CERTIFICATION AND ACCREDITATION OF VA INFORMATION SYSTEMS

1. REASON FOR ISSUE: To provide the Department of Veterans Affairs (VA) with procedures to ensure compliance with Certification and Accreditation (C&A) requirements for VA information systems as required by the Federal Information Security Management Act of 2002 (FISMA); Office of Management and Budget (OMB) Circular A-130, Appendix III, *Security of Federal Automated Information Resources*; and VA Directive and Handbook 6500, *Information Security Program*.

2. SUMMARY OF CONTENTS/MAJOR CHANGES: The enterprise level C&A policy is located in VA Directive and Handbook 6500. This handbook provides further details for the implementation of C&A in accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*.

3. RESPONSIBLE OFFICE: The Office of the Assistant Secretary for Information and Technology (OI&T) (005).

4. RELATED DIRECTIVE: VA Directive and Handbook 6500, *Information Security Program*.

5. RESCISSIONS: NONE.

CERTIFIED BY:

/S/
Robert T. Howard
Assistant Secretary for Information and Technology

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/S/
Robert T. Howard
Assistant Secretary for Information and Technology

Distribution: Electronic Only

CERTIFICATION AND ACCREDITATION OF VA INFORMATION SYSTEMS

CONTENTS

CERTIFICATION AND ACCREDITATION OF VA INFORMATION SYSTEMS

APPENDICES **PAGE**

TABLES

CERTIFICATION AND ACCREDITATION OF VA INFORMATION SYSTEMS

1. PURPOSE

a. The Department of Veterans Affairs (VA) Directive and Handbook 6500, *Information Security Program*, provides the highest level of policy to ensure VA information systems adhere to and are in compliance with established Federal laws and regulations.

b. This handbook provides the next level of policy, while specific procedures necessary to accomplish Certification and Accreditation (C&A) activities are contained within Appendices C-G of this document.

c. These policies and procedures are in accordance with Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB) Circular A-130, Appendix III, and applicable National Institute of Standards and Technology (NIST) publications.

d. This handbook is designed to include a complete overview of the C&A process to educate and provide specific, consistent policy on standardized C&A activities throughout the VA. The intent of this Handbook is to inform readers on C&A processes, specifically:

(1) The requirements of the C&A process;

(2) How the C&A process works;

(3) Which individuals are responsible for specific tasks; and

(4) How other Information Technology (IT) security activities relate to and/or interact with the C&A process.

2. SCOPE/OVERVIEW

a. The policies stated in this document apply to all individuals (VA employees, contractors, researchers, students, volunteers, representatives of Federal, State, local, or Tribal agencies, and any others not specifically mentioned in this list) involved in, or in support of, the C&A process for VA systems.

b. The requirements for C&A apply to all VA-owned or operated information systems and applications, as well as all non VA-owned systems and applications containing VA information regardless of the physical location of the system but are still included in the information system accreditation boundary.

3. CERTIFICATION AND ACCREDITATION BACKGROUND

a. Certification and Accreditation

(1) C&A is the process used to ensure information systems including Major Applications (MA) and General Support Systems (GSS) have effective security safeguards which have been implemented, planned for, and documented in a system security plan as commensurate with potential risks to the

system's information. When possible, minor applications should be included with the major application or GSS for C&A purposes as many of the security controls are shared with the major application/GSS. Minor applications will be required to complete a security plan to ensure compliance with the major application/GSS security controls. Minor applications that can not be included with a major application or GSS are required to complete the entire C&A process. The successful completion of the C&A process provides formal management authority for a system to operate and process information. C&A is based on the approval of the Authorizing Official (AO) who is the senior most agency official assigned responsibility for IT systems. C&A is required by information security legislation and Federal regulation and provides a framework for auditing the efficiency and effectiveness of security controls.

(2) C&A should not be viewed as an administrative burden. It provides realistic, measurable, and cost-effective benefits for operating a system and protecting its information. The goal is to minimize system risk to an acceptable level for processing information. Risks will always exist; however, identifying weaknesses and prioritizing corrective actions to mitigate vulnerabilities is the foundation of the C&A process.

(3) All information systems (GSSs or MAs) containing VA information must be authorized to operate. This authorization is achieved through VA's C&A process. At the completion of this process, the GSS or MA will receive either an Authorization to Operate (ATO), an Interim Authorization to Operate (IATO) or a Denial of Authorization to Operate. For existing systems already in operation or production, C&A is required whenever a significant change to the system occurs, OR every three years (known as re-certification and re-accreditation). For systems in development, C&A must be completed prior to the system achieving operational or production status.

(4) The C&A process consists of four distinct phases:

(a) Phase 1- Initiation;

(b) Phase 2- Certification;

(c) Phase 3- Accreditation; and

(d) Phase 4- Continuous Monitoring.

(5) Each phase consists of a set of well-defined requirements (tasks and steps) to be completed, as indicated, by the responsible individual(s). These required activities are performed on an information system at appropriate phases in the system life cycle.

(6) The successful completion of the C&A process provides VA officials with the necessary confidence that the information system has adequate security controls in place and functioning as intended, any vulnerabilities in the system have been considered in the risk-based decision to authorize processing, and appropriate plans and funds have been identified to plan for and correct all deficiencies in the information system that can be addressed.

b. C&A as it Relates to Other Information Security Activities

(1) In accordance with the provisions set forth by FISMA, VA is required to have an agency-wide information security program which is effectively integrated into the Agency's business processes and especially in the overall system life cycle of every Agency IT system.

(2) For new information systems (or major upgrades to existing information systems), the C&A tasks begin early as possible in the System Development Life Cycle (SDLC) in the Initiation, Development, and Acquisition phases and are important in shaping and influencing the security capabilities of the system. Refer to the following NIST Special Publications (SP) 800-30, *Risk Management Guide for Information Technology Systems*; 37, *Guide for the Security Certification and Accreditation of Federal Information Systems*; 39, *Managing Risk from Information Systems: An Organizational Perspective*; 64, *Security Considerations in the Information System Development Life Cycle*; 100, *Information Security Handbook: A Guide for Managers*, as well as VA Handbook 6500 for additional information on the SDLC. For operational and legacy systems, the C&A tasks will begin later in the SDLC; however, all C&A activities must be completed to ensure:

(a) The information system has received the necessary attention with respect to security; and

(b) The AO explicitly accepts the risk to VA operations, VA assets, or individuals based on the implementation of an agreed-upon set of security controls.

4. RESPONSIBILITIES

The responsibilities listed below are specific responsibilities related to C&A. For overall information security program responsibilities for these positions, see VA Directive and Handbook 6500.

a. **The Secretary of Veterans Affairs** has designated the Assistant Secretary for Information Technology as the senior agency official responsible for the C&A of VA information systems.

b. **Assistant Secretary for Information and Technology** is the Chief Information Officer (CIO) and is the **Authorizing Official (AO);** the AO is the senior management official authorized to assume the responsibility and accountability for operating an information system at an acceptable level of risk. The AO is involved with all activities associated with the C&A of VA systems and, as such, is responsible for:

(1) Assuming formal responsibility and accountability for the risks associated with operating an information system;

(2) Overseeing budget and business operations of the information system within the VA;

(3) Reviewing and approving the System Security Plan (SSP) for the information system;

(4) Determining the acceptability of the residual risk to VA operations or assets based on information generated during the security certification;

(5) Authorizing operation of an information system which includes either;

(a) An ATO;

(b) An Interim ATO under which certain terms and conditions may exist for operation; or

(c) A Denial of Authorization to Operate. Denying authorization includes the authority to halt existing operational systems after consulting with the System Owner if unacceptable security risks exist;

(6) Initiating security re-accreditation actions; and

(7) Receiving notification when continuous monitoring results indicate a significant change in security status for any information system.

c. **Deputy Assistant Secretary for Information Protection and Risk Management (IPRM**) is the **Authorizing Official Designated Representative** (AODR); the DAS for IPRM is responsible for:

(1) Acting on the AO's behalf in coordinating and performing the necessary activities required for the C&A process of an information system;

(2) Interacting with the System Owner, Information Security Officer (ISO), Certification Agent (CA), User Representatives and other interested parties during the C&A process;

(3) Reviewing all final C&A packages and making a decision recommendation to the AO to issue an IATO, ATO, or Denial of Authorization to operate;;

(4) Providing an IATO extension in the event local management can demonstrate continuous monitoring and security due diligence are being provided; and

(5) Checking with the AO to determine if the AO will be empowering the AODR to perform the following:

(a) Making decisions with regard to the planning and resources of the C&A activities;

(b) Accepting SSPs and security controls assessment plans;

(6) Assisting the AO by recommending a systems operational risk determination to VA operations, VA assets, and individuals; and

(7) Under the CIOs IT Single Authority, maintaining and managing the VA enterprise cyber security budget.

d. **Associate Deputy Assistant Secretary (ADAS) for Cyber Security** is the Chief Information Security Officer (CISO) for VA and is responsible for:

(1) Carrying out designated CIO duties and tasks under FISMA;

(2) Possessing professional qualifications, including training and experience, required to administer the information security program functions;

(3) Having information security duties as his/her official primary duty;

(4) Heading an office with the resources and mission to assist in ensuring VA compliance with FISMA;

(5) Serving as the primary liaison to the AO, AODR, System Owners, and ISOs;

(6) Reporting immediately to the Secretary any significant deficiency in compliance and providing immediate notification to the Secretary of any presumptive data breach; and

(7) Notifying the AO when continuous monitoring results indicate a significant change in security status for any information system.

e. **Associate Deputy Assistant Secretary for Privacy and Records Management** is responsible for:

(1) Establishing VA requirements and providing guidance regarding the development, completion, and updating of Privacy Impact Assessments (PIA);

(2) Assisting system owners in conducting PIAs as required; and

(3) Coordinating and assisting ISOs with privacy-related issues/activities associated with C&A activities.

f. **Associate Deputy Assistant Secretary for Risk Management Incident Response** is responsible for: Developing guidance and assisting in the identification, implementation, and maintenance of enterprise-wide information identity protection and risk assessment policies and procedures in coordination with stakeholders.

g. **Director, Business Continuity in the Office of Information Protection Risk Management** is responsible for:

(1) Establishing VA requirements and providing procedural guidance for the development of continuity of business plans for VA OI&T data processing facilities and VA information systems; and

(2) Assisting system owners and facility directors in preparing business continuity plans for VA facilities and information systems as required.

h. **Deputy Assistant Secretary for Enterprise Operations and Field Development** in the development of any new VA system, is responsible for:

(1) Assigning a program manager to implement security for all field development systems in the development phase of a system life cycle;

(2) Ensuring security requirements for the new system are defined and documented in the RA, SSP, and Contingency Plan;

(3) Creating, implementing, and documenting a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation;

(4) Creating, implementing and documenting a security control assessment plan;

(5) Ensuring a Privacy Impact Assessment is performed;

(6) Ensuring a C&A of the information system is completed prior to operational deployment; and

(7) Creating, implementing, and maintaining a process to continuously monitor the security controls of operational IT systems in cooperation with IPRM and the Oversight and Compliance Management Division; and

(8) Coordinating with the DAS for Information Protection and Risk Management to ensure security incorporated in each phase of SDLC.

i. **Deputy Assistant Secretary for Enterprise Development,** in Office of Information and Technology (OI&T), is responsible for:

(1) Assigning a program manager to implements security for all system software applications in the development phase of a system life cycle;

(2) Ensuring security requirements for the new system software applications are defined and documented in the RA, SSP, and Contingency Plan;

(3) Creating, implementing, and documenting a configuration management plan that controls changes to the system software applications during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation;

(4) Creating, implementing and documenting a security control assessment plan;

(5) Ensuring a Privacy Impact Assessment is performed; and;

(6) Ensuring a C&A of the information system software applications are completed prior to operational deployment; and

(7) Coordinating with the DAS for Information Protection and Risk Management to ensure security incorporated in each phase of SDLC.

i. **Executive Director, Oversight and Compliance Management Division,** in Office of Information and Technology (OI&T), is responsible for:

(1) Ensuring VA compliance with FISMA and 38 U.S.C. 5721-28 and other related security, privacy, and record management requirements promulgated by NIST, OMB, and VA information and

information security policies;

(2) Validating the successful remediation of system and security program POA&M items as identified in the Security Management and Reporting Tool (SMART) database; and

(3) Ensuring VA systems that have undergone a C&A are continuing to monitor and operate at their accredited level of risk by repeating a selection of security control assessment tests.

j. **Certification Agents (CA)** should be independent of those individuals responsible for correcting security deficiencies identified during the certification. This independence is an important factor in assessing the credibility of the security assessment results and ensuring the AO receives the most objective information possible in order to make an informed, risk-based, accreditation decision. The VA Certification Program Office (CPO) fulfills the role of the CA within VA and as such is responsible for:

(1) Conducting or overseeing security certification testing, a comprehensive assessment of the management, operational, and technical security controls for an information system, 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;

(2) Listing or describing the recommended corrective actions to reduce or eliminate vulnerabilities in the information system;

(3) Completing an independent assessment of the SSP as part of the Security Control Assessment (SCA) activities to determine if the SSP addresses a set of security controls which are consistent with the Federal Information Processing Standards (FIPS) Security Categorization and Risk Assessments completed for the information system. In addition, these security controls must be reviewed for adequacy and must meet all applicable security requirements;;

(4) Recommending corrective actions regarding SCA findings to reduce or eliminate, vulnerabilities identified for the information system via a Plan of Action & Milestones (POA&M); and

(5) Documenting an independent SCA based on testing results and providing a professional, honest opinion of whether the system security controls are operating as intended to achieve an acceptable level of risk, taking into consideration system and information sensitivity, and the timely completion of control deficiency remediation plans as outlined in the POA&M.

k. **System Owners (Information System Owners) (Regional Directors)** are responsible for:

(1) The overall procurement, development, integration, modification, daily operation, and maintenance of VA information and information systems; including ensuring each system under their responsibility is assigned a System Owner (local CIOs, System/Network administrators) responsible for the security of the system;

(2) The development and maintenance of system documentation including the SSP and contingency plan to ensure the system is deployed and operating according to the agreed-upon security requirements;

(3) Preparing POA&M items in SMART database to reduce or eliminate vulnerabilities in the information system;

(4) Tracking POA&M items in SMART database;

(5) Closing POA&M items in SMART database

(6) Informing VA key management officials of the need to conduct a C&A of the information system and ensure appropriate budget and resources are available for the effort;

(7) Providing the necessary system-related security documentation to the CA in a complete C&A package as described in this handbook;

(8) Receiving the security assessment results from the CA;

(9) Assembling the final security certification package and submitting the package to the AO for adjudication;

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

(11) Coordinating with business owners, local System Administrators (SA), ISO, and functional "end-users" for nationally deployed systems in regards to contingency planning;

(12) Reviewing and updating the SSP and contingency plans at least on an annual basis and when a significant change to the system occurs;

(13) Reviewing, updating, and testing the system contingency plan on an annual basis and when a significant change to the system occurs, as well as documenting the test results;

(14) Developing, implementing and maintaining the IT System Configuration/ Change Management Plan;

(15) Ensuring system users and support personnel receive required security training;

(16) Assisting local SAs in the identification, implementation, and assessment of common security controls;

(17) Ensuring risk assessments are periodically performed and at least one formal assessment is accomplished every three years or when a major change is incurred by the system, that risk determinations are reviewed/updated annually, and mitigation strategies are developed with the assistance of other VA officials with significant information and information system responsibilities;

(18) Ensuring a C&A of the information system is completed prior to operational deployment and systems are re-certified/accredited every three years, or whenever a significant change occurs;

(19) Ensuring each decision to utilize compensating controls or enhance the recommended security controls of the information system is fully documented and approved as a risk-based decision and

included in the ATO package submitted to the Certifying Official;

(20) Assisting other VA officials with significant IT responsibilities to remediate and update the POA&M identified during the C&A process, and conduct periodic compliance validation reviews and the FISMA annual assessment to reduce or eliminate system vulnerabilities;

(21) Ensuring continuous monitoring activities are being performed by reviewing regular system security reports and periodically re-testing a subset of system controls annually;

(22) Conducting Privacy Impact Assessments (PIA) as required; such as with the initial development of a system or upon major changes in the functionality; and

(23) Providing notification to the AO and ADAS of Cyber Security, in writing, when continuous monitoring results indicate a significant change in security status for their information system.

l. **Information (Data) Owners (Facility Directors/Program Managers)** are responsible for:

(1) The data or information stored within, processed by, or transmitted by an information system. It should be noted that a single information system may contain data from multiple Information Owners;

(2) Participating in RAs whenever deemed necessary or at a minimum, every three years, or when there is a major change to the system that requires officials to re-evaluate the sensitivity of the system, its data, the risks, and mitigation strategies;

(3) Providing input to System Owners regarding the data security requirements and the security controls for the information systems where their data resides;

(4) Providing assistance to the VA CIO regarding security requirements and appropriate level of security controls for the information system or system(s) where their information is currently created, collected, processed, disseminated, or subject to disposal;

(5) Determining which individuals have access to the system(s) containing their information, include types of privileges and access rights, and ensuring access privileges are reviewed on a regular basis in accordance with VA policy;

(6) Assisting the VA CIO by providing input for the identification and assessment of common security controls for systems where information resides; and

(7) Providing assistance to Administration and staff involved in the development of new systems regarding the appropriate level of security controls for his/her information.

(8) Ensuring respective staff, with defined FISMA security roles, provide the ISO (in a timely manner, as needed) with the information required to complete C&A activities and quarterly FISMA reporting to OI&T and OMB; and

(9) Ensuring all POA&M corrective actions are taken by their respective staff, and validating corrective actions taken by the System Owner with whom their data resides.

m. **Local CIOs/System Administrators/Network Administrators** are responsible for day-to-day system operations. The role of an SA must include security of Local Area Network (LAN) or application administration and account administration. The System/Network Administrator is responsible for:

(1) Ensuring system operational compliance with Federal security regulations and VA security policies;

(2) Assisting in the development and maintenance of SSPs, configuration management plans, and contingency plans for all systems under their responsibility;

(3) Participating in RAs whenever they are deemed necessary or when there is a major change to the system to re-evaluate sensitivity of the system, risks, and mitigation strategies;

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

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

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

(7) Ensuring the integrity in implementation and operational effectiveness of technical security controls by periodically conducting and repeating technical control testing and SCAs at the proper levels of assurance per NIST guidance and over the life cycle of the system;

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

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

(10) Acting as a representative of the VA user population in identifying mission/operational requirements and for complying with the security requirements and security controls described in the SSP;

(11) Providing information on users and/or the system in support of any reports or documents necessary for oversight and C&A;

(12) Understanding which systems, or parts of systems, for which they are directly responsible (network equipment, servers, LAN, etc.), the sensitivity of the information contained in these systems, and the appropriate measures to take to protect the information; and

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

n. **All Program Management** is responsible for:

(1) Assisting in the development and maintenance of information SSPs, configuration management plans, and contingency plans for all systems under their responsibility;

(2) Providing assistance to Administrations and Staff Offices involved in the development of new systems regarding the appropriate level of security controls for information systems and data;

(3) Providing oversight in the form of resource leveling, assignments or responsibility, work flow efforts, etc.;

(4) Identifying system assets, threats and vulnerabilities for facility risk assessment;

(5) Participating in RAs every three years, review/update annually, or when there is a major change to the system to re-evaluate sensitivity of the system, risks, and mitigation strategies;

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

(7) Providing assistance to the VA CIO regarding security requirements and appropriate level of security controls for the information system or system(s) where their information is currently created, collected, processed, disseminated, or subject to disposal;

(8) Verifying and validating, in conjunction with System Owners and VA Officials with daily system operating responsibilities, appropriate security measures are implemented and functioning as intended;

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

(10) Acting as a representative of the VA user population in identifying mission/operational requirements and for complying with the security requirements and security controls described in the SSP.

(11) Assigning a project manager to implement security for all systems in the development phase of a system life cycle.

o. **Information Security Officer (ISO);** ISOs are assigned responsibility by OI&T Field Security Operations to ensure the appropriate operational security posture is maintained for an information system or program and, as such, are responsible for:

(1) Serving as the principal staff advisor to the AO, AODR, System Owner , or ADAS of Cyber Security on all matters (technical and otherwise) involving the security of the information system;

(2) Serving as the primary POC and coordinator for all C&A activities within the facilities under his/her area of responsibility;

(3) Assisting the System Owner in developing and reinforcing security policies for information and the information system;

(4) Assisting the System Owner in managing and controlling changes to the information system, as well as, assessing the security impacts of those changes;

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

(6) Managing his/her local information security programs and serving as the principal security advisor to System Owners regarding security considerations in applications, systems, procurement or development, implementation, operation and maintenance, and disposal activities (life cycle management);

(7) Assisting the System Owner in the determination of an appropriate level of security commensurate with the risk categorization of the system;

(8) Coordinating, advising, and participating, under the guidance of the System Owner, in the development, maintenance, and uploading of SSPs, configuration management plans, and contingency plans for all systems under his/her responsibility;

(9) Ensuring risk assessments are accomplished every three years and reviewed/updated annually; and when there is a major change to the system to re-evaluate sensitivity of the system, risks, and mitigation strategies with the assistance of other VA officials with significant information and information system responsibilities;

(10) Verifying and validating, in conjunction with System Owners and VA Officials with daily system operating responsibilities, appropriate security measures are implemented and functioning as intended;

(11) Participating in security self-assessments, external and internal audits of system safeguards and program elements, and in C&A of the systems supporting the offices and facilities under his/her responsibility;

(12) Assisting other VA officials, with significant IT responsibilities (system managers, contracting staff, human resources staff, and police) in:

(a) Remediating and updating the POA&Ms identified during the C&A process;

(b) Completing and reviewing the input of the annual FISMA assessment with the system owners; and

(13) Acting as a representative of the VA user population while working in conjunction with Business Owners in identifying mission/operational requirements and for complying with the security requirements and security controls described in the SSP.

5. FUNDAMENTAL REQUIREMENTS

This section provides a global, high level perspective of basic concepts including documentation, process, and responsibilities associated with, or contained within, the C&A process and throughout the system life cycle. These requirements are fundamental to the success of the C&A process and, ultimately, the security of VA information and information systems.

a. Mission Requirements

(1) The determination of VA program-level or agency-level risk generally requires a broader, more strategic view of the VA than can be obtained from the more technically focused, system-level view of the information system which results from certification.

(2) AOs are better positioned to make mission risk determinations based on the known vulnerabilities remaining in the information system after the implementation of an agreed-upon set of security controls. The ultimate decision on the acceptability of such risk is the responsibility of the AO. AOs may, when needed, consult other individuals within VA, such as the ADAS for Cyber Security, ISO, System Owner, or the CA, at any phase in the C&A process to obtain advice on the security of the information system.

b. Capital Planning

(1) FISMA and other Federal regulations charge agencies with integrating information security technology, and Capital Planning and Investment Control (CPIC) processes which have been previously performed independently by security and capital planning practitioners. With increased competition for limited Federal budgets and resources, agencies must effectively bridge the gap between information system security technology and capital planning to help ensure available funding is applied to the highest priority information security and technology investments. Applying funds toward higher priority security investments supports the objective of maintaining appropriate security controls, both at the enterprise-wide and system level, commensurate with levels of risk and data sensitivity.

(2) OMB requires VA to prepare budget information for VA-specific investments (including the information system security technology component) and present them to the OMB on an annual basis using OMB Circular A-11, Exhibits 53 (Information Technology and E-Government) and 300 (Planning, Budgeting, Acquisition, and Management of Capital Assets). VA management prepares budget information for VA-specific investments and contracts incorporating the expenditures necessary to comply with Federal and VA information security standards and requirements as part of the budget preparation process, and throughout the expected life cycle of the budget line item. Cost expenditures include certification and re-certification which occurs every three years or when a significant change to the system has been made. System Owners may be required to fund certification efforts from the budget of the operating group in the event of a failure to reach an ATO in the initial C&A phase.

c. Acquisition

(1) VA relies heavily on vendor-provided information system security technology products and services, as well as cooperative agreements such as Memorandum of Understanding (MOU) and Memorandum of Agreement (MOA). Federal and VA information system security policies and requirements to safeguard the information and information systems are critical in the acquisition of VA products and services and in the awarding of contracts, grants, and cooperative agreements. Management is required to understand the risk and ramifications of purchasing products and awarding contracts, grants and cooperative agreements.

(2) VA management works with the VA office responsible for procurement via the approved VA IT tracking system. The procurement information contained within the VA IT tracking system is reviewed and approved by the VA OI&T Acquisition Team. This group is responsible for ensuring support service contracts and grants are flexible enough to ensure additional security requirements are incorporated quickly and efficiently, as required by law and by VA. Contractor information systems are subject to all requirements for Federal information systems (including the development and maintenance of SSPs, contingency plans, and C&A) as outlined in VA Directive and Handbook 6500. Contractors will require the same of all subcontracts or cooperative agreements.

d. Certification and Accreditation Media Protection and Document Marking

(1) VA considers information concerning VA IT systems to be SENSITIVE information. This includes, but is not limited to the following documents created for and in support of the C&A of VA systems, whether in electronic or hard copy:

(a) System inventories;

(b) System descriptions;

(c) System configurations for servers, desktops, and networking devices;

(d) Diagrams;

(e) Risk Assessments;

(f) Security controls;

(g) SSPs ;

(h) Contingency Plans;

(i) Privacy Impact Assessment

(j) POA&Ms;

(k) Standard Operating Procedures (SOP);

(l) Network monitoring (logs and network/vulnerability scans); and

(m) Penetration Test Reports.

(2) All SOPs, reports, logs, and records pertaining to C&A security issues are also considered SENSITIVE information. If the publication of any security related information could diminish or jeopardize the ability of VA to accomplish its mission, that information is also considered SENSITIVE information. Documents containing SENSITIVE information must be marked and protected in accordance with VA Handbook 6500.

(3) All C&A documentation is considered SENSITIVE information regardless of the Security Categorization (LOW, MODERATE, and HIGH) of the system. All users involved with VA SENSITIVE C&A information are required to ensure it is secured. All forms of hard copy and electronically stored media are also subject to the security requirements for SENSITIVE information. When SENSITIVE information is transmitted, it must be encrypted in accordance with FIPS Publication 140-2, *Security Requirements for Cryptographic Modules*. SENSITIVE information is not allowed to reside on non-VA systems or devices unless a waiver has been granted by the VA CIO or the ADAS for Cyber Security (as the designated representative of the CIO). All of these requirements for securing SENSITIVE information apply to any remote location(s) used for accessing or handling of that information.

6. CERTIFICATION AND ACCREDITATION PROCESS

a. Overview

(1) C&A are important activities which support a risk management process and are an integral part of the VA's information security program. Table 1, shown on the following page, presents a high-level view of the C&A process which is broken down into four phases. Table 1 includes the requirements (tasks) associated with each phase of the process. As in many processes, the last phase will eventually return to the first phase when the requirements to re-certify and re-accredit a system occur.

(2) Changes in law, Directives, policies, or regulations, while not always directly related to the information system, can potentially affect the security of a system and trigger a reaccredidation action. VA System Owners must be aware of such changes and perform a C&A accordingly. C&As must be performed, at least, every three years. The Enterprise Security Change Control Board (ESCCB) will assist System Owners in identifying changes resulting in a requirement for re-accreditation. Examples of significant changes may include but are not limited to:

(a) Installation of new or upgraded Operating Systems (OS), middleware components, or applications;

(b) Modification to system ports, protocols, or services; and

(c) Significant changes to the system physical or hardware environment.

Table 1: C&A Phases and Associated Requirements

Phase	Requirement
Phase 1- Initiation	• Preparation • Notification and Resource identification • SSP Analysis, Update, and Acceptance
Phase 2- Certification	• SCA • Certification Documentation
Phase 3- Accreditation	• Accreditation Decision • Accreditation Documentation
Phase 4- Continuous Monitoring	• Configuration Management & Control • Security Control Monitoring • Status Reporting and Documentation

(3) For detailed, step-by-step instructions for each phase, see the following Appendices of this document:

(a) Appendix C: Phase 1- Initiation;

(b) Appendix D: Phase 2- Certification;

(c) Appendix E: Phase 3- Accreditation; and

(d) Appendix F: Phase 4- Continuous Monitoring.

b. Phase 1: Initiation Summary

(1) The Initiation Phase consists of three tasks:

(a) Task A: Preparation;

(b) Task B: Notification and Resource Identification; and

(c) Task C: SSP Analysis, Update, and Acceptance.

(2) The objective of the Initiation Phase is to ensure the AO and ISO are in agreement with the contents of the SSP, including the documented security requirements and boundaries of the system, before the CA begins the assessment of the security controls within the information system. The early involvement of the AO and ISO, with key participants such as the ADAS for Cyber Security, System Owner , CA, and User Representatives are paramount to the success of the C&A effort.

(3) Phase 1: Initiation of the C&A process contains six elements serving as checkpoints to confirm the SSP and risk assessment have been completed. If a System Owner has not completed a risk assessment and a SSP, those activities must be completed prior to proceeding with the C&A process.

(4) A significant portion of the information needed to successfully complete the Initiation Phase is generated during the initial information system or facility risk assessment; the development of the SSP; and the results of previously conducted assessments such as, SCA, FISMA Annual Self-Assessment, Independent Verification and Validation (IV&V), and independent audits.

(5) For new information systems or systems undergoing major upgrades, this information is produced at the beginning of the system life cycle when system requirements are established.

(6) For systems currently in operation, this information is obtained from the most recent SSP and risk assessment.

(7) In most cases, SSPs have been previously reviewed and approved by the AO; therefore, the steps listed below in the preparation task should not require additional work on the part of the System Owner beyond what has already been accomplished.

(8) Table 2, shown on the following page, contains the high level tasks which must be satisfied in order to complete Phase 1, as well as the individuals responsible for each task. For detailed, step-by-step instructions, see Appendix C of this document.

Table 2: Phase 1-Initiation High-Level Summary of Required Tasks

Element	Task	Subtask Description	Responsibility	References
System Description	Preparation Task A	Confirm the information system has been fully described and documented in the SSP.	System Owner	NIST SP 800-18 NIST SP 800-30 NIST SP 800-37 VA Handbook 6500, Appendix D, CM-8, Information System Inventory
Security Categorization	Preparation Task A	Confirm the Security Categorization of the information system has been based upon the risk categorization of the data and documented in the SSP.	System Owner	FIPS Publication 199 NIST SP 800-18 NIST SP 800-30 NIST SP 800-37 NIST SP 800-59 NIST SP 800-60 VA Handbook 6500, Appendix D, RA-2, Security Categorization
Threat Identification	Preparation Task A	Confirm potential threats that could possibly exploit information system flaws or weaknesses have been documented in the SSP or Risk Assessment (RA).	System Owner and ISO	NIST SP 800-18 NIST SP 800-30 NIST SP 800-37 VA Handbook 6500, Appendix D, RA-3 Risk Assessment
Vulnerability Identification	Preparation Task A	Confirm flaws or weaknesses in the information system that could be exploited by potential threat sources have been identified and documented in the SSP or RA.	System Owner and ISO	NIST SP 800-30 NIST SP 800-37 NIST SP 800-40 VA Handbook 6500, Appendix D, RA-5, Vulnerability Scanning

Table 2: Phase 1-Initiation High-Level Summary of Required Tasks (Con't)

Element	Task	Subtask Description	Responsibility	References
Security Control Identification	Preparation Task A	Confirm security controls (either planned or implemented) have been identified and documented in the SSP.	System Owner	NIST SP 800-18 NIST SP 800-30 NIST SP 800-37 NIST SP 800-53 VA Handbook 6500, Appendix D, CM-6, Configuration Settings, CM-2, Baseline Configurations
Initial Risk Determination (anticipated)	Preparation Task A	Conduct a risk assessment to confirm the anticipated risk to VA operations, assets, or individuals has been determined and documented in the SSP.	System Owner	FISMA OMB Circular A-130, Appendix III NIST SP 800-30 NIST SP 800-37
Notification	Notification & Resource Identification Task B	Inform the ADAS for Cyber Security, AO, CA, User Representatives, and interested officials that the information system requires C&A support.	System Owner	OMB Circular A-130, Appendix III
Planning and Resources	Notification & Resource Identification Task B	Determine the level of effort and resources required for the C&A of the information system including the organizations involved and the preparation of a plan of execution.	AO, ADAS for Cyber Security, System Owner, and CA	OMB Circular A-130, Appendix III
Security Categorization Review	SSP Analysis, Update & Acceptance Task C	Review FIPS Publication 199 Security Categorization described in the SSP to determine if the assigned impact values, with respect to the potential loss of Confidentiality, Integrity, or Availability (CIA), are consistent with VA's actual mission requirements.	AO, ADAS for Cyber Security, and CA	FIPS Publication 199 NIST SP 800-37 NIST SP 800-60

Table 2: Phase 1-Initiation High-Level Summary of Required Tasks (Con't)

Element	Task	Subtask Description	Responsibility	References
SSP Analysis	SSP Analysis, Update & Acceptance Task C	Analyze the SSP to determine if the expected vulnerabilities in the information system and the resulting risk to VA operations (including mission, functions, image, or reputation) or VA assets are actually what the plan would produce, if implemented.	AO, ADAS for Cyber Security, and CA	NIST SP 800-18 NIST SP 800-37 VA Handbook 6500, Appendix D, PL-2, System Security Plan CM-1, Configuration Management Policy and Procedures
SSP Update	SSP Analysis, Update & Acceptance Task C	Update the SSP based on the results of the independent analysis and recommendations of the CA, AO and ADAS for Cyber Security.	System Owner	NIST SP 800-18 NIST SP 800-37 VA Handbook 6500, Appendix D, PL-3, System Security Plan Update
SSP Acceptance	SSP Analysis, Update & Acceptance Task C	Review the SSP to determine if the risk to VA operations (including mission, functions, image or reputation) or VA assets is acceptable.	AO and ADAS for Cyber Security	NIST SP 800-30 NIST SP 800-37

(9) Phase 1: Initiation, a Final Note: The following questions must be answered by the System Owner before proceeding to Phase 2:

(a) Does the FIPS 199 Security Categorization of the information system described in the SSP appear to be correct?

(b) Have the resources required to complete the C&A of the information system been identified and allocated successfully?

(c) Does the risk to VA operations (including mission, functions, image, or reputation), VA assets, or individuals described in the SSP appear to be correct?

(d) Having decided the anticipated risk appears to be correct and documented, would the risk be acceptable?

c. Phase 2: Certification

(1) Phase 2: Certification consists of two tasks:

(a) Task A: SCA; and

(b) Task B: Certification Documentation.

(2) The purpose of this phase is to determine the extent to which the security controls in the information system are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. This phase also addresses specific actions taken or planned, to correct deficiencies in the security controls, and to reduce or eliminate known vulnerabilities in the information system.

(3) Upon successful completion of this phase, the AO will have the information needed from the certification process to determine the actual risk to VA operations and VA assets and, thus, will be able to render an appropriate accreditation decision for the information system.

(4) Table 3, shown on the following page, contains the high level tasks which must be satisfied in order to complete Phase 2, as well as the individuals responsible for each task. For detailed, step-by-step instructions, see Appendix D of this document.

Table 3: Phase 2- Certification High-Level Summary of Required Tasks

Element	Task	Description	Responsibility	References
Documentation and Supporting Materials	SCA Task A	Assemble any documentation and supporting materials necessary for the assessment of the security controls in the information system which may include, but are not limited to: Previous security control assessments, audits, security certifications, security reviews, self-assessments, SCA reports, PIA, Common Criteria validations, and FIPS Publication 140-2 validation cert number and date (if applicable). Review all findings, results and evidence.	System Owner and CA	Documents and supporting materials included or referenced in the SSP FIPS Publication 140-2, Common Criteria NIST SP 800-53A
Reuse of Evaluation Results	SCA Task A	Assemble and review the findings, results, evidence, and documentation from previous assessments of the security controls in the information system which may include, but are not limited to: independent audits, security reviews, test and evaluation reports and self-assessments.	System Owner and CA	Documents and supporting materials included or referenced in the SSP
Methods and Procedures	SCA Task A	Select, or develop when needed, appropriate methods and procedures to assess the management, operational, and technical security controls in the information system.	CA	NIST SP 800-53A
Security Assessment	SCA Task A	Assess the security controls in the information system using techniques and procedures selected or developed to determine the effectiveness of those controls in a particular environment of operation.	CA	NIST SP 800-53A VA Handbook 6500, Appendix D, CA-4, Security Certification CA-2, Security Assessments
Security Assessment Report	SCA Task A	Prepare the final SCA report. See Appendix G of this document for a sample report format.	CA	NIST SP 800-53A
Findings and Recommendations	Certification Documentation Task B	Provide the System Owner with the SCA report.	CA	NIST SP 800-30 NIST SP 800-37

Table 3: Phase 2- Certification High-Level Summary of Required Tasks (Con't)

Element	Task	Description	Responsibility	References
SSP Update	Certification Documentation Task B	Update the SSP and RA based on the results of the SCA and any recommendations from the CA, AO and ADAS for Cyber Security.	System Owner	NIST SP 800-18 VA Handbook 6500, Appendix D, PL-3, System Security Plan Update
POA&M Preparation	Certification Documentation Task B	Prepare the POA&M document, based on the results of the SCA.	System Owner	OMB Memorandum 02-01 NIST SP 800-30 NIST SP 800-37 VA Handbook 6500, Appendix D, CA-5, Plan of Action and Milestones
Accreditation Package Assembly	Certification Documentation Task B	Assemble the accreditation package and submit to the AO. See Appendix G of this document for a sample Accreditation Package Transmittal Letter.	System Owner	OMB Circular A-130, Appendix III NIST SP 800-37

(5) Phase 2: Certification a Final Note:

The following questions must be answered by the System Owner before proceeding to Phase 3: Accreditation:

(a) To what extent are the security controls in the information system implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system?

(b) What specific actions have been taken, or are planned, to correct deficiencies in the security controls and to reduce or eliminate known vulnerabilities in the information system?

d. Phase 3: Accreditation

(1) The Accreditation process determines risk to VA based on the Certification results. Phase 3: Accreditation consists of two tasks:

(a) Task A: Accreditation Decision; and

(b) Task B: Accreditation Documentation.

(2) The purpose of this phase is to ensure the risk to VA operations, VA assets, or individuals is acceptable to the AO, and the acceptability of that risk forms the basis of the accreditation decision.

(3) Upon successful completion of this phase, the System Owner will have been granted one of the following:

(a) An ATO;

(b) An IATO; or

(c) Denial of authorization to operate the information system.

(4) Table 4, shown on the following page, contains the high level tasks which must be satisfied in order to complete Phase 3: Accreditation, as well as the individuals responsible for each task. For detailed, step-by-step instructions, see Appendix E of this document.

Table 4: Phase 3 Accreditation-High Level Summary of Required Tasks

Element	Task	Description	Responsibility	References
Final Risk Determination (Actual)	Accreditation Decision Task A	Determine the final actual risk to VA operations, VA assets, or individuals based on the vulnerabilities in the information system and any planned, or completed, corrective actions to reduce or eliminate those vulnerabilities- in accordance with identified system criticality to mission.	AO	NIST SP 800-30 VA Handbook 6500, Appendix D, CA-6 – Security Accreditation
Final Risk Acceptability	Accreditation Decision Task A	Determine if the final actual risk to VA operations, VA assets, or individuals is acceptable and prepare the final accreditation decision letter. See Appendix G of this document for a sample Accreditation Decision Letter.	AO	OMB Circular A-130, Appendix III NIST SP 800-37 VA Handbook 6500, Appendix D, CA-6, Security Accreditation
Accreditation Package Transmission	Accreditation Documentation Task B	Provide copies of the final accreditation package including the accreditation decision letter (in either paper or electronic form), to the System Owner and any other VA officials with a need to know in the security of the information system. If provided in electronic form, the documents must be encrypted per VA 6500. If the documents are provided in paper form, the documents must be properly marked as SENSITIVE per VA 6500.	AO	OMB Circular A-130, Appendix III NIST SP 800-37 VA Handbook 6500, Appendix D, CA-6, Security Accreditation

Table 4: Phase 3 Accreditation-High Level Summary of Required Tasks (Con't)

Element	Task	Description	Responsibility	References
SSP Update	Accreditation Documentation Task B	Update the SSP based on the final determination of risk to VA operations, VA assets, or individuals.	System Owner	NIST SP 800-18 VA Handbook 6500, Appendix D, CA-6, Security Accreditation, PL-3- System Security Plan Update

(5) Phase 3: Accreditation A Final Note: The following questions must be answered [by the AO and understood by the System Owner] before proceeding to Phase 4:

(a) How do the known vulnerabilities in the information system translate into VA agency level risk, and risk to VA operations, assets or individuals?

(b) What are the actual risks the AO is authorizing?

(c) Is the VA agency-level risk acceptable?

e. Phase 4: Continuous Monitoring

(1) Continuous Monitoring is routinely conducted on the information system. The SSP is updated continuously and security controls are reviewed, as needed, to ensure the security controls remain implemented and operate as intended.

(2) Phase 4: Continuous Monitoring consists of three tasks:

(a) Task A: Configuration Management and Control;

(b) Task B: Security Control Monitoring; and

(c) Task C: Status Reporting and Documentation.

(3) The purpose of this phase is to provide oversight and monitoring of the security controls for the information system on an ongoing basis and to inform the System Owner and the AO when changes occur impacting the security of the system. The activities in this phase are performed continuously throughout the system life cycle. Re-accreditation may be required due to specific changes made to the information system or when Federal or VA policies require periodic reauthorization of the information system.

(4) A Continuous Monitoring program is designed to determine, on an ongoing basis, if the security controls continue to be effective and provide essential, near real-time security status information. This enables the VA to make ongoing risk determinations and to take dynamic risk mitigation actions in order to make credible, risk-based decisions regarding the protection of the data and the secure operation of the system.

(5) A thorough Continuous Monitoring process provides updates to various system documents especially SSPs, assessment reports, and POA&Ms, and requires the following:

(a) Configuration Management and control processes;

(b) Security Impact Analysis (SIA) of changes;

(c) Assessment of selected security controls; and

(d) Status reporting.

(6) Current RA, results of previous assessments, and operational requirements guide the selection of the security controls to be monitored. Security control selection considers the following types of controls:

(a) High volatility controls (controls which change frequently);

(b) Security controls previously identified as ineffective or failed (listed in the POA&M);

(c) Baseline threats; an example of baseline threats can be found at http://www.sans.org. The SANS baseline threat list is updated annually and referred to as the SANS Top-20 Most Critical Internet Security Vulnerabilities List; and

(d) Security controls currently being monitored by normal operations.

(7) The ability of the Continuous Monitoring Process to provide frequent updates to the assessment report becomes a critical aspect of the overall system security program; therefore, it becomes increasingly important to provide updates on an ongoing basis to three key documents:

(a) SSP;

(b) Assessment Report; and

(c) POA&M.

(8) These documents provide the best indication of the overall security status of the information system and the ability of the system to protect, to the degree necessary, the VA's operations, VA's assets, individuals, and other organizations.

(9) Table 5, shown on the following page, contains the high level tasks which must be satisfied in order to complete Phase 4, as well as the individuals responsible for each task. For detailed, step-by-step instructions, see Appendix F of this document.

Table 5: Phase 4 Continuous Monitoring– High Level Summary of Required Tasks

Element	Task	Description	Responsibility	References
Documentation of Information System Changes	Configuration Management (CM) and Control Task A	Using established VA CM and control procedures, document proposed or actual changes to the information system including: hardware, software, firmware, and surrounding environment.	System Owner and/or ESCCB	VA's CM policies and procedures VA Handbook 6500, Appendix D, CM-3 Configuration Change Control
Security Impact Analysis	CM and Control Task A	Analyze the proposed or actual changes to the information system including hardware, software, firmware, and the surrounding environment to determine the security impact of such changes.	System Owner ISO	NIST SP 800-30 NIST SP 800-37 VA Handbook 6500, Appendix D, CM-4- Monitoring Configuration Changes
Security Control Selection	Security Control Monitoring Task B	Select the security controls in the information system to be monitored on a continuous basis, as needed and identified during Risk Assessment.	System Owner	NIST SP 800-37 NIST SP 800-53 OMB Circular A-130, Appendix III
Security Control Assessment	Security Control Monitoring Task B	Annually assess an agreed upon subset of security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.	System Owner	FISMA OMB Circular A-130, Appendix III NIST SP 800-37 NIST SP 800-42 NIST SP 800-53A VA Handbook 6500, Appendix D, CM-4, Monitoring Configuration Changes, CM-7 – Continuous Monitoring

Table 5: Phase 4 Continuous Monitoring– High Level Summary of Required Tasks (Con't.)

Element	Task	Description	Responsibility	References
SSP Update	Status Reporting and Documentation Task C	Update the SSP based on the documented changes to the information system including hardware, software, firmware, and surrounding environment and the results of the continuous monitoring process.	System Owner	NIST SP 800-18 VA Handbook 6500, Appendix D, PL-3, System Security Plan Update
POA&M Update	Status Reporting and Documentation Task C	Update the POA&M based on the documented changes to the information system and the results of the continuous monitoring process.	System Owner	NIST SP 800-37 OMB Memorandum 02-01 VA Directive 6500 Appendix D
SSP Reporting	Status Reporting and Documentation Task C	Report the status of the information system to the AO and ADAS for Cyber Security.	System Owner	FISMA OMB Circular A-130, Appendix III NIST SP 800-37

(10) Phase 4: Continuous Monitoring A Final Note: The following questions must be answered by the System Owner prior to reinitiating the C&A process for the information system:

(a) Have any changes to the information system affected the security controls within the system, or introduced new vulnerabilities into the system?

(b) If so, has the VA agency level risk (the risk to VA operations, VA assets, or individuals) been affected?

(c) Has a specified time passed requiring the information system to be reauthorized in accordance with Federal, NIST or VA policy?

7. REFERENCES

These requirements comply with established Federal information security laws and regulations, including:

a. E-Government Act of 2002, Public Law 107-347 § 208, 116 Stat. 2899, 2921 (2002);

b. Freedom of Information Act, 5 U.S.C. 552;

c. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191 § 264, 110 Stat. 1936, 2003;

d. Privacy Act of 1974, 5 U.S.C. 552a;

e. 38 U.S.C.§§ 5721-28;

f. Office of Management and Budget (OMB) Circular A -11, Planning, Budgeting, Acquisition of Capital Assets, Strategic Plans, Performance Plans;

g. Office of Management and Budget (OMB) Circular A -123, *Management's Responsibility for Internal Control*;

h. Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*;

i. National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Documents;

j. NIST's Special Publications (SP) SP-800 series; and

k. VA Directive and Handbook 6500, Information Security Program.

APPENDIX A: TERMS AND DEFINITIONS

1. **Accreditation**: The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.

2. **Accreditation Boundary**: All components of an information system to be accredited by an authorizing official and excludes separately accredited systems, to which the information system is connected.

3. **Accreditation Package**: The evidence provided to the authorizing official to be used in the security accreditation decision process. Evidence includes, but is not limited to the: (i) system security plan; (ii) assessment results from the security certification; and (iii) plan of action and milestones.

4. **Adequate Security**: Security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to, or modification of, information.

5. **Application**: The use of information resources (information and information technology) to satisfy a specific set of user requirements.

6. **Assessment Method**: A focused activity or action employed by an assessor for evaluating a particular attribute of a security control.

7. **Assessment Procedure**: A set of activities or actions employed by an assessor to determine the extent to which a security control is implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

8. **Authentication**: The process by which a user is identified for authorized access to VA information and information systems. Authentication consists of something a user knows (such as a password), something the user has (such as a token or smart card), or something the user is (such as a fingerprint).

9. **Authorizing Official**: Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.

10. **Authorizing Official's Designated Representative (AODR)**: Individual selected by an authorizing official to act on their behalf in coordinating and carrying out the necessary activities required during the security certification and accreditation of an information system.

11. **Availability**: Ensuring timely and reliable access to and use of information.

12. **Certification**: A comprehensive assessment of the management, operational and technical security controls in an information system, made in support of security accreditation, 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.

13. **Certification Agent (CA)**: The individual, group, or organization responsible for conducting a security certification.

14. **Chief Information Officer (CIO)**: Agency official responsible for: (i) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure information technology is acquired and information resources are managed in a manner consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency; (ii) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and (iii) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.

15. **Common Security Control**: Security control that can be applied to one or more agency information systems and has the following properties: (i) the development, implementation, and assessment of the control can be assigned to a responsible official or organizational element (other than the information system owner); and (ii) the results from the assessment of the control can be used to support the security certification and accreditation processes of an agency information system where that control has been applied.

16. **Compensating Security Controls**: The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high baselines described in NIST SP 800-53, which provides equivalent or comparable protection for an information system.

17. **Confidentiality**: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

18. **Configuration Control**: Process for controlling modifications to hardware, firmware, software, and documentation to ensure that the information system is protected against improper modifications before, during, and after system implementation.

19. **Countermeasures**: Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.

20. **Encryption**: The translation of data into a form that is unintelligible without a deciphering mechanism.

21. **General Support System (GSS)**: An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.

22. **High Impact System**: An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high. Refer to the definition provided under Potential Impact for more information.

23. **Improper or Inappropriate Usage**: Improper or inappropriate usage occurs when an individual uses VA information or information systems in violation of this Handbook and VA Directive 6001.

Examples of improper or inappropriate use are: a user provides illegal copies of software to others through peer-to-peer file sharing services or a person threatens another person through e-mail.

24. **Incident**: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. The term incident means security incident as defined in 38 U.S.C. 5727(18).

25. **Information Owner**: Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

26. **Information Resources:** Information in any medium or form and its related resources, such as personnel, equipment, funds, and information technology.

27. **Information Security**: A means for protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability.

28. **Information Security Officer (ISO)**: Individual responsible to the senior agency information security officer, authorizing official, or information system owner for ensuring the appropriate operational security posture is maintained for an information system or program.

29. **Information Security Policy**: Aggregate of directives, regulations, rules, and practices' prescribing how an organization manages, protects, and distributes information.

30. **Information Security Requirements**: Information security requirements promulgated in accordance with law, or directed by the Secretary of VA, the National Institute of Standards and Technology, and the Office of Management and Budget, and, as to national security systems, the President.

31. **Information Sensitivity**: Information sensitivity reflects the relationship between the characteristics of the information processed (e.g., personnel data subject to protection under the Privacy Act) and the mission need to ensure the confidentiality, integrity, and availability of the information (e.g., legal requirements to protect confidentiality of personal data). Sensitivity may vary from low, to medium, to high.

32. **Information System**: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, whether automated or manual.

33. **Information System Owner**: Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. Term is synonymous with System Owner

34. **Information Technology:** Any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive

agency. If the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use: (i) of that equipment; or (ii) of that equipment to a significant extent, in the performance of a service or the furnishing of a product. Includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but does not include any equipment acquired by a federal contractor incidental to a federal contract.

35. **Information Type**: A specific category of information, (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management), defined by an organization, or in some instances, by a specific law, Executive Order, directive, policy or regulation.

36. **Integrity**: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

37. **Interconnection Security Agreement (ISA)**: An agreement established between the VA and other organizations that own and operate connected IT systems to document the technical requirements of the interconnection. The ISA also supports a Memorandum of Understanding or Agreement between the organizations.

38. **Low Impact System**: An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low. Refer to the definition provided under Potential Impact.

39. **Local Area Network (LAN)**: Computer network that spans a relatively small area, such as a single building or group of buildings.

40. **Major Application**: An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

41. **Media**: Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks; magnetic disks; Large-Scale Integration (LSI) memory chips; and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.

42. **Memorandum of Agreement/Understanding (MOA/U)**: A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. In this guide, an MOA defines the responsibilities of two or more organizations in establishing, operating, and securing a system interconnection.

43. **Minor Application**: An application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Minor applications are typically included as part of a general support system.

44. **Moderate Impact System**: An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate and no security objective is assigned a FIPS 199 potential impact value of high. Refer to the definition provided under Potential Impact.

45. **Operating Unit**: An Operating Unit consists of any, and all, individuals responsible for the management, operation, maintenance, and security of VA's information and information systems within their area of responsibility. Examples of individuals who are part of the Operating Unit include, but are not limited to: Directors, Program Managers, and formation and Technology staff (system managers, SAs, and ISOs).

46. **Personally Identifiable Information (PII)**: See "Sensitive Personal Information" (SPI)

47. **Plan of Action and Milestones (POA&M)**: A documented plan that identifies tasks needing to be accomplished. It may also be used as a basis for the quarterly reporting requirements of OMB that includes the following information: (a) A description of the security weakness; (b) The identity of the office or organization responsible for resolving the weakness; (c) An estimate of resources required to resolve the weakness by fiscal year; (d) The scheduled completion date; (e) Key milestones with estimated completion dates; (f) Any changes to the original key milestone date; (g) The source that identified the weakness; and (h) The status of efforts to correct the weakness.

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

49. **Privacy Impact Assessment (PIA)**: An analysis of how information is processed: (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.

50. **Public Key Infrastructure (PKI)**: PKI is an environment based on the use of digital certificates and public and private key technology to secure communication of information. A fully deployed PKI supports encryption, authentication, privacy, and non-repudiation of information.

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

52. **Remote Location**: Any location at which the individual is conducting VA business and is not able to connect his/her computer directly to a VA controlled local area network or VA controlled wide area network that contains the systems needed for official duties. This includes a worker's home, a traveler's

hotel room, or an emergency worker's field location. Work from remote locations requires the use of telecommunications capabilities such as dial-up modems, Internet connectivity, or wireless networks to access VA information systems and information for official duty purposes.

53. **Remote User**: Any user who requires access to VA IT systems from a remote location. Users may include VA federal employees and contractors, employees of other federal agencies who require remote access to VA systems, and remote researchers processing VA information.

54. **Residual Risk**: Remaining risk not eliminated by implementation of security controls or countermeasures.

55. **Risk**: The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.

56. **Risk Assessment**: Process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses.

57. **Risk Management**: Process of managing risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system. It includes risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal authorization to operate the system. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations.

58. **Safeguards**: Protective measures prescribed to meet the security requirements (confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices (synonymous with security controls and countermeasures).

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

60. **Security Category**: The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.

61. **Security Controls**: The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

62. **Security Controls Assessment (SCA)**: Process used to examine the effectiveness of IT system controls with the objective of determining the true risk, or exposure, of the system to certain threats. Through the conduct of control tests, the Information Security Officer and system owner identify vulnerabilities that result from improper use of controls, missing controls, inherent system vulnerabilities,

or mismanagement. Through the application of SCA methods, the certification agent analyzes the current state of the system by reviewing the system objects and searching for anomalies that might indicate vulnerabilities that could permit an attack. SCA results in development of a plan of actions and milestones to track corrective actions necessary to mitigate vulnerabilities and reduce risk.

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

64. **Security Control Enhancements**: Statements of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control.

65. **Security Impact Analysis**: The analysis conducted by an agency official, often during the continuous monitoring phase of the certification and accreditation process, to determine the extent to which changes to the information system have affected the security posture of the system.

66. **Security Requirements:** Types and levels of protection necessary for equipment, data, information, applications, and facilities to meet laws, Executive Orders, directives, policies, or regulations.

67. **Senior Agency Information Security Office**: Official responsible for carrying out the Chief Information Officer (CIO) responsibilities under FISMA and serving as the CIO's primary liaison to the agency's authorizing officials, system owners and information security officers. The ADAS of Cyber Security is the Senior Agency Information Officer within VA.

68. **Senior Program Officials**: Upper-level managers in charge of line offices who directly report to the Operating Unit Head. For example, if the Operating Unit Head is an Under Secretary, then the senior program officials are the assistant secretaries or office directors, as applicable if the Operating Unit Head is a Director, then the senior program officials are the associate directors.

69. **Sensitive Personal Information (SPI)**: The term, with respect to an individual, means any information about the individual maintained by an agency, 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.

70. **Significant Change**: A significant (major) change is one that alters the baseline system configuration through the addition, deletion, or change of a configuration item within the system. Examples of significant changes to an information system that should be reviewed for possible re-accreditation include but are not limited to: (i) installation of a new or upgraded operating system, middleware component, or application; (ii) modifications to system ports, protocols, or services; (iii) installation of a new or upgraded hardware platform or firmware component; or (iv) modifications to cryptographic modules or services. Changes in laws, directives, policies, or regulations, while not always directly related to the information system, can also potentially affect the security of the system and trigger a re-accreditation action.

71. **Storage Media**: Any device or hard copy method for the retention of applications and data so that they are available for use. Storage media include: paper, hard drives, removable drives (such as Zip disks), Compact Disc (CD) - Read Only Memory (ROM) or CD-Recordable (CD-R) discs, Digital Versatile Disks (DVD), flash memory, USB drives, and floppy drives.

72. **Subsystem**: A major subdivision or component of an information system consisting of information, information technology, and personnel performing one or more specific functions.

73. **System**: See Information System.

74. **System Interconnection**: The direct connection of two or more IT systems for the purpose of sharing data and other information resources.

75. **System Owner**: See "Information System Owner".

76. **System Security Plan (SSP)**: Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.

77. **System-specific Security Control**: A security control for an information system that has not been designated as a common security control.

78. **Tailoring**: Process by which a security control baseline selected in accordance with the FIPS 199 security categorization of the information system is modified based on: (1) the application of scoping guidance; (2) the specification of compensating security controls, if needed; and (3) the specification of organization-defined parameters in the security controls, where allowed.

79. **Threat:** Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

80. **Threat Assessment**: Formal description and evaluation of threat to an information system.

81. **Threat Source**: Either: (i) intent and method targeted at the intentional exploitation of a vulnerability; or (ii) a situation and method that may accidentally trigger a vulnerability.

82. **Thumb Drive**: A USB Flash Drive is essentially NAND-type flash memory integrated with a USB 1.1 or 2.0 interface used as a small, lightweight, removable data storage device.

83. **Training**: A learning experience in which an individual is taught to execute a specific information security procedure or understand the information security common body of knowledge.

84. **Unauthorized Access**: Gaining logical or physical access to VA information or information systems either without authorization or in excess of previously authorized access.

85. **User Representative**: An individual that represents the operational interests of the user community and serves as the liaison for that community throughout the system development life cycle of the information system.

86. **VA Data or Information**: Information owned or in the possession of VA or any entity acting for or on the behalf of VA.

87. **VA Information System**: An information system used or operated by VA, by a contractor of VA, or by another entity on behalf of VA.

88. **VA National Rules of Behavior**: A set of Department rules that describes the responsibilities and expected behavior of personnel with regard to information system usage.

89. **VA Sensitive Data or Information**: All Department data, on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, records about individuals requiring protection under various confidentiality provisions such as the Privacy Act and the HIPAA Privacy Rule, and information that can be withheld under the Freedom of Information Act. Examples of VA sensitive information include the following: individually-identifiable medical, benefits, and personnel information; financial, budgetary, research, quality assurance, confidential commercial, critical infrastructure, investigatory, and law enforcement information; information that is confidential and privileged in litigation such as information protected by the deliberative process privilege, attorney work-product privilege, and the attorney-client privilege; and other information which, if released, could result in violation of law or harm or unfairness to any individual or group, or could adversely affect the national interest or the conduct of federal programs.

90. **Vulnerability**: A flaw or weakness in an information system, system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) by a threat source and may result in a security breach or a violation of the system's security policy.

91. **Vulnerability Assessment**: Formal description and evaluation of the vulnerabilities in an information system.

APPENDIX B: ABBREVIATIONS/ACRONYMS USED IN HANDBOOK AND APPENDICES

Abbreviation / Acronym	Description
ADAS	Associate Deputy Assistant Secretary
AO	Authorizing Official
AODR	Authorizing Official Designated Representative
ATO	Authority to Operate
C&A	Certification and Accreditation
CA	Certification Agent
CCB	Change Control Board
CD	Compact Disc
CD-ROM	Compact Disc Read Only Memory
CIA	Confidentiality, Integrity, and Availability
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CM	Configuration Management
CPIC	Capital Planning and Investment Control
CPO	Certification Program Office
DVD	Digital Versatile Disc
FAX	Facsimile
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GSS	General Support System
HIPAA	Health Insurance Portability and Accountability Act
IATO	Interim Authority to Operate
IPRM	Information Protection and Risk Management
ISA	Interconnection Security Agreement
ISO	Information Security Officer
IT	Information Technology
IV&V	Independent Verification and Validation
LAN	Local Area Network
MA	Major Application
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
ODCP	Organizationally Defined Control Parameters
OI&T	Office of Information and Technology
OMB	Office of Management and Budget
OS	Operating System
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
POC	Point of Contact
RA	Risk Assessment

Abbreviation / Acronym	Description
SA	System Administrator
SC	Security Control
SCA	Security Control Assessment
SMART	Security Management and Reporting Tool
SDLC	System Development Life Cycle
SIA	Security Impact Analysis
SOP	Standard Operating Procedures
SP	Special Publications
SSP	System Security Plan
ST&E	Security Testing and Evaluation
USC	United States Code
VA	Department of Veterans Affairs

APPENDIX C
PHASE 1: INITIATION

1. PHASE 1: INITIATION

The following steps provide the information necessary to satisfy the requirements of Phase 1- Initiation. Those requirements are:

a. Preparation;

b. Notification and Resource Identification; and

c. SSP Analysis, Update, and Acceptance.

2. TASK A: PREPARATION

This task focuses on preparing for C&A by reviewing the SSP to verify the contents of the document are consistent with the initial RA.

a. Step 1: Information System Description

(1) The System Owner is responsible for confirming the information system has been fully described and documented in the SSP. The level of detail in the SSP is commensurate with the FIPS Publication 199 Security Categorization of the information system (the level of detail in the SSP increases as the potential impact on VA operations, VA assets, or individuals' increases). Descriptive information about the information system is either documented in the system identification section of the SSP, or included as an attachment.

(2) Each system must have a system description listed in the SSP which must include the following:

(a) Name of the information system;

(b) A unique identifier in SMART database allowing the information system to be tracked for FISMA reporting requirements;;

(c) Status of the information system with respect to the system life cycle;

(d) Name and location of the organization(s) responsible for the information system;

(e) Contact information for the System Owner or other individual(s) knowledgeable about the information system;

(f) Contact information for the individual(s) responsible for the security of the information system;

(g) Purpose, functions, and capabilities of the information system;

(h) Types of information processed, stored, and transmitted by the information system;

(i) Boundary of the information system for operational authorization (accreditation);

(j) Functional requirements of the information system;

(k) Applicable laws, directives, policies, regulations, or standards affecting the security of information and the information system;

(l) Individuals using and supporting the information system (including individuals' organizational affiliations, access rights, privileges, and citizenship, if applicable);

(m) Architecture of the information system;

(n) Hardware and firmware devices (including wireless devices);

(o) System and application software (including mobile code);

(p) Hardware, software, and system interfaces (internal and external);

(q) Information flows (inputs and outputs);

(r) Network topology;

(s) Network connectivity rules for communicating with information systems external to the accreditation boundary as documented in Interconnection Security Agreements (ISA) and Memorandums of Understanding (MOU) (any systems external to VA must also be documented in the SSP);

(t) Interconnected information systems external to VA boundary and unique identifiers for each of those systems as documented in Interconnection Security Agreements (ISA) and Memorandums of Understanding (MOU);

(u) Encryption techniques used for information processing, transmission, and storage;

(v) Public key infrastructures, certificate authorities, and certificate practice statements;

(w) Physical environment in which the information system operates; and

(x) Web protocols and distributed, collaborative computing environments (processes and applications).

(3) The System Owner is responsible for ensuring the information system name, POC information for the System Owner, Local POC, and Regional Director are listed in the VA Enterprise Wide Assessment Tool, SMART. For information concerning SMART, including:

(a) Obtaining access;

(b) Adding/updating a system name/owner;

(c) Instructions on verifying a system is currently located in SMART; and

(d) Instructions on uploading a document into SMART, contact the SMART Help desk:

1. Via telephone;

2. Via email at vaocssmart@va.gov; or

3. Visit the Information Protection Portal at http://vaww.infoprotection.va.gov.

b. Step 2: Security Categorization

(1) FIPS Publication 199 establishes three potential impact levels (LOW, MODERATE, and HIGH) for each of the stated security objectives (confidentiality, integrity, and availability (CIA)) relevant to securing Federal information systems. These impact levels focus on the potential impact and magnitude of harm the loss of CIA would have on VA operations, VA assets, or individuals.

(2) An information system may contain more than one type of information (for instance, privacy-protected information, medical information, proprietary information, financial information, contractor sensitive information, system security information), each of which is subject to Security Categorization. The Security Categorization of an information system which processes, stores, or transmits multiple types of information should be the highest impact level determined for each type of information for each security objective of CIA.

(3) For details on how to determine security categorization, refer to FIPS Publication 199, NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories or VA Handbook 6500 (Section: Policies and Procedures, Subsection: System Security Categorization); and VA Handbook 6500, Appendices D and E.

(4) The System Owner is responsible for confirming the security categorization of the information system has been determined and documented in the SSP, and the SSP has been uploaded into SMART. The function of uploading the SSP into SMART has been delegated by the System Owner as an ISO responsibility.

c. Step 3: Threat Identification

(1) The System Owner is responsible for confirming potential threats which could exploit information, information system flaws, or weaknesses have been identified and documented in the SSP or as an attachment. It is important to consider and document all potential threats which may cause harm to an information system, ultimately affecting the CIA of the system. Some examples of threats include:

(a) Natural (floods, earthquakes, tornadoes, landslides, avalanches, electrical storms);

(b) Human (events either enabled by or caused by human beings); or

(c) Environmental (long-term power failures, pollution, chemicals, liquid leakage).

(2) The most common types of resources available for monitoring cyber threats include, but are not limited to:

(a) Vendor web sites and mailing lists;

(b) Third-party web sites; and

(c) Third-party mailing lists and newsgroups.

(3) Threat resources in general include, but are not limited to the following:

(a) Previous RAs;

(b) Incidents;

(c) Past Threat Assessments;

(d) Current FISMA self-assessment;

(e) Interview with the Information Owner and System Administrator;

(f) Previous Inspector General (IG) Report; and

(g) Privacy Issues and past POA&Ms.

(4) Threat information (including capabilities, intentions, and resources of potential adversaries) for a specific information system is generally nonspecific or incomplete, at best. For an acknowledged set of baseline threats to all information systems, see the SANS Top-20 Most Critical Internet Security Vulnerabilities List found at http://www.sans.org. In today's interconnected and interdependent information systems environment, which encompasses many common platforms and technologies, there is a high likelihood of a variety of threats (both intentional and unintentional) acting to compromise the security of VA information and information systems.

(5) In addition to the generalized assumption concerning threats, specific threat information should be used, if available, during the RA to help guide the selection of security controls for the information system. Threat identification information should be coordinated with the System Owner, ADAS for Cyber Security and the AO to facilitate reuse and sharing with other System Owners, enterprise-wide.

(6) The level of effort applied to the threat identification process should be commensurate with the Security Categorization of the information system. In other words, the level of effort increases as the potential impact on agency operations, agency assets, or individuals increases. Threat identification information is typically documented in the RA, which is either included in the SSP or as an attachment.

(7) For further information regarding Threat Identification, refer to NIST SP 800-30, and VA Handbook 6500, Appendix D, RA-3, Risk Assessment.

d. Step 4: Vulnerability Identification

(1) The System Owner is responsible for confirming flaws or weaknesses in the information system, which could be exploited by potential threat sources, have been identified and documented in the SSP or Risk Assessment. Vulnerability identification may be conducted during any phase of the system life cycle. The vulnerability focus is dependent upon which stage the system is in, such as:

(a) Systems Under Development: Vulnerabilities focus on the organization's security policies, planned security procedures, application of security requirements contained in the VA Enterprise Requirements Repository, system requirement definitions, and developer security product analyses.

(b) Systems Being Implemented: Vulnerability identification is expanded to include more specific information, such as the planned security features described in the system design documentation and the results of the developmental SCA.

(c) Operational Systems: Vulnerability identification includes the analysis of the security controls employed to protect the system. Vulnerability identification may be accomplished in a variety of ways; using questionnaires, on-site interviews, document reviews, and/or automated scanning tools. Vulnerability sources include the following:

1. Previous RA documentation;

2. Audit Reports;

3. System anomaly reports;

4. Security reviews;

5. Self assessments;

6. Results of vulnerability scans and penetration tests;

7. Previous SCA reports;

8. Vulnerability lists;

9. Security advisories;

10. Vendor advisories;

11. Commercial computer incident/emergency response teams and post lists;

12. Information security vulnerability alerts and bulletins; and

13. Hardware, software, or firmware security analyses.

(2) Vulnerability information is coordinated between the System Owner and AO to facilitate reuse and sharing with other System Owners, enterprise-wide. The level of effort applied to the vulnerability identification process should be commensurate with the security controls of the information system. Threat identification information is documented in the RA, which is either included in the SSP or as an attachment.

(3) For further information regarding vulnerability identification, refer to NIST SP 800-30, Section 3.3, Vulnerability Identification, NIST SP 800-40, and VA Handbook 6500 Appendix D, RA-5, Vulnerability Scanning.

e. Step 5: Security Control Identification

(1) The System Owner is responsible for confirming the security controls (either planned or implemented) for the information system have been identified and documented in the SSP, and/or RA.

(2) Minimum security control baselines for LOW, MODERATE, and HIGH risk information systems are listed in NIST SP 800-53, SP 800-53A, and VA Handbook 6500, Appendix D. These predefined sets of security controls (targeted toward the risk levels defined in the FIPS Publication 199 Security Categorization) provide a baseline, or starting point, for VA to address the necessary safeguards and countermeasures required for VA's information systems.

(3) Per VA Handbook 6500, VA Operating Units will perform additional analyses to determine if adjustments to the baseline set of security controls are necessary. These adjustments to the baseline set of security controls may take the form of adding supplemental security controls or eliminating certain security controls based on specific threats and vulnerability information generated during the RA for the information system and VA's determination of an acceptable level of risk.

f. Baseline Tailoring

(1) Tailoring of the baseline, as defined in NIST SP 800-53, is accomplished by applying scoping guidance, creating compensating controls, and defining organizational parameters. The following sections provide a basic foundation for tailoring and scoping the baseline.

(2) Essentially, common sense needs to be applied while tailoring security controls as it is an activity requiring the System Owner to take into consideration all of the potential factors contained with the scoping guidance. For further details, refer to VA Handbook 6500, Appendix D

g. Scoping Guidance

(1) Scoping guidance provides organizations with specific terms and conditions on the applicability and implementation of individual security controls in the security control baselines. There are several considerations, described below, potentially impacting how the baseline security controls are applied by the organization:

(a) Common Controls: are typically identified and assigned to organizational entities during a collaborative VA agency-wide process with the involvement of the CIO, ADAS for Cyber Security, System Owner, AO, and ISO. The organizational entities are determined based on which VA organization is the appropriate group to be responsible for the common security controls. Common controls are then managed by each appropriate organizational entity. All controls must be addressed either by the organizational entity as a common control or by the System Owner as a system specific control. The designation as a common control does not relieve the Information Owner or the ISO from the responsibility of reviewing the control and providing additional information as necessary. The VA may assign a hybrid status to security controls in situations where one part of the control is deemed to be common, while another part of the control is deemed to be system-specific. For example, the VA may view the IR-1 (Incident Response Policy and Procedures) security control as a hybrid control with the policy portion of the control deemed to be common and the procedures portion of the control deemed to be system-specific. Hybrid security controls may also serve as templates for further control refinement. An organization may choose, for example, to implement the CP-2 (Contingency Planning) security control as a master template for a generalized contingency plan for all organizational information systems with individual System Owners tailoring the plan, where appropriate, for system-specific issues.

(b) Operational/Environmental Controls: dependent on the operational environment and are applicable only if the information system is in an environment requiring the controls. For example, temperature and humidity controls may not be applicable outside of a specific room/location containing information systems.

(c) Physical Infrastructure Controls: refer to organizational facilities and only apply to those parts of the facility related to the information system. In other words, the specific room where an information system is located may require protection such as a specific type of lock; however, the entire facility may not require specific locks for all doors.

(d) Public Access Controls: associated with public access systems and may require special consideration. In other words, will public users need to supply identification and authentication in order to access the information system? If yes, then compensating or supplementary controls discussed in following sections must be considered.

(e) Technology Controls: refer to specific technologies which apply only where the technology is used. For example, controls referring to wireless technology only apply where the wireless technology is being used. Also, automated mechanisms are required for MODERATE and HIGH systems where they are available, feasible, and cost-effective. In situations where the automated mechanisms are not employed, compensating security controls are required to satisfy the security requirements and are sufficiently developed to accomplish the same goals.

(f) Policy and Regulatory Controls: are only required if the use of those controls correspond with the information and information system types governed by applicable laws, Executive Orders, directives, policies, standards, or regulations.

(g) Scalability Controls: are scalable and scalability is guided by the FIPS 199 Security Categorization of the information system being protected. For example, the size and complexity of a risk assessment for a FIPS 199 HIGH-impact information system may be significantly greater than the size and complexity of a risk assessment for a FIPS 199 LOW-impact information system. VA organizations will use discretion in applying the security controls to information systems, giving consideration to the scalability factors in particular environments. This approach facilitates a cost-effective, risk-based approach to security control implementation which expends no more resources than necessary, yet achieves sufficient risk mitigation and adequate security.

(h) Security Objectives Controls: uniquely support the individual components of CIA and may be downgraded (to a corresponding control in a lower baseline control), modified, or eliminated. A control may be considered for downgrading, modification, or elimination if, and only if, it meets the requirements in VA Handbook 6500. The applicable condition must be fully documented in the SSP as part of the justification to downgrading, modifying or eliminating a security control.

h. Compensating Controls

(1) A compensating security control is a management, operational, or technical control employed by the VA in lieu of a recommended security control in the LOW, MODERATE, or HIGH baselines as described in VA Handbook 6500, which provides equivalent or comparable protection for an information system.

(2) Compensating controls may be employed only under the following conditions:

(a) It is selected from VA Handbook 6500 Appendix D or if one is not available, a suitable control is adopted;

(b) A rationale is supplied explaining why the baseline control could not be used and how the compensating control provides equivalent protection; and

(c) The risk of using the compensating control is assessed and the System Owner accepts the risk.

(3) The use of compensating controls must be fully documented in the SSP and be approved by the AO.

i. Organizational Defined Control Parameters

(1) For some controls listed in the VA Handbook 6500, Appendix D, a degree of flexibility is provided by allowing organizations to selectively define input values for certain parameters associated with the controls. This flexibility is achieved through the use of assignment and selection operations within the main body of the control. Once specified, the organizationally-defined value becomes part of the control, and the organization is assessed against the completed control statement.

(2) VA Organizationally Defined Control Parameters (ODCP), add the flexibility to define portions of controls and are documented in the SSP. The VA adheres to the ODCP maximum and minimum values (where specified) unless more restrictive values are required. VA Handbook 6500 Appendix E, *Control Configuration Standards*, contains the VA's ODCPs.

j. Supplementing the Baseline Security Controls

(1) The Information Owner, System Owner, and ISO are responsible for the final determination of the appropriate set of security controls necessary to establish and maintain adequate security for VA information systems. Determination of security controls is a function of the information system RA and analysis. Included in this analysis is the review of controls to sufficiently mitigate risks to VA.

(2) Using the tailored security control baseline as the foundation, or starting point, in the selection of adequate security controls for an information system, additional security controls or control enhancements may be needed to address specific threats and vulnerabilities of an information system. Security controls or control enhancements may also be selected to satisfy the requirements of applicable laws, policies, or regulations. The RA of each system provides important inputs to determine the sufficiency of the security controls in the tailored baseline.

(3) The security control catalog in VA Handbook 6500, Appendix D, contains security controls and control enhancements found only in HIGH-impact baselines, or are not included in any of the standard baselines. The VA will make maximum use of the security control catalog to facilitate the process of enhancing security controls or adding controls to the tailored baseline before creating new security controls or enhancements.

(4) If the System Owner, Information Owner or Operating Unit discovers sufficient security controls cannot be applied within an information system to adequately reduce or mitigate mission risk, an alternative strategy considering those risks must be applied. Restrictions on the use of information systems provide such an alternative method to reduce or mitigate risk. For example when:

(a) Security controls cannot be implemented within technology and resource constraints; or

(b) Security controls lack the reasonable expectation of effectiveness against identified threat sources.

(5) When it is not practical to enable mission accomplishments through tailoring or supplementing security controls, restrictions to the VA information system may be necessary. The decision to utilize restrictions is determined by the System Owner. Examples of how to apply restrictions include:

(a) Limiting the information an information system can process, store, or transmit;

(b) Limiting the manner in which a mission (or task) is automated;

(c) Prohibiting external information system access to critical organizational information by removing selected system components from the network (air gapping). In other words, disconnecting system inner-connectivity resulting in a stand alone system; or

(d) Prohibiting MODERATE or HIGH impact information on an information system component to which the public has access, unless an explicit determination is made authorizing such access.

(6) It is essential for the System Owner to document in the SSP the following items regarding supplementary controls:

(a) Decisions made during the security control selection process;

(b) Sound rationale for those decisions;

(c) Agreed-upon set of security controls; and

(d) Any restrictions on the use of the information system.

(7) Adjustments to the baseline set of security controls should be reasonable, appropriate, and fully documented in the SSP along with supporting rationale. Upon completion of the security control identification process, the agreed upon set of controls should satisfy the specified security requirements and adequately protect the CIA of the system and its information. Security control information is typically documented in the Controls sections (management, operational, and technical) of the SSP. The degree of rigor and formality applied to the security control selection process should be commensurate with the FIPS 199 Security Categorization of the information system.

k. Step 6: Initial Risk Determination

(1) The System Owner confirms the anticipated risk to VA operations, VA assets, or individuals has been determined and documented in the SSP and RA.

(2) FISMA and OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, require an assessment of risk as part of a risk-based approach to determining adequate, cost-effective security for an information system. The methods used to assess risk should include consideration of the major factors in risk management including:

(a) Threats to and vulnerabilities in the information system;

(b) Potential impact and magnitude of harm to VA operations, VA assets, or individuals which may result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or the information system; and

(c) The effectiveness of current or proposed security controls.

(3) In most cases, it is impractical to plan for, or implement, security controls which address all potential vulnerabilities. Expected vulnerabilities are those vulnerabilities expected to remain in the information system after the employment of the planned or implemented security controls.

Vulnerabilities resulting from the absence of security controls or the ineffectiveness of controls (controls not implemented correctly, operating as intended, or producing the desired outcome with respect to meeting system security requirements) provide the basis for determining the agency-level risk posed by the operation of the information system.

(4) The degree of rigor and formality applied to the RA should be commensurate with the FIPS 199 Security Categorization of the information system. In other words, the level of effort increases as the potential impact on VA operations, VA assets, or individuals increases.

(5) Assessing risk is an ongoing activity ensuring new threats and vulnerabilities are identified and appropriate security controls are implemented. VA agency-level risk will be documented in the RA which is either included in the SSP or as an attachment.

(6) VA will provide a VA approved risk assessment tool.

3. TASK B: NOTIFICATION AND RESOURCE IDENTIFICATION

a. The objectives of this task are to:

(1) Provide notification to all concerned agency officials as to the impending C&A of the information system;

(2) Determine the resources needed to carry out the effort; and

(3) Prepare a plan of execution for C&A activities reflecting the proposed schedule and key milestones.

b. Step 1: Notification

(1) The System Owner is responsible for informing key VA officials such as the ADAS for Cyber Security, ISO, AO, CA, User Representatives, as well as those VA officials with a valid need-to-know of the system requiring C&A support.

(2) The initial notification- in writing- of key VA officials is an important activity establishing the C&A process as an integral part of the system life cycle. This notification also serves as an early warning to help prepare potential participants for the upcoming tasks necessary to plan, organize, and conduct the C&A.

(3) Supplemental Guidance for LOW Impact Systems: A simplified notification procedure (verbal or in writing) is recommended. The System Owner notifies the AO and CA that a self-assessment of the information system's security controls is planned and provides an estimated completion date.

c. Step 2: Planning and Resources

(1) The AO, ADAS for Cyber Security, System Owner and CA are responsible for determining the level of effort and resources required for the C&A of the information system (including the organization(s) involved) and for preparing a plan of execution.

(2) The level of effort required for security certification is dependent upon three factors:

(a) The size and complexity of the information system;

(b) The FIPS 199 Security Categorization of the system; and

(c) The security controls employed to protect the system.

(3) Identifying appropriate resources (supporting organizations, funding, and individuals with critical skills) needed for the C&A effort is an essential aspect of the initial Preparation activities and is typically integrated within the system life cycle, capital planning, and budgeting processes.

(4) Once a CA is selected (or certification services procured), an execution plan for conducting the C&A is prepared by the CA and approved by the System Owner , AO, and ADAS for Cyber Security. An execution plan contains specific tasks, milestones, and delivery schedule. This information can be reflected in a system development/change plan for the information system.

(5) Supplemental Guidance for LOW Impact Systems: For LOW impact systems, a simplified planning procedure is recommended. The System Owner estimates the level of effort required for a self-assessment (See NIST SP 800-53A) of the information system's security controls. The AO, ADAS for Cyber Security, and CA are not required to participate in the process.

4. TASK C: SYSTEM SECURITY PLAN ANALYSIS, UPDATE, AND ACCEPTANCE

a. The objectives of this task are to:

(1) Perform an independent review of the FIPS 199 Security Categorization;

(2) Obtain an independent analysis of the SSP;

(3) Update the SSP, as needed, based on the results of the independent analysis; and

(4) Obtain acceptance of the SSP by the AO and ADAS for Cyber Security prior to conducting an assessment of the security controls in the information system.

b. The completion of this task concludes the Initiation Phase of the C&A process.

c. Step 1: Security Categorization Review

(1) The System Owner , CA, AO, and ADAS for Cyber Security are responsible for reviewing the FIPS 199 Security Categorization described in the SSP to determine if the assigned impact values, with respect to the potential loss of CIA, are consistent with VA's actual mission requirements.

(2) FIPS Publication 199 is used as a fundamental part of the VA's risk management program. Properly identifying the sensitivity of the data and that of the system used to store and process it is essential when determining appropriate security controls to apply in each information system and to ensure the controls are adequately assessed to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the system's security requirements.

(3) The review of the Security Categorization ensures the System Owner has adequately reflected upon the importance (including criticality and sensitivity) of the information and the system in supporting VA operations and assets. An independent review of the Security Categorization by the CA, AO, and ADAS for Cyber Security is performed, as needed, to ensure appropriate categorization.

(4) Supplemental Guidance for Low Impact Systems: An independent CA is not required to participate in the process.

(5) For further information, refer to VA Handbook 6500 Appendix D, RA-2 Security Categorization.

d. Step 2: System Security Plan Analysis

(1) The AO, ADAS for Cyber Security, and CA are responsible for analyzing the SSP to determine if the vulnerabilities in the information system and the resulting risk to VA operations, VA assets, or individuals are actually what the plan would produce, if implemented.

(2) The SSP provides an overview of the requirements for the protection of the information and information system and describes the security controls in place, or planned, for meeting those requirements. The independent review of the SSP by the CA, AO, and ADAS for Cyber Security during any phase of the system life cycle determines if the plan is complete and consistent with the requirements document for the information system. The review can also determine if the expected remaining vulnerabilities and resulting residual risks appear to be correct and reasonable. Based on the results of the review and analysis, the CA, AO, and ADAS for Cyber Security may recommend changes to the SSP. If these changes are able to be implemented, the System Owner then updates the appropriate section of the SSP, RA, or attachments accordingly.

e. Step 3: System Security Plan Update

(1) The SSP is updated based on the results of the independent analysis and recommendations of the CA, AO, and ADAS for Cyber Security.

(2) The System Owner is responsible for reviewing the changes recommended by the CA, AO, and ADAS for Cyber Security and consults with other VA representatives (ISO, Information Owner or User Representatives), prior to making any final modifications to the SSP.

(3) Modifications to the SSP may include any of the areas described in Task A (adjusting security controls, changing vulnerabilities, or modifying the agency-level risk).

(4) All SSPs should be reviewed annually and must be updated whenever system changes are made (see PL-3 for additional information).

(5) Supplemental Guidance for LOW Impact Systems: An independent CA is not required to participate in the process.

f. Step 4: System Security Plan Acceptance

(1) The SSP is reviewed to determine if the risk to VA operations, VA assets or individuals is acceptable. The VA agency-level risk described in the SSP, RA, or an attachment to the SSP is deemed one of the following:

(a) Unacceptable: The AO and ADAS for Cyber Security are responsible for returning the plan to the System Owner for appropriate action; or

(b) Acceptable: The AO and ADAS for Cyber Security are responsible for accepting the plan.

(2) Acceptance of the SSP represents an important milestone in the C&A of the information system. The AO and ADAS for Cyber Security, by accepting the SSP, are agreeing to the set of security controls proposed to meet the security requirements for the information system. This VA agency-level agreement allows the C&A process to advance to the next phase (the actual assessment of the security controls).

(3) Acceptance of the SSP also approves the level of effort and resources required to complete the associated C&A activities.

(4) Supplemental Guidance for LOW Impact Systems: For LOW impact systems, a simplified review process is recommended. The AO and ADAS for Cyber Security conduct a cursory review of the SSP to determine the acceptability of VA agency-level risk. Minimal analysis is required.

APPENDIX D
PHASE 2: CERTIFICATION

1. PHASE 2: CERTIFICATION

a. The objectives of Phase 2: Certification are:

(1) SCA; and

(2) Certification Documentation.

b. The purpose of this phase is to determine the extent to which the security controls in the information system are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. This phase also addresses specific actions taken, or planned, to correct security control deficiencies and to reduce or eliminate known vulnerabilities in the information system.

c. Upon successful completion of this phase the:

(1) CA will be able to determine the extent to which the security controls in the information system are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system;

(2) CA will be in a position to make recommendations on corrective actions for security control deficiencies and to offer advice to the System Owner and AO on how the known vulnerabilities in the system may translate into agency-level risk.

(3) AO will have the information needed from the certification and CA recommendations to determine the risk to VA operations, VA assets, or individuals and, thus, will be able to render an appropriate accreditation decision for the information system.

d. The VA is required to conduct an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. In other words, the VA will assess all security controls in an information system during the initial security accreditation. Subsequent to the initial accreditation, and in accordance with OMB policy, the VA will assess a subset of the controls annually during continuous monitoring. The VA may use the current year assessment results obtained during certification to meet the annual FISMA assessment requirement.

2. TASK A: SECURITY CONTROL ASSESSMENT

a. The objectives of the SCA task are to:

(1) Prepare for the assessment of the security controls in the information system;

(2) Conduct the assessment of the security controls; and

(3) Document and evaluate the results of the assessment.

b. Preparation for an assessment involves:

(1) Gathering appropriate planning and supporting materials;

(2) Gathering system requirements and design documentation;

(3) Gathering security control implementation evidence;

(4) Gathering results from previous assessments, security reviews, or audits; and

(5) Developing specific methods and procedures to assess the security controls in the information system.

c. At the completion of this task, the CA will be able to:

(1) Determine the extent to which the security controls in the information system are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system;

(2) Make recommendations on corrective actions for security control deficiencies which the System Owner uses to develop the POA&M; and

(3) Offer advice to the System Owner and AO on how the known vulnerabilities in the system may translate into organizational and/or agency-level risk.

d. The VA is required to conduct an assessment of the security controls in the information system at least annually 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. A security control assessment is intended to support the FISMA requirement stating the controls in each information system are assessed with a frequency dependent on risk, but no less than annually. While OMB does not require an annual assessment of all security controls in the VA, it is expected that the VA will assess all of the security controls during the three-year accreditation cycle.

e. Existing security assessment results may be reused to the extent they are still valid and are supplemented with additional assessments, as needed. Reuse of assessment information is critical in achieving a broad-based, cost-effective, and fully integrated security program capable of producing the evidence necessary to determine the actual security status of the information system. The VA may use the current year assessment results obtained during certification to meet the annual FISMA assessment requirement.

3. STEP 1: DOCUMENTATION AND SUPPORTING MATERIALS

a. Assemble any documentation and supporting materials necessary for the evaluation of security controls in the information system.

b. The System Owner is responsible for assisting the CA in gathering all relevant documents and supporting materials from the VA which will be required during the assessment of the security controls. Descriptive information about the information system is documented in the system identification section of the SSP or as an attachment to the plan. Other supporting materials providing evidence of security control implementation are collected including, but not limited to, the following:

(1) Policies and Procedures;

(2) Reports;

(3) Logs; and

(4) Records.

c. Supplemental Guidance for LOW Impact Systems: For LOW impact systems, the information system owner will employ the services of the ISO or other designated individuals (including contractors) to assist in the assembly of documentation and supporting materials necessary for a self-assessment of the information system's security controls and the review of findings, results, and evidence from previous assessments of the security controls. An independent CA is recommended but not required to participate in the process.

4. STEP 2: REUSE OF ASSESSMENT RESULTS

a. Assessing the security controls in an information system can be a costly and time-consuming process. In order to make the C&A process as timely and cost-effective as possible, the CA is responsible for maximizing the use of previous assessment results, when reasonable and appropriate, to determine the extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Other sources of assessment results may include, but are not limited to, the following:

(1) Important information about the effectiveness of the security controls produced during a recent audit of an information system;

(2) Programs testing and evaluating the security features of commercial information technology products;

(3) Previous assessment results from the system developer; and

(4) Previous assessments of the security controls in the information system.

b. Supplemental Guidance for LOW Impact Systems: For LOW impact systems, the System Owner will employ the services of the ISO, or other designated individuals (including contractors), to assist in the assembly and review of findings, results, evidence, and documentation from previous assessments of the information system's security controls. An independent CA is recommended, but not required to participate in the process.

5. STEP 3: METHODS AND PROCEDURES

a. The CA is responsible for selecting, or developing when needed, appropriate methods and procedures to assess or test the security controls in the information system.

b. In lieu of developing unique or specialized methods and procedures to evaluate the security controls in the information system, the CA should consult VA Handbook 6500, Appendix D.

c. The CA, if so directed by the System Owner, AO, or ADAS for Cyber Security, can supplement these assessment methods and procedures. Assessment methods and procedures may need to be:

(1) Created for those security controls not contained in NIST SP 800-53 but employed by the VA; and/or

(2) Tailored for specific system implementations.

d. Supplemental Guidance for LOW Impact Systems: For LOW impact systems, the System Owner will employ the services of the ISO, or other designated individuals (including contractors), to select or develop, when needed, the appropriate methods and procedures necessary to conduct a self-assessment of the information system's security controls. An independent CA is recommended, but not required to participate in the process.

6. STEP 4: SECURITY ASSESSMENT

a. The CA is responsible for assessing the security controls in the information system using methods and procedures selected or developed.

b. An SCA determines the extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The results of the assessment, including recommendations for correcting any security control deficiencies, are documented in the assessment report.

c. Supplemental Guidance for LOW Impact Systems: For LOW impact systems, the System Owner may employ the services of the ISO or other designated individuals (including contractors) to conduct a self-assessment of the information system's security controls. An independent CA is recommended, but not required to participate in the process.

7. SECURITY ASSESSMENT REPORT

a. The CA is responsible for preparing the final SCA report and ensuring the following items are included:

(1) The results and findings of the assessment- the determination of the extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system; and

(2) Recommendations for correcting security control deficiencies and reducing, or eliminating, identified vulnerabilities.

b. The assessment report is part of the final accreditation package, along with the updated SSP and POA&M. The assessment report is the CA's statement regarding the security status of the information system (refer to Appendix G of this document for a sample Security Control Assessment Report).

c. Supplemental Guidance for LOW Impact Systems: For LOW impact systems, the System Owner may employ the services of the ISO, or other designated individuals (including contractors), to prepare the assessment report containing the results of the self-assessment of the information system's security controls. The assessment report may be a short, concise document synopsizing the self-assessment results and highlighting areas needing further attention. An independent CA is not required to participate in the process.

8. TASK B: CERTIFICATION DOCUMENTATION

a. The objectives of the Certification Documentation task are to:

(1) Provide the findings of the certification and recommendations to the System Owner ;

(2) Update the SSP as needed;

(3) Prepare the POA&M; and

(4) Assemble the accreditation package.

b. By implementing the corrective actions recommended by the CA, the System Owner has an opportunity to reduce, mitigate, or eliminate vulnerabilities in the information system prior to the assembly and compilation of the accreditation package and submission to the AO. The CA assesses any security controls modified, enhanced, or added during this process.

c. The Certification Documentation task contains three steps, which are listed on the following page(s). The Certification Phase is considered complete once all steps within Task B have been accomplished.

9. STEP 1: FINDINGS AND RECOMMENDATIONS

a. The CA is responsible for providing the System Owner with the SCA report. The System Owner relies on the security expertise and the technical judgment of the CA to:

(1) Assess the effectiveness of the security controls in the information system; and

(2) Provide specific recommendations regarding how to correct security control deficiencies and to reduce or eliminate vulnerabilities in the information system.

b. If there are specific opportunities to correct security control deficiencies and to reduce or eliminate vulnerabilities, the System Owner may choose to act on selected recommendations of the CA

prior to the accreditation package becoming finalized. To ensure effective allocation of resources agency-wide, any actions taken by the information System Owner prior to the final accreditation decision are coordinated with the AO and the ADAS for Cyber Security. Any changes made to security controls in response to corrective actions by the System Owner must be assessed by the CA and the SCA report updated.

c. Supplemental Guidance for LOW Impact Systems: For LOW impact systems, the ISO or his/her designee (including contractors) provides the System Owner with the assessment report containing the summarized results of the self-assessment of the information system security controls. An independent CA is not required to participate in the process.

10. STEP 2: SYSTEM SECURITY PLAN UPDATE

a. The System Owner is responsible for updating the SSP and RA according to the SCA results and any modifications made to the security controls in the information system. The SSP is updated to contain:

(1) A reflection of the actual state of the security controls after the security assessment;

(2) Any modifications by the System Owner in addressing the recommendations for corrective actions from the CA; and

(3) An accurate list and description of the security controls implemented and a list of identified vulnerabilities such as controls not implemented- this may also require updating the RA.

b. In addition, the security control, PL-3, System Security Plan Update, requires the VA to update the SSP on an ongoing basis so that it reflects the current state of security, both actual and planned. NIST SP 800-18 provides guidance on SSP updates.

c. Supplemental Guidance for LOW Impact Systems: An independent CA is not required to participate in the process.

11. STEP 3: PLAN OF ACTION AND MILESTONES PREPARATION

a. The System Owner is responsible for preparing the POA&M, in a timely and cost-effective fashion, based on the results of the SCA report and depending on the severity and significance of the deficiency that has been detected. It is important to prioritize POA&Ms and determine exactly what a "timely" response is. POA&Ms can be generated at any time a deficiency is noticed in addition to the "en-masse" generation of POA&Ms after the SCA phase of a C&A. The security control CA-5, Plan of Action and Milestones, requires VA Operating Units to develop a POA&M and update it quarterly.

b. The POA&M document is a key document in the accreditation package, as it is developed for the AO and subject to Federal reporting requirements established by OMB. It describes actions taken, or planned, by the System Owner to correct security control deficiencies and to address remaining vulnerabilities in the information system (reduce, eliminate, or accept the vulnerabilities).

c. The POA&M document is based on findings of SCA reports, Security Impact Analysis and continuous monitoring activities and identifies:

(1) Tasks needing to be accomplished;

(2) Resources required to accomplish the elements of the plan;

(3) Any milestones in meeting the tasks; and

(4) Scheduled completion dates for the milestones.

d. The Office of Management and Budget (OMB) issued memorandums provide specific guidance on preparing and submitting the POA&M, and *NIST SP 800-30, Risk Management Guide for Information Technology Systems* provides guidance on risk mitigation.

12. STEP 4: ACCREDITATION PACKAGE ASSEMBLY

a. The System Owner is responsible for the compilation and assembly of the final accreditation package, including inputs from the ISO and the CA, and must submit the package electronically to the SMART in order for the AO to receive it. For information on SMART, contact the SMART Help desk:

(1) Via telephone;

(2) Via email at vaocssmart@va.gov; or

(3) Visit the Information Protection Portal at http://vaww.infoprotection.va.gov.

b. The System Owner is responsible for ensuring the contents of the accreditation package are protected as SENSITIVE in accordance with VA policy. At a minimum, it must contain a SENSITIVE document cover sheet and markings (refer to VA Certification and Accreditation Handbook, section titled “Certification and Accreditation Media Protection and Document Marking”). For further information regarding SENSITIVE information, refer to VA Handbook 6500, Subsection titled “VA Sensitive Data/Information”, and subsection titled “Information Concerns”).

c. A Transmittal Letter accompanies the accreditation package. Refer to Appendix G of this document for a sample Transmittal letter. The accreditation package contains the following:

(1) The assessment report from the CA providing the results of the independent assessment of security controls, including any residual risks, and recommendations for corrective actions;

(2) The POA&M from the System Owner indicating actions taken or planned, to correct security control deficiencies and to reduce or eliminate vulnerabilities in the information system; and

(3) The updated SSP with the latest copy of the Risk Assessment and Contingency Plan;

(4) Configuration Management Plan;

(5) Security Configuration Checklist; and

(6) Privacy Impact Assessment (PIA).

d. The CA input to the final accreditation package provides an unbiased and independent view of the extent to which the security controls in the information system are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

e. The System Owner may consult with other key VA participants, prior to submitting the final accreditation package. The AO will use this information during the Accreditation phase to determine the risk to VA operations, VA assets, or individuals.

f. Refer to OMB Circular A-130, Appendix III, for additional information.

g. Supplemental Guidance for LOW Impact Systems: For LOW impact systems, the accreditation package consists of: The updated SSP including the latest copy of the RA, an abbreviated assessment report (a brief summary of the self-assessment results), and the POA&M.

APPENDIX E
PHASE 3: ACCREDITATION

1. PHASE 3: ACCREDITATION

a. The Accreditation Phase consists of two tasks:

(1) Task A: Accreditation Decision; and

(2) Task B: Accreditation Documentation.

b. The purpose of this phase is to determine if the risk to VA operations, VA assets, or individuals is acceptable to the AO - the acceptability of that risk forms the basis of the accreditation decision. Upon successful completion of this phase, the System Owner will have one of the following:

(1) Full ATO the information system;

(2) An IATO the information system under specific terms and conditions; or

(3) Denial of Authorization to Operate the information system.

c. Security accreditation requires the VA to accredit the information system for processing before operations and to update the authorization at least every three years or when there is a significant change to the system. The AO signs and approves the security accreditation.

d. OMB Circular A-130, Appendix III, establishes policy for the security accreditation of Federal information systems. The organization assesses the security controls employed within the information system before, and in support of, the security accreditation. To reduce the burden of the three-year reaccreditation process, the AO uses the results of the ongoing continuous monitoring process to the maximum extent possible.

2. TASK A: ACCREDITATION DECISION

a. The objectives of the accreditation decision task are to:

(1) Determine the risk to VA operations, VA assets, or individuals; and

(2) Determine if the VA agency-level risk is acceptable.

b. The AO, working with information produced during Phase 2 now has the SCA Report (an independent confirmation of the identified vulnerabilities in the information system), the POA&M (a list of planned or completed corrective actions to reduce, mitigate, or eliminate known vulnerabilities), and the SSP. These documents, provided by the System Owner, ISO, and CA are used to determine the final risk to VA, and the acceptability of that risk.

3. STEP 1: FINAL RISK DETERMINATION

a. Determine the risk to VA operations, VA assets, or individuals based on the vulnerabilities in the information system and any planned, or completed, corrective actions to reduce or eliminate those vulnerabilities.

b. The AO is responsible for the following:

(1) Receiving and reviewing the final accreditation package from the System Owner ;

(2) Assessing the vulnerabilities in the information system confirmed by the CA and determining how those vulnerabilities translate into risk to the VA;

(3) Judging which vulnerabilities are of greatest concern to the VA and evaluating if the vulnerabilities can be tolerated without creating unreasonable risk;

(4) Considering the POA&M in determining the risk to the VA; and

(5) Consulting with the System Owner, CA, or other VA official(s) having a need-to-know of the security of the information system before making the final risk determination, if needed.

c. Supplemental Guidance for LOW Impact Systems: For LOW impact systems, a simplified process for risk determination is recommended. The AO's level of effort in determining the risk and potential impact on VA operations, assets, and/or individuals should be commensurate with the previously determined LOW Security Categorization. An independent CA is recommended but not required to participate in the process.

4. STEP 2: RISK ACCEPTABILITY

a. Determine if the risk to VA operations, VA assets, or individuals is acceptable and prepare the final accreditation decision letter.

b. The AO considers many factors when deciding if the risk to VA operations, VA assets, or individuals is acceptable; balances security considerations with mission and operational needs; reviews all of the relevant information and, where appropriate, consults with key VA official(s) having a need-to-know of the security of the information system. The AO then renders an accreditation decision for the information system, which takes one of the three following forms (refer to Appendix G of this document for samples of each letter):

(1) ATO - if the AO deems the agency-level risk fully acceptable, an ATO is issued and the information system is accredited without any restrictions or limitations on its operation.

(2) IATO - if, after assessing the results of the security certification, the AO deems the agency-level risk unacceptable, but there is an important mission-related need to place the information system into operation or to continue its operation, an IATO may be issued. An IATO may be considered when the identified vulnerabilities in the system resulting from deficiencies in the planned or implemented security controls are significant, but can be addressed in a timely manner. The IATO is a limited

authorization to operate under specific terms and conditions including corrective actions to be taken by the System Owner. An IATO requires a specific timeframe for the completion of those remediation or corrective actions. A detailed POA&M must be submitted by the System Owner and approved by the AO prior to the IATO taking effect. The information system is not accredited during the period of limited authorization to operate. The System Owner is responsible for completing the corrective actions identified in the POA&M and resubmitting an updated accreditation package upon completion of those actions. When the security related deficiencies have been adequately addressed and an updated C&A package is submitted, the IATO may be lifted and the information system authorized to operate.

(a) IATOs granted from VA will extend, at most, to six months.

(b) If an information system is not granted an ATO within this six-month time frame, an IATO extension request for an additional six months may be submitted through the AODR or the AO. Requests must be accompanied by an updated POA&M which contains milestones, thus enabling the information system to reach accreditation within six months.

(3) Denial of Authorization to Operate - if, after assessing the results of the security certification, the AO deems the agency-level risk unacceptable, the information system is not authorized for operation and, thus, is not accredited. If the system is currently in operation, all activity must cease.

c. Failure to receive an ATO usually indicates the presence of major security control deficiencies in the system. The AO works with the System Owner to review the POA&M to ensure proactive measures are taken to correct the security control deficiencies.

d. The AO prepares the final security accreditation decision letter (refer to Appendix G of this document for a sample letter). The accreditation decision letter includes the following:

(1) Accreditation decision (ATO, IATO, or Denial of Authorization to Operate);

(2) Supporting rationale justifying the AO’s decision;

(3) Terms and conditions for the operation of the information system including a description of any limitations or restrictions placed on the operating system which must be adhered to by the System Owner ; and

(4) Any required corrective actions.

e. The contents of the accreditation package shall be protected as SENSITIVE in accordance with VA policy. For further information regarding protecting SENSITIVE documents, see VA Handbook 6500, Sections titled, “VA Sensitive Data/Information, and Information Concerns,” as well as the Media Protection and Document Marking section of this document.

f. Supplemental Guidance for LOW Impact Systems: For LOW impact systems, a simplified process for the determination of risk acceptability is recommended. The AO’s level of effort in determining risk acceptability should be minimal given that the potential impact on VA operations, VA assets, and/or individuals has previously been determined to be LOW.

5. TASK B: ACCREDITATION DOCUMENTATION

a. The objectives of this task are to:

(1) Transmit the final accreditation package to the appropriate VA individual(s) and organization(s); and

(2) Update the SSP with the latest information from the accreditation decision.

b. This task contains two steps which are listed below. The completion of this task concludes Phase 2: Accreditation of the C&A process.

6. STEP 1: ACCREDITATION PACKAGE TRANSMISSION

a. The accreditation package, including the accreditation decision letter, is returned to the System Owner and any other VA official(s) having a need-to-know of the security of the information system. Upon receipt of the accreditation package, the System Owner signs the decision letter thereby acknowledging receipt and accepting the terms and conditions of the authorization.

b. The following steps are taken in this process:

(1) The AO returns the accreditation package including the dated accreditation decision letter to the System Owner ;

(2) The System Owner accepts the terms and conditions of the authorization;

(3) The original accreditation package is kept on file by the System Owner;

(4) The AO and ADAS for Cyber Security also retain copies of the accreditation decision letter and package; and

(5) The accreditation package contains VA SENSITIVE information and must be safeguarded (both electronic and hard copy) and stored centrally so as to be readily available upon request. For further information regarding safeguarding VA SENSITIVE information, refer to VA Handbook 6500.

7. STEP 2: SYSTEM SECURITY PLAN UPDATE

a. The System Owner is responsible for updating the SSP to reflect any changes made to the information system resulting from the Accreditation Phase. Any terms or conditions set forth in the accreditation decision are also documented in the SSP. It is expected that changes to the SSP in this phase of the C&A process will be minimal.

b. The VA requires an update to the SSP on an annual basis so that it reflects the current state of security, both actual and planned.

APPENDIX F
PHASE 4: CONTINUOUS MONITORING

1. PHASE 4: CONTINUOUS MONITORING

a. The Continuous Monitoring Phase consists of three tasks:

(1) Task A: Configuration Management (CM) and control;

(2) Task B: Security Control monitoring; and

(3) Task C: Status reporting and documentation.

b. The purpose of this phase is to provide oversight and monitoring of the security controls in the information system on an ongoing basis and to inform the AO when changes occur which may impact the security of the system. Such changes to the information system may require reaccreditation. Federal and VA policy also requires periodic reaccreditation of the information system. Continuous Monitoring is performed throughout the life cycle of the information system and ensures the integrity of the SSP and security controls.

c. C&A documentation, such as the SSP, is not treated as shelf-ware; instead, it is a living document which is continuously updated as changes occur throughout each week, month, and year as appropriate.

2. TASK A: CONFIGURATION MANAGEMENT AND CONTROL

a. The objectives of this task are to:

(1) Document the proposed or actual changes to the information system; and

(2) Determine the impact of those proposed or actual changes on the security of the system.

b. Typically, information systems are in a constant state of change due to upgrades to hardware, software, or firmware, and modifications to the system environment. In order to maintain the status of a security accreditation, it is essential to document system changes in the SSP and assess the potential impact on the security of the system. This process must be performed on an ongoing basis.

c. The purpose of CM is to manage the effects of changes or configuration differences in an information system or network. CM assists in streamlining change management processes and prevents changes which could detrimentally affect the security posture of a system before they occur. By providing a repeatable mechanism for affecting system modifications in a controlled environment, the CM process reduces the risk that changes made to a system may result in a compromise to the system or loss of data CIA.

d. The change control process is the responsibility of the Change Control Manager and the CCB which involves:

(1) Identifying change;

(2) Evaluating change requests (are they viable, correct, feasible, what do they affect, what are the associated costs);

(3) Making an implementation decision (approving, denying, deferring); and

(4) Implementing approved changes.

e. Configuration change control involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the information system, including upgrades and modifications. It also includes changes to the configuration settings of information technology products (operating systems, firewalls, routers). Any activities associated with configuration changes to the information system must be audited.

f. Changes resulting from the remediation of flaws via patch management must be visible to the configuration change control process. The patch management process is also an integral part of the continuous monitoring process.

g. Configuration Change Control requires the VA to authorize, document, and control changes to the information system when the Security Categorization is MODERATE or HIGH. The information system change control board monitors changes to the system and ensures impact analyses are completed and changes are documented with the system configuration management plan which is part of the information system security plan documentation.

h. In addition, the VA is required to monitor changes to the information system and to conduct System Impact Analysis to determine the effects of the changes.

3. STEP 1: DOCUMENTATION OF INFORMATION CHANGES

a. The System Owner is responsible for using established VA CM and control procedures; documenting proposed or actual changes to the information or the information system (including hardware, software, firmware, and surrounding environment).

b. Managing, controlling, and documenting change(s) to an information system is critical to the continuous assessment of the security controls protecting the system.

c. Any relevant information about proposed changes to hardware, firmware, or software must be documented. This includes but is not limited to:

(1) Version or release numbers;

(2) New or modified features or capabilities;

(3) Security implementation guidance; and

(4) Changes to the physical environment in which the system resides.

d. The System Owner and ISO use this information in assessing the potential security impact of the proposed or actual changes to the information system. Significant changes to the system should not be undertaken prior to assessing the security impact of such changes.

e. VA SSPs should be augmented with a Change Log documenting relevant system or environmental changes, as well as steps taken to eliminate/mitigate any risks introduced by the plan. See Appendix G of this document for a sample Change Log. The Change Log should be summarized as part of the yearly SSP Status Report provided to the AO.

4. STEP 2 SECURITY IMPACT ANALYSIS

a. The System Owner is responsible for analyzing the proposed or actual changes to the information system (including hardware, software, firmware, and the surrounding environment) to determine the security impact of such changes.

b. The information collected in the previous step (Documentation of Information System Changes) is used by the System Owner and the ISO to assess the potential impact of the proposed or actual changes to the information system. Information system changes may produce new vulnerabilities, change the way current security controls operate, or even generate a need for new security controls. When an SIA indicates the proposed or actual changes to the information system will affect, or have affected security requirements, corrective action is required and the POA&M must be revised in a timely fashion.

c. Prior to implementing any security-related changes, it may be necessary to consult with other VA officials. If an SIA reveals a significant change in security posture, the AO is immediately notified so a decision can be made regarding whether or not reaccredidation is necessary. Conducting an SIA is part of the ongoing assessment of risk within the VA.

d. The degree of rigor and formality applied to the SIA should be commensurate with the FIPS Publication 199 Security Categorization. In other words, the level of effort increases as the potential impact on VA operations, VA assets, or individuals increases).

5. TASK B: SECURITY CONTROL MONITORING

a. The objectives of the security control monitoring task are to:

(1) Select an appropriate set of security controls currently existing within the information system to be monitored; and

(2) Assess the designated controls using methods and procedures selected by the System Owner.

b. The continuous monitoring of security controls helps to identify potential security-related problems in the information system not identified during the SIA conducted as part of the CM and control process.

c. The VA is required to monitor the security controls in the information system on an ongoing basis and to document the process. Subsequent to the initial accreditation, the VA will assess a subset of the controls. The selection of an appropriate subset of security controls is based on:

(1) The FIPS Publication 199 Security Categorization of the information system;

(2) Specific security controls selected and employed by the organization to protect the information system; and

(3) The level of assurance (grounds for confidence) the organization must have in determining the effectiveness of the security controls in the information system.

d. An effective continuous monitoring program results in ongoing updates to the SSP, SCA report, and POA&M which are the three principle documents in the accreditation package. A rigorous and well-executed continuous monitoring process significantly reduces the level of effort required for the reaccreditation of the information system. The reduced level of effort can be achieved through re-use of security control testing information or work accomplished during the FISMA self assessment phase.

6. STEP 1: SECURITY CONTROL SELECTION

a. The System Owner is responsible for selecting the security controls in the information system to be monitored on a continuous basis.

b. The criteria established by the System Owner for selecting which security controls will be continuously monitored should reflect the following:

(1) VA's priorities and the importance of the information system to the VA; for example, certain security controls may be considered more critical than other controls because of the potential impact on the information system, should the controls be subverted or found to be ineffective;

(2) Importance of the control in maintaining the system's security;

(3) Volatility of the control environment;

(4) History of the reliability of the control (consider POA&M items); and

(5) Cost of performing the monitoring activities (consider controls requiring monitoring as a part of normal operations).

c. The AO and System Owner agree upon a subset of security controls to be monitored, as well as the frequency of the monitoring activities. The System Owner recommends a prioritized list of security controls to the responsible CIO and the ADAS for Cyber Security for approval.

d. The level of effort applied to the security control selection process must be commensurate with the FIPS Publication 199 Security Categorization of the information system.

e. A well-designed and well-managed continuous monitoring program can effectively transform an otherwise static SCA and risk determination into a dynamic process which provides essential, near real-time security status-related information to appropriate organizational officials. This information allows officials to take appropriate risk mitigation actions and to make credible, risk-based authorization decisions regarding the operation of the information system.

7. STEP 2: SECURITY CONTROL ASSESSMENT

a. The System Owner is responsible for assessing an agreed upon set of security controls within the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome in regards to meeting the security requirements of the system.

b. It is at the discretion of the System Owner to choose from a variety of methods and procedures used to assess security controls which may include, but are not limited to:

(1) Reviews;

(2) Self-assessments;

(3) SCAs;

(4) Audits;

(5) Network monitoring; and

(6) Log management and analysis.

c. System Owners should first consult VA Handbook 6500 for standardized methods and procedures for assessing security controls prior to considering developing unique or specialized methods. The monitoring process must be documented and available for review by the AO or ADAS for Cyber Security, upon request.

d. Corrective actions and updates to the POA&M are required whenever the results of continuous monitoring indicate the effectiveness of a control has been reduced and is detrimentally affecting the security of the system. An update to the POA&M may also be required if a new vulnerability is discovered during the continuous monitoring process.

e. The level of effort applied to the assessment of security controls must be commensurate with the FIPS Publication 199 Security Categorization of the information system.

8. TASK C: STATUS REPORTING AND DOCUMENTATION

a. The objectives of this task are to:

(1) Update the SSP to reflect the most recent proposed or actual changes to the information system, as well as any identified or potential security impacts;

(2) Update the POA&M based on the activities carried out during Phase 4: Continuous Monitoring; and

(3) Report proposed or actual changes, as well as identified or potential security impacts, to the AO.

b. The information in the security status reports (typically conveyed through the updated POA&M) should be used to determine the need for security reaccreditation and to satisfy FISMA reporting requirements.

9. STEP 1: SYSTEM SECURITY PLAN UPDATE

a. The System Owner is responsible for updating the SSP based on the documented changes to the information system (including hardware, software, firmware, and the surrounding environment) and the results of the continuous monitoring process.

b. The SSP must contain up-to-date information about the information system and changes to the information system must be reflected in the SSP. While the frequency of updates is at the discretion of the System Owner, updates occur at appropriate intervals to capture significant changes to the information system, but not so frequently as to generate unnecessary paperwork.

c. The CIO, ADAS for Cyber Security, AO, System Owner, ISO, and CA will use the SSP to guide future C&A activities, when required.

d. Security control PL-3 requires the VA to revise the SSP to address system/organizational changes or problems identified during SCAs. It also requires the SSP to be updated on an ongoing basis which results in the plan always reflecting the current state of security, both actual and planned. For additional information refer to NIST SP 800-18 which provides guidance on SSP updates.

10. STEP 2: PLAN OF ACTION AND MILESTONES UPDATE

a. The System Owner is responsible for updating the POA&M based on the documented changes to the information system (including hardware, software, firmware, and surrounding environment) and the results of the continuous monitoring process.

b. The AO uses the POA&M to monitor progress in correcting deficiencies. The POA&M should:

(1) Report progress made on current, outstanding items listed in the plan;

(2) Address vulnerabilities in the information system discovered during the SIA or security control monitoring; and

(3) Describe how the System Owner intends to address those vulnerabilities (reduce, mitigate, eliminate, or accept the identified vulnerabilities).

c. The POA&M update frequency is at the discretion of the System Owner; however, the updates should occur frequently enough to capture significant changes to the information system, but not so often as to generate unnecessary paperwork. The following VA officials will also be utilizing the POA&M to guide future C&A activities:

(1) CIO;

(2) ADAS for Cyber Security;

(3) AO;

(4) System Owner ;

(5) ISO; and

(6) CA.

11. STEP 3: STATUS REPORTING

a. The System Owner is responsible for reporting on the security status of the information system. The security status report is provided to the AO and ADAS for Cyber Security.

b. Continuous monitoring activities contained in the security status report must describe and address the following:

(1) Vulnerabilities in the information system discovered during the security certification;

(2) SIA;

(3) Security control monitoring; and

(4) How the System Owner intends to address (by reducing, mitigating, eliminating, or accepting) the vulnerabilities.

c. The frequency of the security status report is at the discretion of the VA. The status reports will occur at appropriate intervals to transmit significant security-related information about the system, but not so frequently as to generate unnecessary paperwork.

d. A decision to reaccredit the information system:

(1) Is made by the AO and the ADAS for Cyber Security;

(2) Should use the security status reports to determine necessity;

(3) Should begin, as in the original accreditation, with the C&A Initiation Phase (Phase 1); and

(4) Requires the AO to notify the System Owner.

e. Depending upon the magnitude of changes to the information system and the extent of the security controls affected, the extent of the resources required for the re-accreditation may be substantially less than the original accreditation.

f. The security status report must be updated, and properly marked as SENSITIVE and handled in accordance with VA policy.

12. CONCLUSION

The C&A process is used to ensure information systems have effective security safeguards which have been implemented, or planned for, commensurate with the potential risks to the system's information. This process is applicable throughout the system life cycle of all information systems and is only one of several information technology security activities working together to ensure the security of all of VA's information systems.

APPENDIX G
SAMPLE LETTERS AND FORMS

COVER SHEET FOR SENSITIVE DOCUMENTS

Department of Veterans Affairs

SENSITIVE DOCUMENT COVER

To safeguard the attached sensitive document you must consider:

Storage:	Lock in desk, file cabinet or storage container.
Access:	Release only to persons with an official "Need to Know".
Reproduction:	Keep copies to a minimum.
Mailing:	Use two envelopes. Mark inner envelope "SENSITIVE INFORMATION".
Transmission:	Do not facsimile (FAX), Do not transmit on electric mail carts. Do hand-carry.
Destruction:	Shred

SENSITIVE INFORMATION

Department of Veterans Affairs
Washington, D.C. 20420

Office of Cyber Security, March 22, 2004

SAMPLE HEADER FOR MARKING "SENSITIVE" DOCUMENTS

VA SENSITIVE Information.

SAMPLE SECURITY CONTROL ASSESSMENT REPORT

[DATE]
Security Assessment Report

[SYSTEM NAME]
Subject: Security Certification for [SYSTEM NAME]
Purpose: This security evaluation report is to ensure that, in accordance with NIST 800-37, Guidelines for Computer Security Certification and Accreditation, a security assessment has been performed.
References:
[SYSTEM NAME] Final Risk Assessment Report, [month/year]

[SYSTEM NAME] Security Test and Evaluation Report (ST&E), [month/year]

[SYSTEM NAME] System Security Plan (SSP), [month/year]
Background: The certification determination is based on the Final Risk Assessment & ST&E Report. It has been established that the [SYSTEM NAME] complies with applicable Federal policies, regulations, and standards for information security; satisfies the documented and approved security specifications determined by the sensitivity of the [SYSTEM NAME] and the results of testing demonstrate that the installed security safeguards are adequate for the application.
Findings: The risk assessment summarizes the significant findings and presents reasonable recommendations. Overall, the criticality of the [SYSTEM NAME] to the agency mission is [high, moderate, or low], and the impact level of the system is [high, moderate, or low]. As such, the [SYSTEM NAME] system is hereby certified with the clarifications, restrictions, and conditions of certification noted below.
Recommendation: Operational implementation of [SYSTEM NAME] is recommended under the following "Conditions of Certification".
Conditions of Certification: Restrictions and recommendations for this certification regarding technical controls are summarized below and are identified as restrictions or recommended corrective actions. A detailed explanation of each finding is available in the [SYSTEM NAME] ST&E report. Restrictions and recommendations for this certification regarding management and operational controls can be found in the risk assessment. A Plan of Action and Milestones (POA&M) will be developed and approved within 30 days from the date of certification to address each finding.
The risk assessment summarizes the significant findings and presents reasonable recommendations. Based on this risk assessment and other customer-supplied documentation, the [SYSTEM NAME] is hereby certified for a period not to exceed 36 months with the clarifications, restrictions, and conditions of certification noted below.
Operational implementation of [SYSTEM NAME] is recommended under the following "Conditions of Certification".
Restrictions: [List/none]
Recommended Corrective Actions: The following actions are recommended for implementation to further reduce the risk associated with [SYSTEM NAME]:
High
[List HIGH RISK items here]

Medium
[List MEDIUM RISK items here]
Low
[List low risk items here]
Note: Any changes to the system without prior approval of the Authorizing Official will nullify this certification.
Preparer:

Certifier Name and Title	Date

SAMPLE ACCREDITATION PACKAGE TRANSMITTAL LETTER

From: Information System Owner

Date: [DATE]

Through: Senior Agency Information Security Officer

To: Authorizing Official

Subject: Security Accreditation Package for [INFORMATION SYSTEM]

A security certification of the [INFORMATION SYSTEM] and its constituent subordinate system-level components (if applicable) located at [LOCATION] has been conducted in accordance with Office of Management and Budget Circular A-130, Appendix III, Security of Federal Automated Information Resources, NIST Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, and the [AGENCY] policy on security accreditation. The attached security accreditation package contains: (i) current system security plan, (ii) security assessment report, and (iii) plan of action and milestones.

The security controls listed in the system security plan have been assessed by [CERTIFICATION AGENT] using the assessment methods and procedures described in the security assessment report 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. The plan of action and milestones describes the corrective measures that have been implemented or are planned to address any deficiencies in the security controls for the information system and to reduce or eliminate known vulnerabilities.

[Signature]
[Title]

SAMPLE ACCREDITATION DECISION LETTER (AUTHORITY TO OPERATE)

From: Authorizing Official

Date: [DATE]

Thru: Senior Agency Information Security Officer

To: Information System Owner

Subject: Security Accreditation Decision for [INFORMATION SYSTEM]

After reviewing the results of the security certification of the [INFORMATION SYSTEM] and its constituent system-level components (if applicable) located at [LOCATION] and the supporting evidence provided in the associated security accreditation package (including the current system security plan, the security assessment report, and the plan of action and milestones), I have determined that the risk to agency operations, agency assets, or individuals resulting from the operation of the information system is acceptable. Accordingly, I am issuing an authorization to operate the information system in its existing operating environment. The information system is accredited without any significant restrictions or limitations. This security accreditation is my formal declaration that adequate security controls have been implemented in the information system and that a satisfactory level of security is present in the system.

The security accreditation of the information system will remain in effect as long as: (i) the required security status reports for the system are submitted to this office every [TIME PERIOD]; (ii) the vulnerabilities reported during the continuous monitoring process do not result in additional agency-level risk which is deemed unacceptable; and (iii) the system has not exceeded the maximum allowable time period between security accreditations in accordance with federal or agency policy.

A copy of this letter with all supporting security certification and accreditation documentation should be retained in accordance with the agency's record retention schedule.

[Signature]
[Title]
Enclosures:

SAMPLE ACCREDITATION DECISION LETTER (INTERIM AUTHORITY TO OPERATE)

From: Authorizing Official

Date: [DATE]

Thru: Senior Agency Information Security Officer

To: Information System Owner

Subject: Security Accreditation Decision for [INFORMATION SYSTEM]

After reviewing the results of the security certification of the [INFORMATION SYSTEM] and its constituent system-level components (if applicable) located at [LOCATION] and the supporting evidence provided in the associated security accreditation package (including the current system security plan, the security assessment report, and the plan of action and milestones), I have determined that the risk to agency operations, agency assets, or individuals resulting from the operation of the information system is not acceptable. However, I have also determined that there is an overarching need to place the information system into operation or continue its operation due to mission necessity. Accordingly, I am issuing an interim authority to operate the information system in its existing operating environment. An interim authority is a limited authorization to operate the information system under specific terms and conditions and acknowledges greater agency-level risk for a limited period of time. The information system is not considered accredited during the period of limited authorization to operate. The terms and conditions of this limited authorization are described in Attachment A.

A process must be established immediately to monitor the effectiveness of the security controls in the information system during the period of limited authorization. Monitoring activities should focus on the specific areas of concern identified during the security certification. Significant changes in the security state of the information system during the period of limited authorization should be reported immediately.

This interim authority to operate the information system is valid for [TIME PERIOD]. The limited authorization will remain in effect during that time period as long as: (i) the required security status reports for the system are submitted to this office every [TIME PERIOD]; (ii) the vulnerabilities reported during the continuous monitoring process do not result in additional agency-level risk which is deemed unacceptable; and (iii) continued progress is being made in reducing or eliminating vulnerabilities in the information system in accordance with the plan of action and milestones. At the end of the period of limited authorization, the information system must be either authorized to operate or the authorization for further operation will be denied. Renewals or extensions to this interim authority to operate will be granted only under the most extenuating of circumstances. This office will monitor the plan of action and milestones submitted with the accreditation package during the period of limited authorization.

A copy of this letter with all supporting security certification and accreditation documentation should be retained in accordance with the agency's record retention schedule.

[Signature]
[Title]
Enclosures:

SAMPLE ACCREDITATION DECISION LETTER (DENIAL OF AUTHORIZATION TO OPERATE)

From: Authorizing Official

Date: [DATE]

Thru: Senior Agency Information Security Officer

To: Information System Owner

Subject: Security Accreditation Decision for [INFORMATION SYSTEM]

After reviewing the results of the security certification of the [INFORMATION SYSTEM] and its constituent system-level components (if applicable) located at [LOCATION] and the supporting evidence provided in the associated security accreditation package (including the current system security plan, the security assessment report, and the plan of action and milestones), I have determined that the risk to agency operations, agency assets, or individuals resulting from the operation of the information system is unacceptable. Accordingly, I am issuing a denial of authorization to operate the information system in its existing operating environment. The information system is not accredited and [MAY NOT BE PLACED INTO OPERATION or ALL CURRENT OPERATIONS MUST BE HALTED]. Failure to receive an authorization to operate the information system indicates that there are major deficiencies in the security controls in the system and that a satisfactory level of security is not present in the system at this time.

The plan of action and milestones should be revised immediately to ensure that proactive measures are taken to correct the security deficiencies in the information system. The security certification should be repeated at the earliest opportunity to determine the effectiveness of the security controls in the information system after the reduction or elimination of identified vulnerabilities.

A copy of this letter with all supporting security certification and accreditation documentation should be retained in accordance with the agency's record retention schedule.

[Signature]
[Title]
Enclosures:

SAMPLE CHANGE LOG

Record of Changes

Version	Reason for Change	Author	Approved By	Approval Date