecture Definition, and

Task	SDLC Phase	Primary Responsibility	Supporting Role	References
			Information System Security Officer (ISSO) System Privacy Officer (PO)	Design Definition Processes) SP 800-161 (Respond and Chapter 3) IR 8179 CNSSI 1253 NIST CSF (Core Identify, Protect, Detect, Respond, Recover Functions; Profiles)
Task S-3 Control Allocation	New – Initiation (concept/requirements definition) Existing – Operations/Maintenance	Security Architect Privacy Architect Information System Security Officer (ISSO) System Privacy Officer (PO)	Chief Information Officer (CIO) (CIO) Authorizing Official (AO) or Authorizing Official Designated Representative (AODR) Mission or Business Owner Chief Information Security Officer (CISO) Senior Agency Official for Privacy (SAOP) System Owner (SO)	SP 800-39 (Organization, Mission/Business Process, and System Levels) SP 800-64 SP 800-160 v1 (System Requirements Definition, Architecture Definition, and Design Definition Processes) NIST CSF (Core [Identify Function]; Profiles) OMB FEA
Task S-4 Documentation of Planned Control Implementations	New – Development/Acquisition Existing – Operations/Maintenance	System Owner (SO); Common Control Provider	Authorizing Official (AO) or Authorizing Official Designated Representative (AODR) Information Owner or Steward Systems Security Engineer	FIPS 199 FIPS 200 SP 800-18 SP 800-30 SP 800-53 SP 800-64

Task	SDLC Phase	Primary Responsibility	Supporting Role	References
			Privacy Engineer Information System Security Officer (ISSO) System Privacy Officer (PO)	SP 800-160 v1 (System Requirements Definition, Architecture Definition, and Design Definition Processes) SP 800-161 (Respond and Chapter 3) IR 8179 CNSSI 1253 NIST CSF (Core Identify, Protect, Detect, Respond, Recover Functions; Profiles)
Task S-5 Continuous Monitoring Strategy—System	New – Development/Acquisition Existing – Operations/Maintenance	System Owner (SO); Common Control Provider	Senior Accountable Official for Risk Management or Risk Executive (Function) Chief Information Officer (CIO) Chief Information Security Officer (CISO) Senior Agency Official for Privacy (SAOP) Authorizing Official (AO) or Authorizing Official Designated Representative (AODR) Information Owner or Steward Security Architect Privacy Architect	SP 800-30 SP 800-39 (Organization, Mission or Business Process, System Levels) SP 800-53 SP 800-53A SP 800-137 SP 800-161 IR 8011 v1 CNSSI 1253 NIST CSF (Core Detect Function)

Task	SDLC Phase	Primary Responsibility	Supporting Role	References
			Systems Security Engineer Privacy Engineer Information System Security Officer (ISSO) System Privacy Officer (PO)	
Task S-6 Plan Review and Approval	New – Development/Acquisition Existing – Operations/Maintenance	Authorizing Official (AO) or Authorizing Official Designated Representative (AODR)	Senior Accountable Official for Risk Management or Risk Executive (Function) Chief Information Officer (CIO) Chief Acquisition Officer Chief Information Security Officer (CISO) Senior Agency Official for Privacy (SAOP)	SP 800-30 SP 800-53 SP 800-160 v1 (System Requirements Definition, Architecture Definition, and Design Definition Processes)

Table 5: Implement Tasks and Outcomes

Task	SDLC Phase	Primary Responsibility	Supporting Role	References
Task I-1 Control Implementation	New – Development/Acquisition Implementation/Assessment Existing – Operations/Maintenance	System Owner (SO) Common Control Provider	Information Owner or Steward Security Architect Privacy Architect Systems Security Engineer Privacy Engineer Information System Security Officer (ISSO) System Privacy Officer (PO) Enterprise Architect System Administrator	FIPS 200 SP 800-30 SP 800-53 SP 800-53A SP 800-160 v1 (Implementation, Integration, Verification, and Transition Processes) SP 800-161 IR 8062 IR 8179
Task I-2 Update Control Implementation Information	New – Development/Acquisition; Implementation/Assessment Existing – Operations/Maintenance	System Owner (SO) Common Control Provider	Information Owner or Steward Security Architect Privacy Architect Systems Security Engineer Privacy Engineer Information System Security Officer (ISSO) System Privacy Officer (PO) Enterprise Architect System Administrator	SP 800-53 SP 800-128 SP 800-160 v1 (Implementation, Integration, Verification, and Transition, Configuration Management Processes)

Table 6: Assess Tasks and Outcomes

Task	SDLC Phase	Primary Responsibility	Supporting Role	References
Task A-1 Assessor Selection	New – Development/Acquisition; Implementation/Assessment Existing – Operations/Maintenance	Authorizing Official (AO) or Authorizing Official Designated Representative (AODR)	Chief Information Officer (CIO) Chief Information Security Officer (CISO) Senior Agency Official for Privacy (SAOP)	FIPS 199 SP 800-30 SP 800-53A SP 800-55
Task A-2 Assessment Plan	New – Development/Acquisition; Implementation/Assessment Existing – Operations/Maintenance	Authorizing Official (AO) or Authorizing Official Designated Representative (AODR) Control Assessor	Chief Information Security Officer (CISO) Senior Agency Official for Privacy (SAOP) System Owner (SO) Common Control Provider Information Owner or Steward Information System Security Officer (ISSO) System Privacy Officer (PO)	SP 800-53A SP 800-160 v1 (Verification and Validation Processes) SP 800-161 IR 8011 v1
Task A-3 Control Assessments	New – Development/Acquisition; Implementation/Assessment Existing – Operations/Maintenance	Control Assessor	Authorizing Official (AO) or Authorizing Official Designated Representative (AODR) System Owner (SO) Common Control Provider Information Owner or Steward	SP 800-53A SP 800-160 v1 (Verification and Validation Processes) IR 8011 v1

Task	SDLC Phase	Primary Responsibility	Supporting Role	References
			Chief Information Security Officer (CISO) Senior Agency Official for Privacy (SAOP) Information System Security Officer (ISSO) System Privacy Officer (PO)	
Task A-4 Assessment Reports	New – Development/Acquisition Implementation/Assessment Existing – Operations/Maintenance	Control Assessor	System Owner (SO) Common Control Provider Information System Security Officer (ISSO) System Privacy Officer (PO)	SP 800-53A SP 800-160 v1 (Verification and Validation Processes)
Task A-5 Remediation Actions	New – Development/Acquisition Implementation/Assessment Existing – Operations/Maintenance	System Owner (SO) Common Control Provider Control Assessor	Authorizing Official (AO) or Authorizing Official Designated Representative (AODR) Chief Information Security Officer (CISO) Senior Agency Official for Privacy (SAOP) Senior Accountable Official for Risk Management or Risk Executive (Function) Information Owner or Steward	SP 800-53A SP 800-160 v1 (Verification and Validation Processes)

Task	SDLC Phase	Primary Responsibility	Supporting Role	References

			Systems Security Engineer
			Privacy Engineer;
			Information System Security Officer (ISSO);
			System Privacy Officer (PO)	

Task A-6 Plan of Action and Milestones	New – Implementation/Assessment Existing – Operations/Maintenance	System Owner (SO); Common Control Provider	Information Owner or Steward Information System Security Officer (ISSO) System Privacy Officer (PO) Chief Information Security Officer (CISO) Senior Agency Official for Privacy (SAOP) Control Assessor Chief Acquisition Officer	SP 800-30 SP 800-53A SP 800-160 v1 (Verification and Validation Processes) IR 8062

Table 7: Authorize Tasks and Outcomes

Task	SDLC Phase	Primary Responsibility	Supporting Role	References
Task R-1 Authorization Package	New – Implementation/Assessment Existing – Operations/Maintenance	System Owner (SO) (SO) Common Control Provider Senior Agency Official for Privacy (SAOP)	Information System Security Officer (ISSO) Privacy Officer (PO) Chief Information Security Officer (CISO) Control Assessor	OMB A-130 SP 800-18 SP 800-160 v1 (Risk Management Process) SP 800-161 (SCRM Plans)
Task R-2 Risk Analysis and Determination	New – Implementation/Assessment Existing – Operations/Maintenance	Authorizing Official (AO) or Authorizing Official Designated Representative (AODR)	Senior Accountable Official for Risk Management or Risk Executive (Function) Chief Information Security Officer (CISO) Senior Agency Official for Privacy (SAOP)	OMB A-130 SP 800-30 SP 800-39 (Organization, Mission/Business Process, and System Levels) SP 800-137 SP 800-160 v1 (Risk Management Process) IR 8062
Task R-3 Risk Response	New – Implementation/Assessment Existing – Operations/Maintenance	Authorizing Official (AO) or Authorizing Official Designated Representative (AODR)	Senior Accountable Official for Risk Management or Risk Executive (Function) Chief Information Security Officer (CISO) Senior Agency Official for Privacy (SAOP) System Owner (SO) or Common Control Provider Information Owner or Steward;	SP 800-30; SP 800-39 (Organization, Mission/Business Process, and System Levels) SP 800-160 v1 (Risk Management Process) IR 8062 IR 8179 NIST CSF (Core Identify Function)

Task	SDLC Phase	Primary Responsibility	Supporting Role	References
			Systems Security Engineer Privacy Engineer Information System Security Officer (ISSO) Privacy Officer (PO)	
Task R-4 Authorization Decision	New – Implementation/Assessment Existing – Operations/Maintenance	Authorizing Official (AO)	Senior Accountable Official for Risk Management or Risk Executive (Function) Chief Information Officer (CIO) Chief Information Security Officer (CISO) Senior Agency Official for Privacy (SAOP) Authorizing Official Designated Representative (AODR)	SP 800-39 (Organization, Mission/Business Process, and System Levels) SP 800-160 v1 (Risk Management Process)
Task R-5 Authorization Reporting	New – Implementation/Assessment Existing – Operations/Maintenance	Authorizing Official (AO) or Authorizing Official Designated Representative (AODR)	System Owner (SO) or Common Control Provider Information Owner or Steward Information System Security Officer (ISSO); Privacy Officer (PO) Chief Information Security Officer (CISO)	SP 800-39 (Organization, Mission/Business Process, and System Levels) SP 800-160 v1 (Decision Management and Project Assessment and Control Processes NIST CSF (Core Identify, Protect, Detect, Respond, Recover Functions)

Task	**SDLC Phase**	**Primary Responsibility**	**Supporting Role**	**References**
			Senior Agency Official for Privacy (SAOP)	

Table 8: Monitor Tasks and Outcomes

Task	SDLC Phase	Primary Responsibility	Supporting Role	References
Task M-1 System and Environment Changes	New – Operations/Maintenance Existing – Operations/Maintenance	System Owner (SO) or Common Control Provider Chief Information Security Officer (CISO) Chief Information Security Officer (CISO)	Senior Accountable Official for Risk Management or Risk Executive (Function) Authorizing Official (AO) or Authorizing Official Designated Representative (AODR) Information Owner or Steward Information System Security Officer (ISSO) System Privacy Officer (PO)	SP 800-30 SP 800-128 SP 800-137 IR 8062
Task M-2 Ongoing Assessments	New – Operations/Maintenance Existing – Operations/Maintenance	Control Assessor	Authorizing Official (AO) or Authorizing Official Designated Representative (AODR) System Owner (SO) or Common Control Provider Information Owner or Steward Information System Security Officer (ISSO) System Privacy Officer (PO) Chief Information Security Officer (CISO) Senior Agency Official for Privacy (SAOP)	SP 800-53A SP 800-137 SP 800-160 v1 (Verification, Validation, Operation, and Maintenance Processes) IR 8011 v1

Task	SDLC Phase	Primary Responsibility	Supporting Role	References
Task M-3 Ongoing Risk Response	New – Operations/Maintenance Existing – Operations/Maintenance	Authorizing Official (AO) System Owner (SO) Common Control Provider	Senior Accountable Official for Risk Management or Risk Executive (Function) Senior Agency Official for Privacy (SAOP) Authorizing Official Designated Representative (AODR) Information Owner or Steward Information System Security Officer (ISSO) System Privacy Officer (PO) Systems Security Engineer Privacy Engineer Security Architect Privacy Architect	SP 800-30 SP 800-53 SP 800-53A SP 800-137 SP 800-160 v1 (Risk Management Process) IR 8011 v1 IR 8062 NIST CSF (Core Respond Function)
Task M-4 Authorization Package Updates	New – Operations/Maintenance Existing – Operations/Maintenance	System Owner (SO); Common Control Provider	Information Owner or Steward Information System Security Officer (ISSO) System Privacy Officer (PO) Senior Agency Official for Privacy (SAOP) Chief Information Security Officer (CISO)	SP 800-30 SP 800-53A

Task	SDLC Phase	Primary Responsibility	Supporting Role	References
Task M-5 Security and Privacy Reporting	New – Operations/Maintenance Existing – Operations/Maintenance	System Owner (SO) Common Control Provider Chief Information Security Officer (CISO) Senior Agency Official for Privacy (SAOP)	Information System Security Officer (ISSO) System Privacy Officer (PO)	SP 800-53A SP 800-137 NIST CSF (Core Identify, Protect, Detect, Respond, Recover Functions)
Task M-6 Ongoing Authorization	New – Operations/Maintenance Existing – Operations/Maintenance	Authorizing Official (AO)	Senior Accountable Official for Risk Management or Risk Executive (Function) Chief Information Officer (CIO) Chief Information Security Officer (CISO) Senior Agency Official for Privacy (SAOP) Authorizing Official Designated Representative (AODR)	SP 800-30 SP 800-39 (Organization, Mission/Business Process, and System Levels) SP 800-55 SP 800-160 v1 (Risk Management Process) IR 8011 v1 IR 8062

Task M-7
System Disposal
	New – Not Applicable
	Existing – Disposal
		System Owner (SO)	Authorizing Official (AO) or Authorizing Official Designated Representative (AODR)
			Information Owner or Steward
			Information System Security Officer (ISSO)
			System Privacy Officer (PO)
				SP 800-30;
				SP 800-88;
				IR 8062

Task	SDLC Phase	Primary Responsibility	Supporting Role	References
			Senior Accountable Official for Risk Management or Risk Executive (Function) Chief Information Security Officer (CISO) Senior Agency Official for Privacy (SAOP)	