DEPARTMENT OF VETERANS AFFAIRS
Washington, DC 20420

VA HANDBOOK 6500.5
Transmittal Sheet
March 22, 2010

INCORPORATING SECURITY AND PRIVACY INTO THE SYSTEM DEVELOPMENT LIFE CYCLE

1. REASON FOR ISSUE: This Handbook establishes the security and privacy procedures, responsibilities, and departmental framework for incorporating security and privacy in the system development life cycle (SDLC) of information technology (IT) assets that store, process, or transmit Department of Veterans Affairs (VA) information by, or on behalf of, VA as required by the E-Government Act of 2002, Public Law 107-347; to include *Title III, The Federal Information Security Management Act (FISMA)*, and VA Directive and Handbook 6500, *Information Security Program*.

2. SUMMARY OF CONTENTS/MAJOR CHANGES: This Handbook establishes VA policy, responsibilities and processes for incorporating security and privacy in the system development life cycle of VA IT assets that store, process or transmit VA information by, or on behalf of VA.

3. RESPONSIBLE OFFICE: The Office of the Assistant Secretary for Information and Technology (OI&T) (005), Information Protection and Risk Management (IPRM) (005R) is responsible for the content contained in this Handbook.

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

5. RESCISSIONS: None.

CERTIFIED BY:

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

BY DIRECTION OF THE SECRETARY VETERANS AFFAIRS:

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

Distribution: Electronic Only

INCORPORATING SECURITY AND PRIVACY INTO THE SYSTEM DEVELOPMENT LIFE CYCLE

CONTENTS

PARAGRAPH **PAGE**

1. PURPOSE **5**

2. RESPONSIBILITIES **5**

a. Secretary of Veterans Affairs 5
b. VA Chief Information Officer 5
c. Deputy CIO for Office of Enterprise Development 5
d. Deputy CIO for Enterprise Operations and Field Development 6
e. Executive Director for Quality, Performance and Oversight 6
f. Deputy Assistant Secretary for Information Protection and Risk Management 6
g. Associate Deputy Assistant Secretary of Cyber Security 6
h. Deputy Associate Deputy Assistant Secretary for Privacy and Records Management .. 7
i. Director, Business Continuity 7
j. Office of Inspector General (OIG) 7
k. Office of General Counsel (OGC) 8
l. Deputy Assistant Secretary of Acquisition and Logistics 8
m. Authorizing Official 8
n. Under Secretaries, Assistant Secretaries, and Other Key Officials 8
o. Department Information Owners 9
p. Program and Facility Directors 9
q. Information Security Officers 9
r. Local Chief Information Officers and System Administrators/Network Administrators . 10

3. THE FRAMEWORK **10**

a. Introduction to the Framework 10
b. Initiation Phase 13
c. Acquisition and Development Phase 14
d. Implementation and Assessment Phase 14
e. Operations and Maintenance Phase 14
f. Disposal Phase 15

4. IMPLEMENTATION ACROSS THE FRAMEWORK **15**

a. Initiation Phase 17
b. Acquisition and Development Phase 19
c. Implementation and Assessment Phase 29
d. Operations and Maintenance Phase 30
e. Disposal Phase 32

CONTENTS (cont.)

PARAGRAPH **PAGE**

5. SUMMARY 33

7. REFERENCES 37

APPENDICES **PAGE**

A. Definitions A-1

B. Abbreviations/Acronyms Used in Handbook and Appendices B-1

FIGURES **PAGE**

1. Diagram of the SDLC Framework 12

2. Risk Assessment Process 20

TABLES **PAGE**

1. Key Processes of the SDLC 16

2. SDLC Framework Summary 35

INCORPORATING SECURITY AND PRIVACY INTO THE SYSTEM DEVELOPMENT LIFE CYCLE

1. PURPOSE

a. 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 establishes the security and privacy procedures, responsibilities, and departmental framework for incorporating security and privacy in the system development life cycle (SDLC) of information technology (IT) assets that store, process, or transmit Department of Veterans Affairs (VA) information by, or on behalf of, VA as required by the E-Government Act of 2002, Public Law 107-347; to include *Title III, The Federal Information Security Management Act (FISMA)*, and VA Directive and Handbook 6500, *Information Security Program*.

c. This handbook is dependent upon the security requirements established in VA Handbook 6500 and other handbooks in the 6500.x series. (see Reference section for a list)

2. RESPONSIBILITIES

a. **Secretary of Veterans Affairs** has designated the Chief Information Officer (CIO) as the senior agency official responsible for ensuring enforcement and compliance with the requirements imposed on VA under FISMA.

b. **VA CIO** is responsible for:

(1) Establishing, maintaining and monitoring Department-wide information security policies, procedures, control techniques, training and inspection requirements as elements of the VA information security program;

(2) Issuing policies and Handbooks to provide direction for implementing the elements of the information security program to all Department organizations; and

(3) Approving all IT policies and procedures that are related to VA information.

c. **Deputy CIO for Office of Enterprise Development** is responsible for:

(1) Incorporating the security and privacy principles and requirements outlined in this Handbook into the system development processes (initiation, acquisition and development phases) of the organization; and

(2) Ensuring adherence to this policy by VA employees, contractor personnel and other non-Government employees under the Enterprise Development area of responsibility.

d. **Deputy CIO for Enterprise Operations and Field Development** is responsible for:

(1) Incorporating the security and privacy principles and requirements outlined in this Handbook into the systems implementation and assessment, operations and maintenance, and disposal phases for systems managed by the organization; and

(2) Ensuring adherence to this policy by VA employees, contractor personnel and other non-Government employees under the Enterprise Operations and Field Development area or responsibility.

e. **Executive Director for Quality, Performance and Oversight** is responsible for ensuring security throughout the lifecycle of systems by checking for compliance of the security requirements outlined in this Handbook during the Information Technology Oversight Compliance (ITOC) reviews conducted by ITOC staff throughout the year.

f. **Deputy Assistant Secretary for Information Protection and Risk Management (IPRM)** has been designated by the VA CIO, under the provisions of FISMA, to be the VA Chief Information Security Officer (CISO) and is responsible for establishing and directing the VA information security program.

g. **Associate Deputy Assistant Secretary of Cyber Security** has been designated by the CIO to be the VA Deputy CISO and is responsible for operationalizing the responsibilities delegated to the Deputy Assistant Secretary for IPRM. These responsibilities include:

(1) Establishing, maintaining, and monitoring Department-wide information security policies, procedures, control techniques, training, and inspection requirements as elements of the information security program;

(2) Issuing policies and Handbooks to provide direction for implementing elements of the information security program to all Department organizations;

(3) Approving all policies and procedures related to information security for those areas of responsibility that are currently under the management and the oversight of other Department organizations;

(4) Ordering and enforcing Department-wide compliance with, and execution of, any information security policy; and

(5) Establishing minimum mandatory technical, operational, and management information security control requirements for each Department system, consistent with risk, the processes identified in standards of the National Institute of Standards and Technology (NIST), and the responsibilities of the Assistant Secretary to operate and maintain all Department systems currently creating, processing, collecting, or disseminating data on behalf of Department information owners.

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

(1) Providing guidance and procedures for protecting personally identifiable information (PII) as required by the Privacy Act of 1974;

(2) Providing oversight and guidance in order to ensure VA compliance with applicable privacy laws, regulations and policies;

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

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

(5) Coordinating and assisting Privacy Officers (POs) with privacy-related issues.

i. **Director, Business Continuity** is responsible for:

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

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

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

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

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

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

j. **Office of Inspector General (OIG)** is responsible for conducting regular reviews of the security program to ensure that all Federal and VA security and privacy requirements are being met.

k. **Office of General Counsel (OGC)** is responsible for ensuring legal applications and appropriateness of the policies and procedures set forth in this Handbook are sufficient and for settling any questions of law around the issue of VA compliance with legal and regulatory requirements for matters surrounding the SDLC.

l. **Deputy Assistant Secretary of Acquisition and Logistics** is responsible for:

(1) Providing acquisition guidance and procedures to VA contracting officers (COs) and contracting officer's technical representatives (COTRs) to facilitate implementation of VA's information security program for information systems implemented within the Department;

(2) Providing VA guidance to ensure that security requirements and security specifications are explicitly included in information systems and information system support service acquisition contracts;

(3) Providing VA guidance to ensure that contracts contain the language necessary for compliance with FISMA and 38 U.S.C. 5721-28 and provide adequate security for information and information systems used by the contractor; and

(4) Ensuring that COs consult with appropriate ISOs as needed.

m. **Authorizing Official (AO)** for VA is the VA CIO. The AO is authorized to assume the responsibility and accountability for operating an information system at an acceptable level of risk. The AO is involved with Security Assessment and Authorization/Certification and Accreditation (C&A) of VA systems and is responsible for:

(1) Authorizing operation of an information system;

(2) Issuing an interim authorization to operate (IATO) for an information system under certain terms and conditions; and

(3) Denying authorization to operate the information system, or if the system is already operational, halt operations after consulting with the system owner if unacceptable security risks exist.

n. **Under Secretaries, Assistant Secretaries, and Other Key Officials are responsible for:**

(1) Assisting OI&T in the implementation and compliance with security and privacy requirements within their area of responsibilities.

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

(3) **Department Information Owners**, in accordance with the criteria of the Centralized IT Management System, are responsible for the following:

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

(b) Determining who has access to the system or systems containing sensitive personal information, including types of privileges and access rights;

(c) Assisting the Assistant Secretary for IT in the identification and assessment of the common security controls for systems where their information resides; and

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

o. **Program and Facility Directors** are responsible for providing the necessary support to the information security and privacy programs in their organizations to ensure the facility meets all the information security and privacy requirements mandated by Executive and VA policy and other Federal law (e.g., Health Insurance Portability and Accountability Act (HIPAA), FISMA, Privacy Act).

p. **ISOs** are the agency officials assigned responsibility by OI&T Field Operations and Security to ensure that the appropriate operational security posture is maintained for an information system or program. VA ISOs are responsible for:

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

(1) Managing their local information security programs and serving as the principal security advisor to system owners regarding security considerations in applications, systems, procurement or development, implementation, operation and maintenance, disposal activities (e.g., life cycle management);

(2) When assigned to a system development project, will coordinate the security functions as outlined in this Handbook.

(3) Assisting in the determination of an appropriate level of security commensurate with the impact level;

(4) Coordinating, advising, and participating in the development and maintenance of information system security plans (SSPs) and contingency plans for all systems under their responsibility;

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

(1) Verifying and validating, in conjunction with the system owners and managers, that appropriate security measures are implemented and functioning as intended;

(2) Working with the system owner and manager, repeating a selected subset of security control assessment (SCA) test procedures, as it pertains to the information systems at the site, to ensure that controls remain in place, are operating correctly and producing the desired results. Controls most apt to change over time must be included and these tests and results must be documented to support the continuous monitoring program;

(3) Participating in security self-assessments, external and internal audits of system safeguards and program elements, and in Security Assessment and Authorization/C&A of the systems supporting the offices and facility under their areas of responsibility;

(4) Assisting other VA officials with significant IT responsibilities (e.g., local CIOs, system managers, contracting staff, human resources staff, police) in remediating and updating POA&Ms identified during the Security Assessment and Authorization/C&A process, periodic compliance validation reviews and the FISMA annual assessment reports;

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

(6) Working with facility PO to assure information security and privacy policies complement and support each other.

q. **Local CIOs, System Administrators and Network Administrators** are responsible for day-to-day operations of the systems. The role of a system administrator must include security of Local Area Network (LAN) or application administration and account administration.

3. THE FRAMEWORK

a. Introduction to the Framework

(1) The SDLC, as developed in NIST Special Publication (SP) 800-series documents, is a multi-step process specifically focused on implementation of security protections across the life cycle of information systems.

(2) NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, security control SA-3 Life Cycle Support requires VA to manage information systems using an SDLC methodology that includes information security considerations. (See VA Handbook 6500, *Information Security Program, Appendix D* for more information.)

(3) NIST SP 800-53, security control PL-1 Security Planning Policy and Procedures, requires VA to develop and document a formal security planning policy and procedures for implementation of the security controls.

(4) NIST SP 800-53, security controls SA-8 Security Engineering Principles, requires VA to design and implement the information system using security engineering principles that are documented in NIST SP 800-27, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*.

(5) There are five phases in the SDLC as follows (see Figure 1 for a diagram of the SDLC framework):

(a) Initiation phase;

(b) Acquisition and Development phase;

(c) Implementation and Assessment phase;

(d) Operations and Maintenance phase; and

(e) Disposal phase.

(6) When security protections are implemented across the SDLC, security and privacy protection becomes more consistent, more effective, more useful, and more cost efficient.

Figure 1: Diagram of the SDLC Framework

Figure 1: Diagram of the SDLC Framework is a diagram of the System Development Life Cycle (SDLC) that illustrates how the five phases of the SDLC work together.

Phase 1 – Initiation
Phase 2 - Acquisition and Development
Phase 3 - Implementation and Assessment
Phase 4 - Operations and Maintenance
Phase 5 - Disposal

(7) The SDLC is a map of a series of overlapping continual processes. Once an information system is operational, many processes will be running simultaneously across all phases of the SDLC. For the sake of simplicity, the language of this document presents the SDLC map in a linear sequence of processes, but this key concept of simultaneous process flow must not be ignored.

(8) The PM family of security controls is considered to be foundational to the information security program and should be implemented as early as possible in the SDLC. Several other security controls that must get early attention include: PL-1 Security Planning Policy and Procedures, SA-3 Life Cycle Support, and SA-8 Security Engineering Principles.

a. **Initiation Phase**

(1) The Initiation phase begins by defining the need and purpose for the information system and then continues by documenting what has been defined. It is important to involve key stakeholders and business partners in this early stage. General requirements for the information system are established, creating the foundation for security protections. "System Characterization" begins this phase by describing the information system in depth. This description includes conceptual factors such as mission and function as well as an inventory of hardware and software components. It should include interfaces with other systems that will be used to define boundaries and interconnections.

(2) Once the system has been described, both the system itself and the information the system will host must be categorized according to the Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*. FIPS 199 calls for the assignment of impact levels to designate the potential for organizational disruption if the confidentiality, integrity or availability (CIA) of the system, or its data, is compromised. The impact levels of low, moderate, or high will also determine the baseline of security controls that are selected from the catalog of controls in NIST SP 800-53.

(3) Two more steps close this phase out:

(a) Beginning to outline the risk assessment process through a Business Impact Analysis (BIA) and a PIA; and

(b) Collecting key information (this will become an ongoing process throughout all the other phases).

(c) **Acquisition and Development Phase**

The second phase of the SDLC is concerned with defining security protection requirements for the information system and collecting those requirements into documentation that will become the SSP. This is where the risk assessment takes place in order to assess threats and vulnerabilities and to analyze the risks to which the system is exposed. The risk assessment first defines the security requirements of the system and then security controls are assigned to mitigate risk by protecting the system. The documentation of what has been done up to this point is assembled into the SSP which may include, but is not limited to, the following components:

(1) Contingency Plan;

(2) PIA;

(3) Risk assessment;

(4) Configuration management; and

(5) Incident Response Plan.

b. **Implementation and Assessment Phase**

This phase is comprised of two main steps. The first step is the full implementation of the security controls defined in the last phase and documentation of the configuration settings needed to make the controls function in a configuration baseline. As the implementation process moves along, the controls must be tested. The second step of this phase is the authorization process known as Security Assessment and Authorization/C&A. Authorization is a thorough inspection process of the entire SDLC that offers a credible statement of security protection. It produces a Security Assessment Report (SAR) that must be added to the documentation collection. The phase closes by updating existing documentation with any changes.

c. **Operations and Maintenance Phase**

(1) This phase involves continuous monitoring and a portion of the continuing configuration management process known as change control.

(2) Continuous monitoring is the monitoring of all aspects of the information system and its protection. This includes:

(a) Network monitoring;

(b) Patch management; and

(c) POA&Ms.

(d) A change control process is set up to handle any configuration changes that are proposed or detected during the continuous monitoring. Changes detected, or responses needed, may require updating the documentation.

d. **Disposal Phase**

Without properly completing the SDLC, all security protections put into place thus far may be wasted. This phase outlines how to preserve information, sanitize media, and dispose of hardware and software safely. Documentation updates in this phase concentrate on inventory, asset management, and privacy but may include other areas.

4. IMPLEMENTATION ACROSS THE FRAMEWORK

The following section provides details and sequences of security processes in each phase of the SDLC. While most of the process of implementing security controls is found in the Implementation and Assessment phase of the SDLC, smaller parts of the overall implementation process are dispersed across the framework. It is a key point of this section to demonstrate that most security processes don't have a discrete beginning or end point and should be considered as dynamic, continuous processes that are interdependent with each other. The following table illustrates the key processes in the SDLC and the phases in which they are most noticeable.

Table 1: Key Processes of the SDLC

Phase	Process	Applicable VA Directive and/or Handbook (See Reference Section for Full Title)
INITIATION	• Characterize the system • Impact Assessments (BIA, PIA)	• VA Handbook 6500 • VA Handbook, 6500.8 • VA Directive 6508
ACQUISITION AND DEVELOPMENT	• Risk Assessment • Security Control Implementation • Configuration Settings • Security Plan	• VA Handbook 6500 • VA Directive 6004 • VA Handbook 6500.6
IMPLEMENTATION AND ASSESSMENT	• Configuration Baseline • Testing • Security Assessment and Authorization/C&A	• VA Handbook 6500 • VA Directive 6004 • VA Handbook 6500.3
OPERATIONS AND MAINTENANCE	• Continuous Monitoring • Configuration Control	• VA Handbook 6500 • VA Directive 6004 • VA Handbook 6500.2
DISPOSAL	• Media Sanitization	• VA Handbook 6500 • VA Handbook 6500.1

Table 1: Key Processes of the SDLC illustrates the key processes in the SDLC and the phases where they are most evident. It also references VA Directives and/or Handbooks that are applicable to each phase.

a. **Initiation Phase**

(1) Characterization of the system takes place in the Initiation phase and begins by describing the information system.

(2) The system description defines the scope of the information system and in doing so, also sets the scope for risk assessment and the implementation of protective controls that will later be established. It must include the mission and purpose of the information system as well as the architectural design and requirements that have been established. These will be used Security Assessment and Authorization/C&A, and Interconnection Security Agreement (ISA) [see security control CA-3 Information System Connections]. System description continues with a component inventory [see security controls PE-16 Delivery and Removal and CM-8 Information System Component Inventory]. When the description process is complete it should include, but is not limited to, the following categories of information:

(a) System mission and purpose;

(b) System functional requirements;

(c) Organizational policy;

(d) System design architecture;

(e) Network topology;

(f) Boundary definition;

(g) Information flows;

(h) Security controls (both planned and already in place);

(i) Physical and environmental security mechanisms; and

(j) Inventory, which includes the following:

1. Hardware;

2. Software;

3. Interfaces to other systems (connecting two systems together may require an ISA to be created (CA-3). The process of considering security across the connection should include an evaluation of privacy concerns and if an ISA is needed, a formal written statement of privacy requirements should be part of the ISA.); and

4. Data and people.

5. With the system description complete, the next step is System Categorization according to FIPS Publication 199, which requires an impact level to be designated as low, moderate, or high [see security control RA-2 SECURITY CATEGORIZATION]. These levels are determined by examining three security objectives: confidentiality, integrity, and availability. Privacy issues must be considered as part of the determination of confidentiality impact. Establishing the categorization level completes the process of System Characterization.

(3) Once the categorization level has been established, a baseline of security controls is automatically selected from the catalog of controls as found in NIST SP 800-53 which will be used as a foundation for protection in the next phase. The high-impact baseline contains the greatest number of controls and enhancements. The moderate- and low-impact baselines each contain fewer controls and enhancements than the next highest level.

(4) With the system characterization complete and the categorization level selected, contingency planning and impact assessments addressing the following areas must be completed [see security control CP-2 CONTINGENCY PLAN]:

(a) BIA, analyzing how business is impacted, including the following:

1. Identifying critical resources;

2. Identifying disruption impacts and critical timeframes; and

3. Setting recovery priorities.

(b) PIA, analyzing how privacy information is handled [see security control PL-5 PRIVACY IMPACT ASSESSMENT]:

1. Handling must conform to legal, regulatory and policy requirements;

2. Determining the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system;

3. Examining and evaluating protections and alternative processes for handling information to mitigate potential privacy risks; and

4. Adhering to Office of Management and Budget (OMB) Memorandum 03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, which provides guidance for implementing the privacy provisions of the E-Government Act of 2002 as follows:

a. The primary function of the PIA is to determine if a new collection of information qualifies as a system of records under the Privacy Act. When the PIA determines that a new system of records is covered under the Privacy Act, the following actions are required:

(1) OMB approval prior to collecting the information;

(2) Public comments must be collected concerning the proposed collection; and

(3) Inclusion of an Information Collection Request that explains the collection in detail.

b. A list of conditions that may require a PIA to be performed or updated. The PIA, like a risk assessment or SSP, should be considered a dynamic, living document that always represents the current state of privacy in the information system.

c. Privacy Protection on Websites

d. If the PIA determines that a system of records covered under the Privacy Act is being created, a System of Records Notice (SORN) must be published.

(a) Key information generated in this phase must be collected and saved to form the beginning of the System Security Plan and other security and privacy-related documents. This includes data from both the system characterization process and the contingency planning process. All subsequent phases will build upon, and constantly update, this documentation [see security control PL-2 SYSTEM SECURITY PLAN].

b. **Acquisition and Development Phase**

This phase involves risk management, which is defined as the process of assessing risk, establishing security controls that mitigate damage from risk, as well as evaluating and assessing the degree to which the controls are functioning as intended. This begins with a preliminary assessment of risk (BIA and PIA) in the Initiation phase, and then continues with the full risk assessment in the Acquisition and Development phase. Risk mitigation is primarily concerned with selecting, tailoring, and implementing security controls as protection against perceived risk, but mitigation can continue throughout other phases, particularly with processes such as continuous monitoring and POA&Ms. The core of the risk management process closes out with the evaluation and assessment of security controls. Risk can be calculated by estimating the likelihood that a threat source will exercise vulnerability and the impact of that incident upon the organization. See figure 2 below for the risk assessment process.

Figure 2: Risk Assessment Process

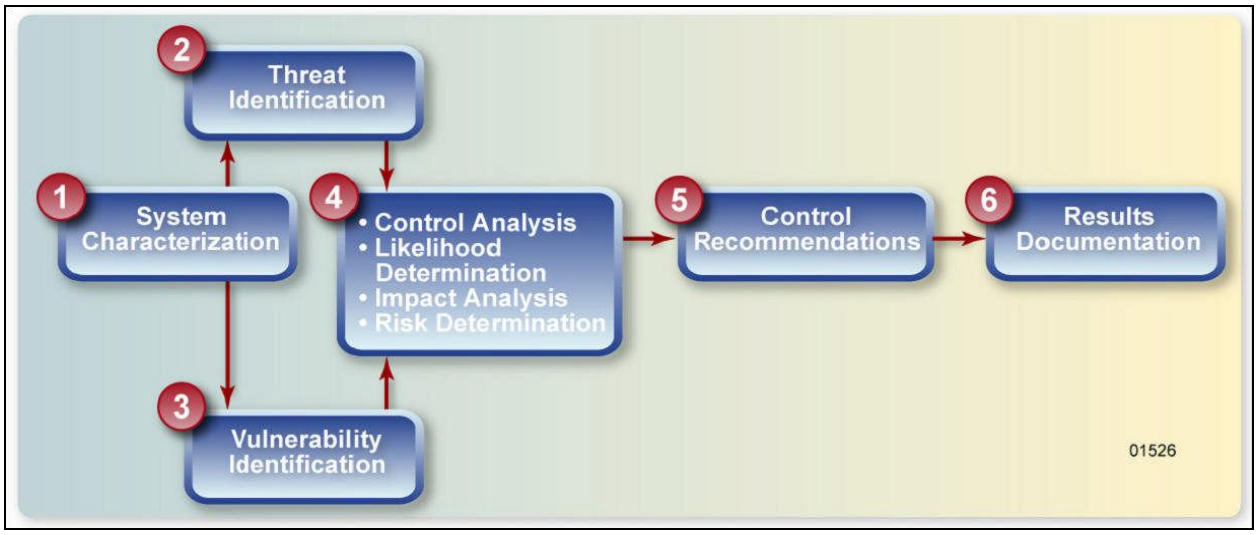

Figure 2: The above flow chart outlines the risk assessment process which includes:

(1) System Characterization
(2) Threat Identification
(3) Vulnerability Identification (concurrent with Step 2)
(4) Control Analysis
Likelihood Determination
Impact Analysis
Risk Determination
(5) Control Recommendations
(6) Results Documentation

(1) Risk assessment includes the following steps (system characterization should have been completed in the initiation phase):

(a) Threat Identification: Consists of identifying threat sources that could potentially exploit weaknesses in the system. This process must consider threat sources and whether those sources are human. In addition, it must also consider the motivation and the possible range of actions based on that motivation. Environmental threats are non-natural threats that can occur in the operational environment of an information system. Power failures due to problems with power supply infrastructure, problems with building infrastructure, malfunctions of various kinds, and more can be examples of this classification of threats. Natural threats include storms, earthquakes, landslides, extreme temperature, and other (mostly weather related) examples. Storms can include floods, tornadoes, hurricanes, electrical storms, winter storms, and more. Human threats include unintentional threats (mostly due to some kind of error) and intentional threats. Intentional threats include hackers, crackers, criminals, terrorists, industrial espionage agents, insiders, and possibly others. Threat motivations that are emotional include ego, challenge, control, revenge, and greed. Threat motivations can also include gain of financial, business, political, or national security advantages. Threat actions come from a fairly small list of categories and many source and motivation pairs may have actions in common, but there are also important differences requiring case-by-case analysis. Common threat actions include system intrusion, defacement, data compromise, bribery, extortion, system disruption, organizational disruption, and many variations of the aforementioned. Threat analysis must be tailored to the specific organization, the environment in which it operates the mission of the information system, and the criticality and sensitivity of its data.

(b) Vulnerability Identification: A vulnerability is a flaw or weakness in system security procedures, design, implementation, or internal controls that can be exercised (accidentally triggered or intentionally exploited) and results in a security or privacy breach or a violation of the system's security and privacy policies. The goal of this step is to produce a list of vulnerabilities that match up with the list of threats and, therefore, represent a point of potential exploitation of the information system or the data found thereon. The type of vulnerabilities that should be considered may vary with both the nature of the information system, the data that the information system will hold, and the phase of the SDLC that it is currently in. The process of identifying vulnerabilities for a system that is being designed may differ considerably from the same process for a system that is fully operational. Vulnerability information may be collected both from lists and by performing security testing. Vulnerability lists and security advisories, both national and vendor-issued, should be reviewed. These include the NIST National Vulnerability Database, US-CERT, SysAdmin, Audit, Network, Security (SANS) Top 20 List, SANS Internet Storm Center, and the Google list of computer security advisories and patches [see security controls RA-5 VULNERABILITY SCANNING and SI-2 FLAW REMEDIATION].

1. System Security Testing is the first step which includes the following activities:

a. Vulnerability scanning;

b. Penetration testing;

c. SCA; and

d. Previous risk assessments and test results.

2. Security Requirements Checklist: Once the vulnerability information has been collected and paired with threats, a security requirements checklist should be assembled. This checklist contains the basic security standards used to systematically evaluate and identify the vulnerabilities associated with the information system. NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, should be used a primary resource.

(c) Risk Analysis: The process of assigning an estimated risk status to the information system and the information that it will hold, based on the information collected and the analysis performed in the preceding steps. Threats and their accompanying motivation and capability levels have been matched up against vulnerabilities. Subsequently these pairs are balanced against protective controls to determine the likelihood of potential exploitation. Privacy is a key issue here and any risk area that includes a possible loss of confidentiality should be examined for privacy concerns. The following steps are used for risk analysis:

1. Control Analysis (using the Security Requirements checklist from above); and

2. Likelihood Determination (low, moderate, or high), which involves the following:

a. Threat source motivation and capability;

b. Nature of vulnerability; and

c. Effectiveness of security controls.

3. Impact Analysis: Impact levels are generally rated as low, moderate, or high, but may also include quantitative or qualitative analysis. The criticality and sensitivity of a system's mission, the data found thereon, related privacy issues, and the sensitivity of the assets and data must also be considered.

4. Risk Determination: The likelihood of a threat being exercised, in combination with the analysis of the impact it may have on the system or the data that it holds, produces a determination of risk.

(d) Control Recommendations: The goal in recommending controls is to reduce the level of risk to the information system and data to a level the organization can accept. This step helps to identify and select controls that will mitigate the risks identified in previous steps. These recommendations are essential for the risk mitigation process, which involves implementing the security controls to create protection.

1. The following factors should be considered in recommending controls:

a. Effectiveness of recommendations;

b. Laws and regulations;

c. Organizational policy;

d. Impact; and

e. Safety and reliability.

2. NIST SP 800-53 contains the catalogue of security controls and may be consulted for further guidance in this area.

(e) Results Documentation: Once all steps in the risk assessment process are completed, a risk assessment report is written to describe the risk posture of the system and submitted to the system owner for review. This must be done within the framework of the standard operational environment, as described during system characterization. The purpose of the risk assessment report is to provide sufficient information to make sound, risk based decisions. This report is considered to be part of the SSP and should contain the following:

1. Scope of the assessment based on the system characterization;

2. Methodology used to conduct the risk assessment;

3. Individual observations resulting from conducting the risk assessment; and

4. Estimation of the overall risk posture of the system.

(f) Risk Mitigation: Once the risk level has been assigned and control recommendations have been made, the effort of mitigating risk begins. This involves the following steps:

1. Preparation:

a. Prioritizing: In allocating resources, top priority should be given to the vulnerability/threat pairs that were assessed as having the highest risk value. These high risk items may require immediate action to protect the system and its mission;

b. Evaluating control options: Different control options may involve different levels of effort (LOE) and cost factors. Feasibility and effectiveness must be analyzed in order to select the most appropriate controls; and

c. Cost benefit analysis: This should describe the costs and benefits of implementing versus not implementing security controls.

2. Selection of security controls involves the following:

a. Baseline control set (selected automatically by security categorization);

b. Tailoring existing controls: Terms and conditions for tailoring the security control baseline are set forth in NIST SP 800-53. Tailoring activities include scoping guidance,

compensating controls, and organizationally defined parameters. All such tailoring activities must be documented in the SSP. Any control tailoring activities related to privacy must be documented in the PIA; and

c. Scoping guidance is offered from NIST SP 800-53 for considerations on the applicability and implementation of individual security controls and can impact how the controls are applied. Scoping guidance covers the following areas:

(1) Common Controls are controls that protect more than one information system and are often part of the organization-wide infrastructure. System-specific controls are those controls that protect an individual information system and are often part of a local operating unit or application. ALL controls MUST be designated as either a common control or assigned to a specific system. Common controls typically exhibit some of the following characteristics:

(a) Serve the organization as a whole;

(b) Are typically deployed as part of the infrastructure;

(c) Information systems within the infrastructure inherit their protection;

(d) Can be hybrid (part common and part system specific);

(e) Can be supplemented by local system owners;

(f) Must have responsibility assigned;

(g) Are candidates for continuous monitoring;

(h) Results must be shared;

(i) Improve cost savings and security consistency.

(2) Policy and Regulatory: Privacy concerns generated in the PIA need to be incorporated into the security controls. The Federal Enterprise Architecture Security and Privacy Profile defines 17 privacy control families. These control families provide a common terminology and framework for privacy controls in a manner similar to the 17 security control families defined in NIST SP 800-53. These control areas are common across most privacy laws and provide a framework for organizing and addressing privacy requirements and capabilities. OMB 03-022 requires a PIA to describe how privacy-related information will be secured. Privacy controls must ensure that:

(a) Individuals have the ability to gain access to any information records pertaining to them;

(b) Individuals have the ability to review, request, and obtain copies of the record;

(c) The VA will accept requests to amend records within 10 days;

(d) The VA will inform the individual of any refusal to amend the record;

(e) A procedure is established for the individual to request a review of the refusal and file a statement setting forth the reasons for their disagreement;

(f) A procedure is established to serve notice to an individual when their information is made available to another person under a legal process;

(g) A disposition schedule and methods for disposition have been established;

(h) Individuals are protected against adverse action as the result of record matching. This is required by the Computer Matching and Privacy Protection Act of 1988 which amended the Privacy Act; and

(i) Any contract for the operation of a system of records by or on behalf of VA to accomplish an agency function will ensure that the provisions of this section are applied to such system.

(3) Scalability; and

(4) Security Objectives.

d. Compensating Controls: Compensating controls can be used in place of a baseline control, but are restricted to the following conditions:

(1) It is selected from NIST SP 800-53 or a suitable control is adopted;

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

(3) The risk of using the control is assessed and accepted and the use of the compensating control is documented in the SSP and the AO or their designated representative (AODR) approves it.

e. Organizationally defined parameters give flexibility by allowing for the fine-tuning of parts of specific controls in order to meet organizational requirements. The values selected should adhere to the suggested maximum and minimum values unless more restrictive values are needed. The parameters must be documented in the SSP and privacy-related parameters documented in the PIA.

3. Supplementing controls: In addition to the tailoring and scoping activities outlined above, NIST SP 800-53 allows for supplementing the baseline with additional controls or enhancements that may be needed to mitigate risk. It is also possible to add restrictions to existing controls. Determining which controls will provide adequate protection is a balance of: risk assessment, establishing the requirements to mitigate risks, and the need for additional controls or enhancements that may be needed to mitigate risks. When additional controls are required the following process should be followed:

a. Use existing baseline controls and enhancements first;

b. Restrictions can be added to existing controls; and

c. It is important to thoroughly document the process of adding supplemental controls.

4. Assigning responsibility: Persons with the appropriate skills and expertise to implement the controls must be assigned to each control.

5. Documentation of security requirements of the information system and the associated data found thereon, and the controls that meet those requirements form the core of the SSP. The SSP also describes the rationale for security categorization, tailoring, and supplementation activities, how individual controls are implemented within specific operational environments, and any use restrictions to be enforced on information systems due to high-risk situations. It provides a description of the risk mitigations that are deemed necessary reflecting the information system trustworthiness required to help ensure mission and business success. The SSP is important because it documents the decisions taken during the security control selection process and the rationale for those decisions. Complete coverage of security controls in the SSP facilitates more comprehensive information security, promotes increased accountability, provides an effective vehicle to better manage the risks resulting from the operation and use of information systems, and is required to adequately support the security certification of systems as part of the accreditation process.

6. Implementation of security controls during the development phase should be considered carefully and planned logically. The controls are turned on and both the controls and the system should be tested to confirm that they are operating as planned in this development stage. Once the controls are in the system and the system is operational and has been tested, the system will then need to be fully integrated into the operating environment and that step comes at the beginning of the next phase. Implementation of controls into the system during development involves the following steps:

a. Identified vulnerability and threat pairs and their associated risk levels;

b. Recommended controls;

c. Prioritized actions;

d. Planned security controls;

e. Resources required for implementation of controls;

f. Staff responsible for implementing controls;

g. Implementation start date;

h. Targeted completion date;

i. Any maintenance requirements; and

j. Implementation of the controls.

7. System Security Control Testing: After security controls have been implemented, they should be assessed for effectiveness using NIST SP 800-53A as a guide. Assessing, evaluating, and testing security controls is another process that winds its way throughout the entire SDLC. Assessing the effectiveness of security controls is found in implementation testing (including risk assessment), integration testing, in the Security Assessment and Authorization/C&A, and in continuous monitoring. To ensure effective security controls, this should be a dynamic and ongoing process. While some testing of controls should be performed during implementation, testing and evaluation during the complete integration of the system into the operating environment is also necessary in order to understand the collective effectiveness of controls. The assessment should be designed to produce a compilation of evidence showing the controls are working as designed to protect the information system and the data it holds, and that the information system, in fact, is delivering the required level of trustworthiness. This process is continuous and parts of it are found in implementation testing (referenced above), in integration testing, Security Assessment and Authorization/C&A, and continuous monitoring.

8. Configuration Management: Once adequate security controls have been selected, adapted, implemented, and assessed configuration settings must be recorded [see security control CM-6 Configuration Settings]. The overall configuration management process begins early in the SDLC with inventory, continues with recording configuration settings and establishing a configuration baseline, and then moves into change control and continuous monitoring. Any configuration settings that are related to privacy issues should be recorded in the PIA. Here is a brief outline of the configuration management process:

a. Inventory;

b. Configuration settings;

c. Configuration baseline;

d. Change control (and protecting configuration information);

e. Continuous monitoring; and

f. Asset management and inventory (at the point of disposal).

(g) Security Control Documentation and SSP

1. Once the configuration settings and the configuration baseline have been documented, all of the documentation pieces necessary for the SSP should be in place. The SSP should provide an overview of the security and privacy requirements for both the information and the information system (and supporting infrastructure within an organization) and should describe the security controls in place, or planned, for meeting those requirements. The SSP should also describe the rationale for security categorization, tailoring, and supplementation activities, how individual controls are implemented within specific operational environments, and any use restrictions to be enforced on the information system due to high-risk situations. Once completed, the SSP will provide a description of the risk mitigations that are deemed necessary reflecting the information system trustworthiness required to help ensure mission and business success [see security control PL-2 System Security Plan].

2. The system characterization performed early in the SDLC supplies the boundary analysis and FIPS 199 impact categorization necessary for the subsequent steps. Selection of a baseline of security controls is provided by the impact category. Tailoring of the baseline to system-specific conditions further refines the controls. Common controls must be identified during the tailoring process before the SSP is assembled. It is important that common controls and the non-system specific portions of hybrid controls are documented in either the SSP or an equivalent document similar to the plan created for individual information systems. All of these security plans must assign responsibility for the development, implementation, and assessment of the agreed upon security controls.

3. Other supporting pieces which may be incorporated into the SSP, or attached as separate documents, include but are not limited to:

a. Risk assessment;

b. Configuration management;

c. ISA;

d. Contingency planning;

e. Awareness and training;

f. Incident response planning;

g. PIA;

h. VA National Rules of Behavior (ROB);

i. Security Assessment and Authorization/C&A components; and

j. POA&M.

c. **Implementation and Assessment Phase**

In this phase, after the information system has been delivered, installed and accepted, all security controls are fully integrated into the information system and it's environment, configuration settings are recorded, the controls are tested and the authorization process (Security Assessment and Authorization/C&A) takes place. For further details regarding the Security Assessment and Authorization/C&A process please reference VA Handbook 6500.3, *Certification and Accreditation of VA Information Systems*.

(1) All security controls that were implemented as called for in the risk assessment and risk mitigation processes in the previous development phase must now be fully integrated into both the information system and the operational environment that it has been deployed into.

(2) Configuration settings for the controls must be recorded [see security control CM-2 Baseline Configuration].

(3) Security controls must be tested once they are in operation.

(4) Security Assessment and Authorization/C&A (now known as the authorization process) contains four parts:

(a) Preparation: The preparation portion of the Security Assessment and Authorization/C&A process involves the following steps previously described in the SDLC framework:

1. Characterize the system;

2. Select security controls;

3. Implement security controls; and

4. Assess security controls [see security control CA-2 Security Assessments].

(b) Assessment: The sub-steps involved in the assessment portion of Security Assessment and Authorization/C&A include:

1. Assessor selection;

2. Assessment plan;

3. SCA: As the security controls are assessed, privacy concerns must also be considered;

4. SAR;

5. Remediation;

6. SSP update; and

7. POA&Ms [see security control CA-5 Plans Of Action And Milestones].

(c) Authorization [see security control CA-6 Security Authorization]:

1. Prepare the authorization package;

2. Determine the risk in the system;

3. Decide whether or not to accept the risk in the system; and

4. Document the decision.

(d) Continuous Monitoring - Continuous Monitoring of Controls: The continuous monitoring of controls by the system owner is a critical part of the risk assessment, configuration management, and Security Assessment and Authorization/C&A processes. Continuous monitoring of controls is a dynamic security process requiring near real-time security status information. The credibility of risk-based decisions is at stake. Many other security processes feed on the information relayed by continuous monitoring and will find themselves influenced by how current the information is. Some of these include: security status awareness, risk posture viewpoint, mitigation decisions, and effectiveness of actions. Begin this step by deciding which controls should be continuously monitored. Selection of controls should begin by considering which controls are most volatile, common controls, and POA&M items. Many common controls are likely being monitored on a routine basis and this monitoring may only need to be reported in an appropriate fashion. The monitoring process should be designed to both detect any unanticipated changes as well as easily receive proposals for any planned changes. It is important to consider how information from continuous monitoring will be shared with organizational partners. This is important with common controls, but is also important with hybrid controls that have a split responsibility across both single systems and organizational infrastructure. Both network monitoring and audit logging may have implications for privacy concerns. It is possible for information discovered during monitoring to change the risk and security status of the system, requiring processes such as security categorization, risk assessment or others to be repeated in order to keep them up to date and reflecting the actual security profile of the system. [See security control CA-7 Continuous Monitoring].

(e) Update documentation: Any changes made in this phase must be considered for inclusion into the existing security documents. While it is obvious that configuration setting changes should be updated in documentation, any changes in the risk profile, as a result, should also be considered. It may become necessary to update both the risk assessment and the SSP.

d. **Operations and Maintenance Phase**

(1) Continuous monitoring is an ongoing assessment of security control effectiveness to determine if there is a need to modify or update security controls based on changes to the information system or its operating environment. [To develop a monitoring strategy, see security controls SI-4 Information System Monitoring Tools and Techniques, RA-5 Vulnerability Scanning, AU-6 Audit Monitoring, Analysis, and Reporting, SI-7 Software and Information Integrity, and IR-4 Incident Response]. When continuous monitoring detects events that have changed the security status or risk posture of the system, it may become necessary to reconsider or re-assess the state and may trigger some of the following steps:

(a) Documenting both proposed and detected change;

(b) Performing an impact analysis;

(c) Performing a PIA;

(d) Performing ongoing remediation [see security controls SI-2 Flaw Remediation and CA-5 Plans Of Action and Milestones];

(e) Updating security documents as needed;

(f) Performing ongoing risk determination and acceptance (essentially, a gateway into an ongoing Authorization process); and

(g) System removal (when a system becomes a candidate for removal, it must go through the change control process and impact analysis before entering the disposal phase and sanitization process).

(2) Configuration Control (end of configuration management process): The end of the configuration management process covers configuration control and monitoring. This can include continuous monitoring, previously discussed in the section above; because it is also part of several other processes [see security control CM-3 Configuration Change Control]. The steps in configuration control are:

(a) Monitor for change, either planned or detected change [see security control CM-4 Monitoring Configuration Changes];

(b) The output from continuous monitoring and change control monitoring must be scrutinized for documentation updates by the system owner that may be required as a result of the new knowledge. Key areas for this concern include:

1. POA&M;

2. SSPs;

3. SCAs;

4. PIAs, and

5. Enterprise Change Control Board (ECCB).

(c) Evaluate the change based on risk: For some continuous monitoring, the sharing of information and updates to documentation may end this part of the process, but if any configuration changes have been detected, an evaluation of how that change will affect the security posture or privacy implications of the system must be undertaken. This will probably require some form of risk assessment, although it may be limited in scope. The intent is to fully understand any ripple effect the change may have on security controls and the protections they are designed to implement.

(d) Make a risk-based decision on how to handle the change: Once the evaluation of risk is completed, a decision must be reached on whether to allow the implementation of change or reject it or to defer the decision.

(e) Take action based on the decision and document it: The key stakeholders must be notified of the decision, any actions required as a result of the decision must be implemented and the entire process must be documented.

(3) Update documentation: Once again, any changes resulting from the processes in this phase must be considered for inclusion into the security documentation and any changes in the risk profile must be examined carefully. The SSP, PIA, and risk assessment may need to be updated.

e. **Disposal Phase: Media Sanitization involves the following steps:**

(1) Information preservation – Archive, discard, or destroy decision: An archive, discard, or destroy decision on how to handle data and configuration information residing on systems scheduled to be disposed of must be made. This decision may involve legal or statutory requirements to retain information [see security control MP-5 Media Transport]. If the system owner and the information owner are different, it is important that they communicate on information preservation issues before the data is cleared. It may be necessary to consult with POs, Freedom of Information Act (FOIA) officers and the records retention office during information preservation and before any media are sanitized. The end of life cycle for privacy relation information requires an update to the PIA and the SORN may need to be revoked. Special attention should be given to any cryptographic keys remaining on such equipment.

(2) Media sanitization: It is possible to satisfy cleaning requirements by deleting information, overwriting it, degaussing the hardware, and/or destroying the hardware. The sensitivity level of the data must be considered when making this decision [see security control MP-6 Media Sanitization and Disposal].

(3) Disposal of hardware and software: Once any important information has been archived and any VA sensitive information has been sanitized, the equipment may be either

disposed of or destroyed as required.

(4) Update documentation: This process is not complete without updating documentation, as with any other phase of the SDLC. Inventory and asset management resources must be updated [see security control CM-8 Information System Component Inventory]. Other parts of the SSP, such as the risk assessment, configuration management, contingency plan, and other system documentation may also need to be updated.

5. SUMMARY

a. The SDLC framework has five phases and is a collection of continuous processes. Once the information system is operational, all of the processes across all five phases will run simultaneously.

b. Many of the processes and controls are interdependent.

c. The implementation of controls occurs across the entire SDLC framework, particularly with the following processes:

(1) The selection of security controls;

(2) Tailoring of security controls;

(3) Supplementing security controls; and

(4) The continuous monitoring of controls.

d. Two very important elements of the SDLC are:

(1) Common controls which improve cost and consistency; and

(2) Continuous monitoring which adds dynamic status information.

e. Here is how some key security processes map into those phases:

(1) **Initiation phase** (PL-1, PL-2, PL-5, CM-8, RA-2, CA-3, PE-16): System Characterization process; and

(2) **Acquisition and Development phase**, which includes:

(a) Risk assessment process (RA-3, RA-5, SI-2);

(b) Security Control Selection process (All families and controls); and

(c) Security Planning Process (PL-2, PL-4, PL-5, RA-4, AT, CP, IR).

(3) **Implementation and Assessment phase**, which includes:

(a) The configuration management process (CM-2); and

(b) The authorization (Security Assessment and Authorization/C&A) process (PL-3, RA-4, RA-5, CA-2, CA-4, CA-5, CA-6).

(4) **Operations and Maintenance phase** (PL-3, CM-3, CM-4, RA-4, SI-2, SI-3, SI-4, SI-7, IR-3, IR-4, IR-5, IR-6, CA-7): Continuous monitoring process; and

(5) **Disposal phase** (PL-3, CM-8), RA-4, MP-6): Media Sanitization process.

f. Most of these processes are ongoing and may include aspects that are spread out across the framework. In this list, the processes are placed where the core concentration of the process is located.

g. The figure below adds the security control families and key controls, as well as demonstrates the range across the SDLC framework where the controls may be expected to be involved. Only a few key controls are represented here and this is by no means a comprehensive list. Note: The slot where “ALL Families and ALL Security Controls” is marked. This is the point where all controls are considered when the baseline of controls is tailored, enhanced, and supplemented.

h. The range of the controls is ongoing across the SDLC framework and they overlap each other. When a process or group of controls is described, they are often presented in an isolated framework that makes it seem as if they operate in a simple linear sequence and independently of anything else; however this is rarely the case. They almost always operate simultaneously with other processes and controls and are usually spread out across the framework.

Table 2: SDLC Framework Summary

	PL	CM	RA	SI	other	CA
	INITIATION phase					
Characterize	**PL-1,2,5**	**CM-8**	**RA-2**		**PE-16**	**CA-3**
	ACQUISITION and DEVELOPMENT phase					
Risk Assessment			**RA-3,5**	**SI-2**		
Security Controls		**ALL Families… ALL Security Controls**				
Security Plan	**PL-2,4,5**		**RA-4**		**AT,CP,IR**	
	IMPLEMENTATION and ASSESSMENT phase					
Configuration		**CM-2**				
Authorization	**PL-3**		**RA-4,5**			**CA-2,4,5,6**
	OPERATION and MAINTENANCE phase					
Continuous Monitoring	**PL-3**	**CM-3,4**	**RA-4**	**SI-2,3,4,7**	**IR-3,4,5,6**	**CA-7**
	DISPOSAL phase					
Media Sanitization	**PL-3**	**CM-8**	**RA-4**		**MP-6**	

Table2: SDLC Framework Summary demonstrates the range across the SDLC framework where the controls may be expected to be involved. (Reference Paragraph 5, Summary)

i. Some controls have been marked in places outside of either the core of a related process or the primary scope of a control family.

j. In the **Implementation phase**, the authorization (Security Assessment and Authorization/C&A) process acts as an inspection process and checks all of the primary processes across the framework to ensure security controls are in place and offering the protection they were designed to deliver.

6. REFERENCES

a. 5 CFR Part 1320, Controlling Paperwork Burdens on the Public;

b. 38 C.F.R. §§ 1.550-1.559 Release of Non-Claimant Information from VA Files

c. 38 C.F.R. §§ 1.575-1.584 Safeguarding Personal Information in VA Records

d. 38 U.S.C. 5721-5727, Information Security;

e. 38 U.S.C. 7332, Confidentiality of Certain Medical Records;

f. 60 Fed. Reg. 44634, Electronic Records Management, (1995);

g. FEA Security and Privacy Profile, Version 2.0

h. FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*;

i. FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems;*

j. FOIA, 5 U.S.C. 552

k. NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*;

l. NIST SP 800-27, *Engineering Principles for Information Technology Security;*

m. NIST SP 800-30, *Risk Management Guide for Information Technology Systems;*

n. NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems;*

o. NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*;

p. NIST SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective*;

q. NIST SP 800-40, *Creating a Patch and Vulnerability Management Program*;

r. NIST SP 800-42, *Guideline on Network Security Testing*;

s. NIST SP 800-47, *Security Guide for Interconnecting Information Technology System*;

t. NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*;

u. NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*

v. NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*

w. NIST SP 800-64, *Security Considerations in the System Development Life Cycle*;

x. NIST SP 800-88, *Guidelines for Media Sanitization*;

y. NIST SP 800-100, *Information Security Handbook: A Guide for Managers*;

z. NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*;

aa. OMB M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*;

bb. OMB M-06-16, *Protection of Sensitive Agency Information*;

cc. OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*;

dd. Privacy Act of 1974

ee. Pub. L. 99-508 Electronic Communications Privacy Act of 1986, as amended;

ff. Pub. L. 104-13, Paperwork Reduction Act of 1995;

gg. Pub. L. 109-461, Section 902;

hh. VA Handbook 6004, *Configuration, Change, and Release Management Programs;*

ii. VA Directive 6310, *Forms, Collections of Information, and Reports Management*;

jj. VA Handbook 6310.2, *Collections of Information Procedures, December 1, 2001*;

kk. VA Handbook 6500, *Information Security Program*;

ll. VA Handbook 6500.1, *Electronic Media Sanitization*;

mm. VA Handbook 6500.2, *Incident Management;*

nn. VA Handbook 6500.3, *Certification and Accreditation of VA Information Systems*;

oo. VA Handbook 6500.6, *Contract Security*;

pp. VA Handbook 6500.8, *Information Technology Contingency Planning;*

qq. VA Directive 6502, *VA Enterprise Privacy Program*

rr. VA Directive 6508, *Privacy Impact Assessments*

DEFINITIONS

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.

Accreditation Boundary - All components of an information system to be accredited by an authorizing official, excluding separately accredited systems to which the information system is connected.

Applications - Programs that give a computer instruction that provide the user with tools to accomplish a task.

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.

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.

Availability - Ensuring timely and reliable access to and use of information.

Business Continuity Preparedness - Creation and validation of a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption.

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.

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.

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

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.

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).

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.

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.

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.

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.

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.

Information Technology/Information Technology Assets - 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.

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.

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

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

Interim Authorization to Operate - Granted to complete the remaining certification requirements and expeditiously mitigate deficiencies.

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

Management Controls - The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security. They consist of: risk assessment; planning; system and services acquisition; and certification, accreditation, and security assessment.

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.

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, formation and Technology staff (system managers, system administrators, and ISOs).

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

Personally Identifiable Information (PII) - Information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.

Plan of Action and Milestones (POA&M) - A plan used as a basis for the quarterly reporting

requirements of the Office of Management and Budget 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. (H) The status of efforts to correct the weakness.

Privacy Impact Assessment (PIA) - An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Protected Health Information (PHI) - PHI is individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv), and employment records held by a covered entity in its role as employer.

Risk - 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.

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.

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.

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

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.

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.

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

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.

System Development Life Cycle - The process of creating or altering systems, and the models and methodologies that people use to develop these systems. The concept generally refers to computer or information systems.

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.

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: (i) the application of scoping guidance; (ii) the specification of compensating security controls, if needed; and (iii) the specification of organization-defined parameters in the security controls, where allowed.

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.

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.

VA Information - Information owned or in the possession of VA or any entity acting for or on

the behalf of VA.

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.

VA Sensitive Information/Data - 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.

Vulnerability - A flaw or weakness in system security procedures, design, implementation, or internal controls that can be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system’s security policy

ABBREVIATIONS/ACRONYMS USED IN HANDBOOK AND APPENDICES

Abbreviation / Acronym	Description
AO	Authorizing Official
AODR	Authorizing Official's Designated Representative
AT	Awareness and Training
BIA	Business Impact Analysis
C&A/CA	Security Assessment and Authorization/Certification and Accreditation
CIA	Confidentiality, Integrity, and Availability
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CM	Configuration Management
CO	Contracting Officer
COTR	Contracting Officer's Technical Representative
CP	Contingency Planning
ECCB	Enterprise Change Control Board
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
HIPAA	Health Insurance Portability and Accountability Act
IATO	Interim Authorization to Operate
IPRM	Information Protection and Risk Management
IR	Incident Response
ISA	Interconnection Security Agreement
ISO	Information Security Officer
IT	Information Technology
LAN	Local Area Network
LOE	Level of Effort
MP	Media Protection
NIST	National Institute of Standards and Technology
NSOC	VA Network and Security Operations Center
OGC	Office of General Counsel
OI&T	Office of Information and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PE	Physical and Environmental Protection
PIA	Privacy Impact Assessment

PL	Planning
PM	Program Management
PO	Privacy Officer
POA&M	Plan of Action and Milestones
RA	Risk Assessment
ROB	VA National Rules of Behavior
SANS	SysAdmin, Audit, Network, Security
SAR	Security Assessment Report
SCA	Security Control Assessment
SDLC	System Development Life Cycle
SI	System and Information Integrity
SORN	System of Records Notice
SP	Special Publication
SSP	System Security Plan
VA	Department of Veterans Affairs